**Leçon 108 : Exemples de parties génératrices d'un groupe. Applications.**

Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$ et $E$ un $\mathbb{K}$-espace vectoriel de dimension $n$. [Rom21].

# I Généralités

Soit $G$ un groupe noté multiplicativement.

## I.1 Sous-groupes engendrés par une partie

**Thm 1.** L'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous-groupes de $G$, est un sous-groupe de $G$.

**Cor 2.** Soit $X$ une partie de $G$. L'intersection de tous les sous-groupes de $G$ contenant $X$, est un sous-groupe de $G$. On note $< X >$ un tel sous-groupe, et on l'appelle sous-groupe engendré par X.

**Déf 3.** Si $X$ est une partie de $G$, on dit que $X$ engendre $G$ si $G =< X >$.

**Prop 4.** Soit $X$ une partie non vide de $G$. On note $X^{-1} = \{x^{-1} : x \in X\}$. Alors les éléments de $< X >$ sont de la forme $x_1 \cdots x_r$, où $r \in \mathbb{N}^*$ et les $x_k$ sont dans $X \cup X^{-1}$.

**Thm 5.** Pour tout $p \in \mathbb{N}^*$ et tout $p$-uplet $(g_1, \dots, g_p)$ d'éléments de $G$ qui commutent deux à deux, on a que $< g_1, \dots, g_r >= \{g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r} : (\varepsilon_1, \dots, \varepsilon_p) \in \mathbb{Z}^p\}$.

## I.2 Cas des groupes monogènes et cycliques

**Déf 6.** On dit que $G$ est monogène s'il existe $g \in G$ tel que $G =< g >$. Si de plus $G$ est fini, on dit qu'il est cyclique.

**Ex 7.**
1. $(\mathbb{Z}, +)$ est monogène, et pour tout $n \in \geq 2$, $(\mathbb{Z}/nZ, +)$ est cyclique.
2. Pour tout $n \geq 1$, le groupe des racines $n$-ième de l'unité $(\mathbb{U}_n, \cdot)$ est cyclique.

**Prop 8.** Les sous-groupes de $G =< a >$ sont tous cycliques.

**Prop 9.** Pour tout diviseur $d$ de $n$, il existe un unique sous-groupe d'ordre $d$ de $G$.

**Thm 10.** Un groupe abélien fini $G$ d'ordre $n \geq 1$ est cyclique, si et seulement si, pour tout diviseur $d$ de $n$, il existe un unique sous-groupe d'ordre $d$ de $G$.

**Cor 11.** Soit $p$ un nombre premier. Alors $(\mathbb{Z}/p\mathbb{Z}, \cdot)^\times$ est cyclique. Plus généralement, si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}^*$ est cyclique.

## I.3 Cryptosystème El-Gamal

[Ulm18] Alice et Bob veulent échanger des messages un système à clef publique sans que d'autres puissent déchiffrer leurs messages. Ici, un message est un nombre entier.

**Prop 12.** Considérons un groupe cyclique $G =< \gamma >$ d'ordre $n$. $\gamma$ et $n$ sont publiques.
1. Alice choisit une clef privée $1 < a < n-1$, et envoie $\gamma^a \in G$ à Bob.
2. Bob choisit une clef privée $\rho := \gamma^b \in G$, et envoie la paire $(\gamma^k, \rho \cdot (\gamma^a)^k)$ à Alice, où $k$ est un entier choisit aléatoirement.

Alice peut alors lire le message de Bob, en calculant l'inverse de $(\gamma^a)^k = (\gamma^k)^a$. Le cryptosystème est basé sur le fait qu'Alice et Bob partagent le secret $(\gamma^a)^k = (\gamma^k)^a$.

**Rq 13.** La sécurité du système réside dans la difficulté de résoudre le problème du "logarithme discret", c'est à dire, la difficulté de trouve $a$ en connaissant $\gamma^a$

**Ex 14.** Considérons $f = X^7 + 2X + 2012 \in \mathbb{F}_{2017}[X]$, qui est irréductible. Le corps $K = \mathbb{F}_{2017}[X]/(f)$ possède $2017^7$ éléments et $\gamma = \overline{X}$ est un générateur de $K^*$ d'ordre $2017^7 - 1$. Alice choisit comme clef secrète $a = 20162017$, et rend public $\gamma^a = 1362z^6 + 554z^5 + 220z^4 + 468z^3 + 1038z^2 + 868z + 6$. Afin d'envoyer le message $\rho = 66z^6 + 55z^5 + 44z^4 + 33z^2 + 22z + 11z$ à Alice, Bob choisit un entier au hasard, disons $k = 7654321$, et calcule $(\gamma^k, \rho \cdot (\gamma^a)^k)$.

# II Groupes matriciels

## II.1 Groupe linéaire et groupe spécial linéaire

**Déf 15.** Soit $\varphi$ une forme linéaire non nulle sur $E$. On appelle transvection d'hyperplan $\operatorname{Ker}\varphi$ toute application linéaire définie par $u = \mathrm{Id}_E + a\varphi$, où $a \in \operatorname{Ker}\varphi$. On notera $\tau_{\varphi,a}$ une telle transvection.

**Prop 16.** Soient $\varphi \in E^*$ non nulle, et $a \in \operatorname{Ker}\varphi$ :

1. $\tau_{\varphi,a}^2 = \tau_{\varphi,2a}$ est une transvection.
2. $\tau_{\varphi,a} \in GL(E)$, son inverse est la transvection $\tau_{\varphi,-a}$, 1 est son unique valeur propre, l'espace propre associé étant $\operatorname{Ker}\varphi$ si $a \neq 0$.
3. Le conjugué dans $GL(E)$ d'une transvection est une transvection.

**Prop 17.** $u \neq \mathrm{Id}_E$ est une transvection, si et seulement si, il existe une base dans laquelle la matrice $u$ est $T_{ij} = I_n + \lambda E_{ij}$, où $1 \leq i, j \leq n$ et $\lambda \in \mathbb{K}^*$.

**Déf 18.** Soit $\varphi$ une forme linéaire non nulle sur $E$. On appelle dilatation d'hyperplan $\operatorname{Ker}\varphi$ toute application linéaire $u \in \mathscr{L}(E)$ définie par $u = \mathrm{Id}_E + a\varphi$, où $a \in E \setminus \operatorname{Ker}\varphi$. On notera $\delta_{\varphi,a}$ une telle dilatation.

**Prop 19.** $\delta_{\varphi,a} \in GL(E)$, si et seulement si, $\lambda := 1 + \varphi(a) \neq 0$. Lorsque c'est le cas, on dit que $\delta_{\varphi,a}$ est une dilatation de rapport $\lambda$.

**Prop 20.** L'inverse d'une dilatation de rapport $\lambda$, est une dilatation de rapport $\dfrac{1}{\lambda}$.

**Prop 21.** $u \in \mathscr{L}(E)$ est une dilatation de rapport $\lambda \in \mathbb{K}^*$, si et seulement si, il existe une base de $E$ telle que la matrice de $u$ dans cette base est $\begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$.

**Lemme 22.** Soient $H_1, H_2$ deux hyperplans distincts de $E$, et $a \in E \setminus (H_1 \cup H_2)$.

1. L'ensemble $H = (H_1 \cap H_2) \oplus \mathbb{K}a$ est un hyperplan de $E$. De plus, $E = H \oplus H_1 = H \oplus H_2$.
2. Il existe une transvection $u$ telle que $u(a) = a$ et $u(H_1) = H_2$

**Cor 23.** Pour tout $x, y \in E \setminus \{0_E\}$, il existe $u \in SL(E)$ produit de une ou deux transvections tel que $y = u(x)$.

**Thm 24.** Le groupe $SL(E)$ est engendré par les transvections.

**Thm 25.** Le groupe $GL(E)$ est engendré par les transvections et les dilatations.

## II.2 Application à la résolution de système linéaire

**Thm 26.** $GL_n(\mathbb{K})$ définit une action sur $M_{n,m}(\mathbb{K})$ : $\forall P \in GL_n(\mathbb{K})$, $\forall M \in M_{n,m}(\mathbb{K})$, $P \cdot M = PM$. On l'appelle action par translation (à gauche).

**Thm 27.** Deux matrices ont même orbite pour cette action, si et seulement si, elles ont même noyau.

**Notation 28.** Soit $A = (a_{ij})_{1 \leq i \leq n,\ 1 \leq j \leq m} \in M_{n,m}(\mathbb{K})$. Pour $i \in \{1, \ldots, n\}$, on note $L_i$ sa $i$-ème ligne, $d_i = \min\{j \in \{1, \ldots, m\} : a_{ij} \neq 0\}$.

**Déf 29.** On dit qu'une matrice $A \in M_{n,m}(\mathbb{K})$ est échelonnée en lignes si elle est nulle, ou si il existe $1 \leq r \leq n$ tel que :

— Pour tout $i \in \{1, \ldots, r\}$, $L_i \neq 0$.

— Pour tout $i \geq r + 1$, $L_i = 0$.

— $1 \leq d_1 < \ldots < d_r \leq m$

**Déf 30.** On dit qu'un système linéaire $AX = b$, $A \in M_{n,m}(\mathbb{K})$ et $b \in \mathbb{R}^n$, est échelonné si la matrice $A$ est échelonnée en lignes.

**Thm 31** (Pivot de Gauss)**.** On considère les opérations élémentaires suivantes :

— La multiplication à droite par une matrice de dilatation $D_i(\lambda)$ a pour effet de remplacer $L_i$ par $\lambda L_i$.

— La multiplication à droite par une matrice de transvection $T_{ij}(\lambda)$ a pour effet de remplacer $L_i$ par $L_i + \lambda L_j$

**Thm 32.** Soit $A \in M_{n,m}(\mathbb{K})$, il existe une matrice $P \in GL_n(\mathbb{K})$, produit de matrice de permutations et de transvections, telle que la matrice $PA$ soit échelonnée en ligne. Une telle matrice est la forme normale de l'orbite de $A$ pour cette action.

**Cor 33.** Une opération élémentaire sur les lignes d'un système $Ax = b$ le transforme en un système équivalent.

## II.3 Matrices à coefficients entiers

. Soit $n \geq 1$.

**Prop 34.** $M_n(\mathbb{Z})$ est un anneau. Son groupe des inversibles est $GL_n(\mathbb{Z})$.

**Prop 35.** $SL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{Z})$ d'indice 2.

**Rq 36.** $SL_2(\mathbb{Z})$ est aussi engendré par les transvections.

**Thm 37** (DEV 1)**.** Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors $S$ et $T$ engendrent $SL_2(\mathbb{Z})$.

**Rq 38.** Ce système générateur a le bon gout d'avoir un nombre fini de générateurs.

**Cor 39.** $SL_2(\mathbb{Z}) \simeq < S, T : S^4 = I_2,\ (ST)^3 = -I_2 >$

**Prop 40** (DEV 1)**.** Soit $N \geq 2$. On pose $\Gamma_N = \{A \in SL_2(\mathbb{Z}) : A \equiv I_2 \pmod N\}$. Alors $SL_2(\mathbb{Z})/\Gamma_N \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$ et $[SL_2(\mathbb{Z}) : \Gamma_N] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$, $p$ premier.

**Cor 41.** $SL_2(\mathbb{Z}/N\mathbb{Z})$ est engendré par la classe modulo $N$ de $S$ et $T$.

**Je mettrai pas les résultats ci-dessous sur mon plan final. Je l'écris juste ici pour moi, pour me préparer à des questions**

**Thm 42.** Le groupe $SL_2(\mathbb{Z})$ agit par biholomorphisme sur le demi plan supérieur complexe, aussi appelé demi-plan de Poincaré, $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ par : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$

**Cor 43.** Sous cette action $S \cdot z = -\frac{1}{z}$, et $T^k \cdot z = z + k$.

**Prop 44.** Le point $i$ est fixé par $S$. Donc $\mathrm{Stab}(i) = < S >$, c'est un groupe cyclique d'ordre 4. Le point $e^{\frac{2i\pi}{3}}$ est fixé par $ST$. Donc son stabilisateur est un groupe cyclique d'ordre 6.

# III Groupes symétrique

[Rom21] Soit $E$ un ensemble fini de cardinal $n$ non nul.

**Déf 45.** On appelle groupe des permutations de $E$, noté $\mathfrak{S}(E)$, le groupe des bijections de $E$ dans lui même. Si $E = \{1, \dots, n\} \subseteq \mathbb{N}$, on le note $\mathfrak{S}_n$, et on l'appelle groupe symétrique.

**Prop 46.** Soit $\sigma \in \mathfrak{S}(E)$. Le groupe $H = < \sigma >$ agit sur $E$ par $\sigma^k \cdot x = \sigma^k(x)$, $x \in E$. Les orbites de cette action sont les ensemble $H \cdot x = \{\sigma^k(x) : k \in \mathbb{Z}\}$. On les appelle $\sigma$-orbite.

**Prop 47.** Soit $\sigma \in \mathfrak{S}(E) \backslash \{\mathrm{Id}_E\}$ et $O$ une $\sigma$-orbite de cardinal $r \geq 2$. Pour tout $x \in O$, $r$ est le plus entier naturel non nul tel que $\sigma^r(x) = x$, et $O = < \sigma > \cdot x = \{x, \sigma(x), \dots, \sigma^{r-1}(x)\}$.

**Thm 48.** Une permutation $\sigma \in \mathfrak{S}(E)$ est un cycle d'ordre $r \geq 2$, si et seulement si, il n'y a qu'une seule $\sigma$-orbite non réduite à un point.

**Déf 49.** Soit $\sigma \in \mathfrak{S}(E)$. On appelle support de $\sigma$ l'ensemble $\mathrm{Supp}(\sigma) = \{x \in E : \sigma(x) \neq x\}$. Deux cycles de $E$ sont disjoints s'ils ont un support un disjoint.

**Thm 50.** Toute permutation $\sigma \in \mathfrak{S}(E) \backslash \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints, c'est à dire que le groupe $\mathfrak{S}(E)$ est engendré par les cycles. Une telle décomposition est unique, et si l'on a $\sigma = \gamma_1 \dots \gamma_p$, alors $\mathrm{Supp}(\sigma) = \bigcup_{i=1}^{p} \mathrm{Supp}(\gamma_i)$, et $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(\gamma_1), \dots, \mathrm{ord}(\gamma_p))$.

**Cor 51.** Le groupe $\mathfrak{S}(E)$ est engendré par les transpositions.

**Ex 52.** Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$, on a $\sigma = (1,2)(2,3)(3,4)(4,5)(6,7)$

**Déf 53.** Pour $\sigma \in \mathfrak{S}(E)$, on note $\mu(\sigma)$ le nombre de $\sigma-$orbites distinctes. La signature d'une permutation $\sigma \in \mathfrak{S}(E)$ est alors l'élément défini par $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$

**Lemme 54.** Pour tout $\sigma \in \mathfrak{S}(E)$, et toute transposition $\tau$, $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$

**Cor 55.** Si $\sigma \in \mathfrak{S}(E)$ est produit de $p$ transpositions, alors $\varepsilon(\sigma) = (-1)^p$.

**Thm 56.** Les seuls morphismes de groupes de $(\mathfrak{S}(E), \circ)$ dans $(\mathbb{R}^*, \cdot)$ sont l'application constante égale à 1, et $\varepsilon$.

# IV Groupe orthogonal et spécial orthogonal

## IV.1 Système générateur

Dans cette partie, $E$ désigne un espace euclidien de dimension $n$, munit du produit scalaire $< \cdot, \cdot >$. Soit $\|\cdot\|$ sa norme associée.

**Déf 57.** Soit $F$ un sous-espace vectoriel de $E$. La symétrie orthogonale par rapport à $F$ est l'application définie sur $E$ par : $\forall x \in E$, $s_F(x) = p_F(x) - p_{F^\perp}(x)$. Où $p_F$ désigne le projeté orthogonal sur $F$.

**Déf 58.** On appelle réflexion une symétrie orthogonale par rapport à un hyperplan. On appelle retournement une symétrie orthogonale par rapport à un sous-espace de dimension $n-2$.

**Prop 59.** Soit $F$ un sous-espace vectoriel de $E$. $s_F^2 = s_F$ et $s_F$ est auto-adjoint. $s_F \in O(E)$. Enfin, si $F$ est de dimension $1 \leq p \leq n-1$, il existe une base dans laquelle la matrice de $s_F$ est $\begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}$. D'où $\det s_F = (-1)^{n-p}$.

**Thm 60.** Si $\dim E \geq 2$, $O(E)$ est engendré par les réflexions. Précisément, toute isométrie de $E$ peut s'écrire comme le produit d'au plus $n$ réflexions.

**Thm 61.** $SO(E)$ est engendré par les retournements.

**App 62.** $SO_3(\mathbb{R})$ est simple.

## IV.2 Application aux quaternions

[CG17]

**Déf 63.** On appelle corps des quaternions, et l'on note $\mathbb{H}$ l'algèbre de dimension 4 sur le corps des réels, ayant pour base $(\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k})$, dans laquelle la multiplication est définie par :

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \text{ et } \mathbf{ijk} = -1.$$

**Notation 64.** On note $SU_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : |a|^2 + |b|^2 = 1 \right\}$.

**Prop 65.** $SU_2(\mathbb{C})$ est un sous-groupe de $GL_2(\mathbb{C})$, homéomorphe avec $\mathbb{S}^3$.

**Notation 66.** On note $H^* \simeq \mathbb{R}_+^* I_2 \times SU_2(\mathbb{C}) \subseteq GL_2(\mathbb{C})$.

**Thm 67.** $\mathbb{H} \simeq H^* \cup \{0\}$. On notera alors $\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : a, b \in \mathbb{C} \right\}$.

**Notation 68.**

1. Si $x, y, z, t \in \mathbb{R}$, et si l'on note $a = x + iy$, $b = z + it$, un élément de $\mathbb{H}$ s'écrit $h = x\mathbf{1} + y\mathbf{i} + z\mathbf{j} + t\mathbf{k} = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$.
2. On note $\overline{h} = x\mathbf{1} - y\mathbf{i} - z\mathbf{j} - t\mathbf{k}$ le conjugué de $h$.
3. On note $N(h) = \det h = |a|^2 + |b|^2 = x^2 + y^2 + z^2 + t^2$.
4. On note $\mathbb{I} = \mathrm{Vect}_{\mathbb{R}}(\mathbf{i}, \mathbf{j}, \mathbf{k})$.

**Prop 69.** $N$ définit une norme sur $\mathbb{H}$, et $N(hh') = N(h)N(h')$ pour tout $h, h' \in \mathbb{H}$.

**Thm 70.** $\mathbb{H}$ est une sous-algèbre de $M_2(\mathbb{C})$. De plus, c'est un corps non commutatif. Son centre est $\mathbb{R}$.

**Thm 71** (DEV 1)**.** Il existe deux isomorphismes de groupes :

1. $SU_2(\mathbb{C})/\{\pm I_2\} \simeq SO_3(\mathbb{R})$.
2. $SU_2(\mathbb{C}) \times SU_2(\mathbb{C})/\{(I_2, I_2), (-I_2, -I_2)\} \simeq SO_4(\mathbb{R})$.

## Bibliographie


[CG17] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome second*. Calvage et Mounet, 2017.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation : Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 2021.

[Ulm18] Felix Ulmer. *Anneaux, corps, résultants*. ellipses, 2018.