Générateurs de $\mathrm{SL}_2(\mathbb{Z})$

Julie Parreaux

2018-2019

Référence du développement : Alessandri, *Thèmes en géométrie* [1, p.81]

Leçons où on présente le développement : 182 (Nombres complexes en géométrie) ; 183 (Groupe et géométrie).
Leçons où on peut en parler : 101 (Actions de groupe) ; 108 (Générateurs d'un groupe).

1 Introduction

Connaître un ensemble de générateurs pour un groupe est rarement simple. La géométrie est une méthode permettant de déterminer les générateurs ; on fait agir le groupe dont on souhaite connaître les générateurs sur un ensemble bien choisi. Pour le groupe $SL_2(\mathbb{Z})$: on fait agir ce groupe par homographie sur le plan complexe. Cet étude fait émerger une étude du demi-plan de Poincaré.

2 Étude des générateurs de $\mathrm{SL}_2(\mathbb{Z})$

Théorème. *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par les matrices* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Schéma du développement

Ce développement est très long, il est difficile (voire impossible) de tout faire : il faut faire des choix (le plus pertinent, le plus technique, les endroit où on est le plus à l'aise, ...).

1. Le groupe $\mathrm{Sl}_2(\mathbb{Z})$ agit sur P par homographie (lemme 1).
2. $G = \langle S, T \rangle$ agit sur P : toutes les orbites rencontrent $D = \{z \in P \mid |z| \geq 1, |\Re(z)| \leq \frac{1}{2}\}$ (lemme 2).
   (a) Dire qu'il existe un nombre fini de couple d'entier $(c, d) \in \mathbb{Z}^2$ tel que $|cz + d| \leq 1$.
   (b) Dire que $I_z = \{\Im(u) \mid u \in O_z\} = \{\Im(A * z) \geq \Im(z)\}$ admet un maximum : M_z donné par A_1.
   (c) On pose $z_1 = A_1 * z$, $n = \lfloor \Re(z_1) + \frac{1}{2} \rfloor$ et $z_2 = T^{-n} * z_1$. D'où $z_2 \in D$ et $\Im(z_2) = M_z$.
      i. Dire que si $u \in P$ alors $T * u = u + 1$.
      ii. Montrer que $|\Re(z_2)| \leq \frac{1}{2}$.
      iii. Montrer que $|z_2| \geq 1$.
      iv. Montrer que $S * z_2 \in O_z$.
3. $A \in \mathrm{SL}_2(\mathbb{Z})$ tel que $A * z \in D$ est une matrice de G (lemme 3).
   (a) Dire que $c \in \{0, -1, 1\}$.
   (b) Étude du cas $c = 0$.
4. Conclure en appliquant les deux lemmes.

Démonstration. Soit $P = \{z \in \mathbb{C}, \mathrm{Im} > 0\}$ le demi-plan de Poincaré.

Lemme 1. *Le groupe* $\mathrm{SL}_2(\mathbb{Z})$ *agit sur* P *par homographie : si* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $A * z = \frac{az+b}{cz+d}$.

Démonstration. Soit A et $B \in \mathrm{SL}_2(\mathbb{Z})$ et $z \in P$:

$$\begin{array}{rcll} \Im(A*z) & = & \frac{(ab-dc)}{|cz+d|^2}\Im(z) & (A*z = \frac{ac|z|^2+bd+adz+bc\bar{z}}{|cz+d|^2}) \\ & = & \frac{\Im(z)}{|cz+d|^2} & (ab-dc = \det A = 1) \\ & > & 0 & (\text{hypothèse sur } z) \end{array}$$

Donc $\mathrm{SL}_2(\mathbb{Z})$ opère par homographie sur P. □

Notons G le sous-groupe engendré par S et T et $D = \{z \in P \mid |z| \geq 1, |\Re(z)| \leq \frac{1}{2}\}$.

Lemme 2. *G agit via l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *sur P. Alors, pour cette action de G, toutes les orbites rencontre D.*

Démonstration. *Idée* : Construire un point "d'altitude maximale" sur l'orbite O_z, z fixé dans P puis de le translater à "altitude constante" (grâce à T) pour rentrer dans D. Les étapes de cette preuves doivent être effectuer dans le bon ordre pour être correcte : il faut commencer par trouver le point maximum avant de le translater. Enfin il faut vérifier si on appartient à D. La translation doit être effectuer avant la vérification sinon on peut la vérifier avant mais plus après.

Étape a : montrons qu'il existe un nombre fini de couple d'entier $(c,d) \in \mathbb{Z}^2$ **tel que** $|cz+d| \leq 1$. On a

$$\begin{array}{rcll} |c|\,\Im(z) & = & |\Im(cz+d)| & (d \in \mathbb{Z}) \\ & \leq & |cz+d| & |w| = \sqrt{\Re(w)^2+\Im(w)^2} \geq |\Im(w)| \\ & \leq & 1 & (\text{hypothèse}) \end{array}$$

Donc $|c| \leq \frac{1}{\Im(z)}$ (car $\Im(z) > 0$ et $|d| \leq 1 + |c|\,|z|$ (par les propriétés du module). On en déduit le nombre fini de couple.

On pose $I_z = \{\Im(u) \mid u \in O_z\} = \{\Im(A*z) \geq \Im(z)\}$.

Étape b : montrons que I_z admet un maximum.

— On a un nombre fini de (c,d) tel que $\Im(A*z) \geq \Im(z)$ (on applique l'égalité précédente à celle de $\Im(A*z)$).

— Il existe A_1 tel que $M_z = \Im(A*z)$ soit le maximum de I_z (on inclut dans la sphère unité qui est compacte).

On pose $z_1 = A_1 * z$, $n = \lfloor \Re(z_1) + \frac{1}{2} \rfloor$ et $Z_2 = T^{-n} * z_1$.

Étape c : montrons que z_2 appartient à la bande d'équation $|\Re(u)| \leq \frac{1}{2}$ et, de plus, on a $\Im(z_2) = M_z$.

— Soit $u \in P$, montrons que $T*u = u+1$.

$$T*u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} * u = \frac{u+1}{1} = u+1$$

— Montrons que $|\Re(z_2)| \leq \frac{1}{2}$.

  — Montrons que $\Re(z_2) = \Re(z_1) - n$.

$$\begin{array}{rcll} \Re(z_2) & = & \Re(T^{-n} * z_1) & (\text{définition de } z_2) \\ & = & \Re(\frac{z_1-n}{1}) & (\text{définition de } A*z \text{ et } T^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}) \\ & = & \Re(z_1 - n) & (\text{calcul}) \\ & = & \Re(z_1) - n & (n \in \mathbb{Z}) \end{array}$$

— Montrons que $-\frac{1}{2} \leq \Re(z_2)$: on montre que $-\frac{1}{2} \leq \Re(z_1) - n$.

$$\begin{array}{rcll} \Re(z_1) - n & = & \Re(Z) - \lfloor \Re(z_1) + \frac{1}{2} \rfloor & \text{(par définition de } n\text{)} \\ & \leq & \Re(z_1) - \Re(z_1) - \frac{1}{2} & \text{(définition de la borne inférieure)} \\ & \leq & -\frac{1}{2} & \text{(par calcul)} \end{array}$$

— Montrons que $\Re(z_2) \leq \frac{1}{2}$: on montre que $\Re(T^{-n} * z_1) \leq \frac{1}{2}$. Or comme $T^{-n} * u = u - n$, et que $z_1 = z + n$ où $\Re(z) \leq \frac{1}{2}$, alors, $\Re(T^{-n} * z_1) \leq \frac{1}{2}$.

— Montrons que $|z_2| \geq 1$ (on le montre bien pour z_2 et non pour z_1 car sans la translation on peut être de module supérieur à un mais pas après la translation). On raisonne par l'absurde : on suppose que $|z_2| < 1$. Dans ce cas,

$$\begin{array}{rcll} \Im(S * z_2) & = & \frac{\Im(z_2)}{|z_2|^2} & \text{(propriété de l'action de groupe évaluer en les valeurs de } S\text{)} \\ & > & M_z & (|z_2| \geq 1 \text{ (par hypothèse))} \end{array}$$

Or,

$$\begin{array}{rcll} \Im(z_2) & = & \Im(T^{-n} * z_1) & \text{(définition de } z_2\text{)} \\ & = & \Im(z_1) & (T^{-n} * z_1 = z_1 - n \text{ avec } n \in \mathbb{Z}) \\ & = & M_z & \text{(par définition de } M_z\text{)} \end{array}$$

— Montrons que $S * z_2 \in O_z$.

$$\begin{array}{rcll} S * z_2 & = & S * T^n A_1 * z_1 & \text{(par définition de } z_2\text{)} \\ & = & ST^n A_1 * z_1 & \text{(par propriété de l'action)} \\ & \in & O_z & \text{(définition de l'orbite)} \end{array}$$

□

On cherche maintenant à caractériser les matrices de $\mathrm{SL}_2(\mathbb{Z})$ tel que $A * z \in D$ pour z fixé. Posons $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $A * z \in D$.

Lemme 3. *A est une matrice de G.*

Démonstration. **Cas** $\Im(A * z) \geq \Im(z)$: $|cz + d| \leq 1$. Montrons que $c \in \{0, -1, 1\}$ et examinons chacun de ces cas.

$$\begin{array}{rcll} |c| & \leq & \frac{1}{\Im(z)} & \text{(début du lemme 2)} \\ & \leq & \frac{2}{\sqrt{3}} & \text{(égalité dans le cas } j \text{ ou } -\frac{1}{j}\text{)} \\ & < & 2 & (\sqrt{3} > 1) \end{array}$$

Comme $c \in \mathbb{Z}$, on en déduit que $c \in \{0, -1, 1\}$.

Cas $c = 0$ On a $ad = 1$ (car $\det A = 0$ et $c = 0$). Quitte à changer A en $-A$ (invariant pour le déterminant et l'action de groupe), on suppose que $a = d = 1$ et $A * z = z + b$ (calcul de l'action).

— Si $|\Re(z)| < \frac{1}{2}$ alors $b = 0$ et $A \in \{Id, -Id\}$ ($A * z = z + b \in D$ et $b \in \mathbb{Z}$, 0 est la seule valeur qui convient).

— Si $|\Re(z)| = -\frac{1}{2}$ alors $b \in \{0, 1\}$ et $A \in \{Id, -Id, T\}$ (même argument).

— Si $|\Re(z)| = \frac{1}{2}$ alors $b \in \{0, -1\}$ et $A \in \{Id, -Id, T^{-1}\}$ (même argument).

Cas $c = 1$ On a alors $|z + d| \leq 1$. On a déduit que $d = 0$ ou $z = j$ et $d = 1$ (car $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ donc $|j + 1| = \frac{1}{2} + i\frac{\sqrt{3}}{2} = 1$) ou $z = -\frac{1}{j}$ et $d = -1$ (car $\frac{1}{j} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ donc $|j - 1| = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = 1$).

— Si $d = 0$, alors $1 = \det A = -b$ ($\det A = ad - bc$ avec $d = 0$ et $c = 1$) et $A * z = a - \frac{1}{z}$ (car $A * z = \frac{az+b}{cz+d}$ avec $d = 0$ et $c = 1$. Comme $|z| \leq 1$ (par hypothèse) et $|z| \geq 1$ (car $z \in D$), on a $|z| = 1$.

— Dans ce cas $\frac{1}{z}$ est le symétrique de z par rapport à l'axe des imaginaires purs.

— $\left(a - \frac{1}{z}\right)$ ne peut être dans D que si $a = 0$ ou si $z = j$ et $a = -1$ ou si $z = \frac{1}{j}$ et $a = 1$ ($z \in D$ si et seulement si $|z| \geq 1$ et $|\Re(z)| \leq \frac{1}{2}$).

Dans ce cas, $A \in \{S, (ST)^2, TS\}$.

— Si $z = j$ et $d = 1$. Comme $\det A = 1 = a - b$ et $A * j = \frac{aj+(a-1)}{j+1} = a - \frac{1}{j} = a + j$. Comme $a + j \in D$ alors $a = 0$ ou $a = 1$. Dans ce cas, $A \in \{ST, TST\}$

— Si $z = -\frac{1}{j}$ et $d = -1$. De même, on trouve que $A \in \{(TS)^2, T^{-1}ST^{-1}\}$.

Cas $c = -1$ On se ramène au cas précédent en considérant A par $-A$ (ce qui ne modifie pas $A * z$).

Cas $\Im(A * z) \geq \Im(z)$ Comme $\Im(A * z) < \Im(A^{-1}(A * z))$, on applique le cas précédent à A^{-1}.

□

Soit $z \in \mathring{D}$. Soit $A \in G$, $A * z$ est sur l'orbite de O_z de z.

— Le lemme 2 assure qu'il existe $B \in G$ tel que $B * (A * z) = BA * z \in D$.

— Le lemme 3 assure que $BA \in \{Id, -Id\}$ et donc $A \in \{B, B^{-1}\}$ (on est nécessairement dans le cas $c = 0$ et $|\Re(z)| < \frac{1}{2}$ car sinon $z \notin \mathring{D}$) (car c'est le seul cas qui considère un élément dans l'intérieur de D).

— Comme $S^2 = -Id$, $G = SL_2(\mathbb{Z})$.

□

3 Compléments sur les actions de groupes

Les actions de groupes [3, p.195] sont des notions importantes car elles permettent d'agir sur un ensemble. Elles ont plusieurs applications notamment en géométrie (c'est la base de la géométrie) ou en dénombrement si le groupe est fini (via les formules sur les cardinaux).

Remarque : Il y a deux monde : celui des groupes et des objets sur lesquels ils agissent. La translation dans le monde des objets (par application de l'action) se traduit par la conjugaison dans les groupes.

Définition (Action de groupes)**.** Une action de groupe d'un groupe G sur un ensemble X est une application $f : G \times X \to X$ telle que $\forall x \in X, f(e, x) = x$ et $\forall g_1, g_2 \in G, \forall x \in X, f(g_1.g_2, x) = f(g_1, f(g_2, x))$.

Une action de groupe de G sur X peut être également la donné d'un morphisme de G dans $\mathfrak{S}_{|X|}$.

Définition (Action fidèle [2, p.174])**.** Soit G un groupe agissant sur E. On dit que G agit fidèlement sur E si pour tout $g \in G$, $gx = x$ pour tout $x \in E$ implique $g = 1_G$ (le neutre). Autrement dit si le morphisme de l'action est injectif.

Exemple (Actions de groupes) : Donnons quelques exemples classiques d'actions de groupes.

— G opère sur G par translation à gauche.

— G opère sur $\mathcal{P}(G)$ par translation à gauche.

— G opère sur G par conjugaison.

— G opère sur $\mathcal{P}(G)$ par conjugaison.

Définition (Stabilisateur)**.** On définit le stabilisateur de l'action, pour tout élément $x \in X$, comme $\text{Stab}(x) = \{g \in G, f(g, x) = x\}$.

Remarque : Le stabilisateur d'un élément x de X est vu comme l'ensemble des éléments (de G) qui stabilise, "laisse fixe" x lors de l'application de f. On vérifie facilement que $\text{Stab}(x)$ est un sous-groupe de G.

Définition (Action libre [4, p.16])**.** Une action de G sur X est libre si tous les stabilisateurs des points de X sont triviaux.

Proposition ([4, p.15])**.** *Soit G un groupe opérant sur un ensemble X et $x \in X$. Alors,* $\text{Stab}(g.x) = g\text{Stab}(x)g^{-1}$.

Démonstration. $\left(g\text{Stab}(x)g^{-1}\right).(g.x)$(Action du groupe $\left(g\text{Stab}(x)g^{-1}\right)$ sur l'image) $= (g\text{Stab}(x)).x$ (calcul des actions) $= g.x$ (stabilisateur). On en déduit l'inclusion $\subseteq$. En remplaçant x par $g.x$ et g par g^{-1}, on obtient par le même procédé, l'inclusion inverse. □

Proposition ([6, p.31])**.** *Soit $\varphi : G \to \mathfrak{S}(X)$ une action de G sur l'ensemble X. Alors,* $\ker(\varphi) = \bigcap_{x \in X} \text{Stab}(x)$.

Démonstration. Si $g \in \ker(\varphi)$, $g.x = \varphi(g)(x) = e.x = x$ et $g \in \bigcap_{x \in X} \mathrm{Stab}(x)$. Inversement, $g.x = \varphi(g)(x) = x$ et $g \in \ker(\varphi)$. □

Remarque : On justifie ainsi la définition d'action fidèle et notamment l'injectivité du morphisme.

Proposition ([6, p.42]). *Si $m \leq n$, alors si $\mathfrak{S}_n$ agit sur $\mathfrak{S}_m$ alors $\mathfrak{S}_m \simeq \bigcap_{p \in \{m+1,\dots,n\}} \mathrm{Stab}(p)$.*

Lemme 4 ([2, p.172]). *Soit G opérant sur un ensemble E. La relation sur E définie par $x \sim y$ s'il existe $g \in G$ tel que $y = g.x$ est une relation d'équivalence.*

Démonstration. **Reflexive** On prend $g = 1_G$

Symétrique On multiplie par g^{-1}

Transitive On utilise les propriétés de calcul □

Définition (Orbite). L'orbite de l'action, pour tout élément $x \in X$, comme : $\mathrm{Orb}(x) = \{y \in X | \exists g \in G, f(g,x) = y\}$.

Remarque : Une orbite est une classe d'équivalence sur la relation d'équivalence définie précédemment. Une orbite d'un élément x de X comme l'ensemble des éléments (de X) atteignable à partir de x en appliquant f à un g.

Exemple (Exemples sur ces notions) : Quelques exemples sur les notions d'orbites et de stabilisateurs.

— G opère sur G par translation à gauche.
  — $\mathrm{Stab}(x) = \{e\}$
  — $\mathrm{Orb}(x) = G$ (ici $X = G$)

Définition (Action transitive [2, p.172]). On dit que G agit transitivement sur E si pour tous $x, x' \in E$, il existe $g \in G$ tel que $x' = gx$.

Lemme 5 ([2, p.172]). *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*

1. *G agit transitivement sur E*
2. *$\forall x \in E$, $\mathrm{Orb}(x) = E$*
3. *$\exists x_0 \in E$ tel que $\mathrm{Orb}(x_0) = E$*
4. *E n'admet qu'une seule orbite : E*

Démonstration. **Montrons** $1 \Rightarrow 2$ $\mathrm{Orb}(x) \subseteq E$: définition. $\mathrm{Orb}(x) \supseteq E$: si $x' \in E$, $\exists g$ tel que $x' = g.x$, alors $x' \in \mathrm{Orb}(x)$.

Montrons $2 \Rightarrow 3$ Évident

Montrons $3 \Rightarrow 4$ Par la relation d'équivalence : les classes forment une partition.

Montrons $4 \Rightarrow 1$ Soient $x, x' \in E$, alors x, x' sont dans la même orbite. Donc, il existe g tel que $x' = gx$. □

Définition (Points fixes). Nous définition les points fixes d'un élément g de G comme l'ensemble des éléments (de X) qui sont stabilisés par g. De manière plus formelle on définit l'orbite comme $\mathrm{Fix}(g) = \{x \in X, f(g,x) = x\}$.

Lemme 6 ([2, p.172]). *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*

1. *x est un point fixe sous l'action de G*
2. *$\mathrm{Orb}(x) = \{x\}$*
3. *$|\mathrm{Orb}(x)| = 1$*
4. *$\mathrm{Stab}(x) = G$*

Démonstration. **Montrons** $1 \Rightarrow 2$ Définition orbite et point fixe.

Montrons $2 \Rightarrow 3$ Évident

Montrons $3 \Rightarrow 4$ $\mathrm{Stab}(x) \subseteq G$: ok ; $\mathrm{Stab}(x) \supseteq G$: comme $|\mathrm{Orb}(x)| = 1$, $\forall g, g.x = x$. Donc $\forall g, g \in \mathrm{Stab}(x)$.

Montrons $4 \Rightarrow 1$ Définition orbite et point fixe. □

Lemme 7. *Soit G un groupe et X un ensemble sur lequel G agit. Pour tout élément $x \in X$, on a la relation suivante : $|\mathrm{Stab}(x)|\,|\mathrm{Orb}(x)| = |G|$*

Démonstration. On prouve cette relation à l'aide d'une bijection entre Orb et G/Stab.

Soit $x \in X$. On pose

$$\varphi_x : \begin{array}{ccc} G/\mathrm{Stab} & \to & \mathrm{Orb} \\ g & \mapsto & f(g,x) \end{array}$$

Cette application est bien définie car Stab est un sous-groupe de G donc le quotient est bien un groupe. (Attention : ce n'est pas un morphisme car Orb est un sous-ensemble de X.) De plus, elle est surjective par définition de l'orbite.

Elle est injective. En effet, si $g_1, g_2 \in G$ tels que $f(g_1,x) = f(g_2,x)$. On a alors, en composant par g_1^{-1}, $f(g_1^{-1}, f(g_1,x)) = f(g_1^{-1}, f(g_2,x))$. Par les propriétés sur f, on a $f(g_1^{-1}g_1, x) = f(g_1^{-1}g_2, x)$. Or, comme $f(e,x) = x$, on a $f(g_1^{-1}g_2, x) = f(g_1^{-1}g_1, x) = f(e,x) = x$.

On a donc bien une bijection entre ces deux ensembles finis et on conclut en passant aux cardinaux. □

Lemme 8. *Soit G un groupe et X un ensemble sur lequel G agit. On a la relation suivante $\sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |\mathrm{Stab}(x)|$*

Démonstration. On pose un ensemble $S = \{(g,x) \in G \times X | f(g,x) = x\}$. On pose ensuite l'application S définie telle que :

$$S: \begin{array}{ccc} G \times X & \to & \{0,1\} \\ g, x & \mapsto & \left\{ \begin{array}{ll} 1 & \text{si } (g,x) \in S \\ 0 & \text{sinon} \end{array} \right. \end{array}$$

Comme $\text{Stab}(x)$ et $\text{Fix}(g)$ forment des partitions respectivement de X et de G, on a $S(.,x) = \mathbb{1}_{\text{Stab}(x)}$ et $S(g,.) = \mathbb{1}_{\text{Fix}(g)}$. On a alors $|S| = \sum_{g\in G} |\text{Fix}(g)| = \sum_{x\in X} |\text{Stab}(x)|$. D'où le résultat. □

Théorème (Formule du Burnside)**.** *Soit G un groupe et X un ensemble sur lequel G agit. Le nombre d'orbite de l'action est $t = \frac{1}{|G|} \sum_{g\in G} |Fix(g)|$*

Démonstration. On va alors montrer que $t\,|G| = \sum_{g\in G} |Fix(g)|$. On remarque que $X = \sqcup_{i=1}^{t} \text{Orb}(x_i)$ où x_i est un représentant d'un des orbites. Comme on a $\sum_{g\in G} |\text{Fix}(g)| = \sum_{x\in X} |\text{Stab}(x)|$ (lemme 8) $= \sum_{i=1}^{t} |\text{Orb}(x_i)| \frac{|G|}{|\text{Orb}(x_i)|}$ (lemme 7) $= t\,|G|$ (G indépendant somme). D'où le résultat. □

Remarque : On voit apparaître une version de la formule des classes.

Actions associées à l'action d'un groupe et invariants [5, p.47]

Proposition. *Soit G un groupe opérant sur un ensemble E, $p \in \mathbb{N}*$, alors G opère de façon naturelle sur $E^p = E_\times \cdots \times$ par $g(x_1, \ldots, g_p) = (gx_1, \ldots gx_p)$.*

G opère aussi sur $\mathcal{P}(E)$, l'ensemble des sous-ensembles de E par l'action : si $A \in \mathcal{P}(E)$, $gA = \{ga, a \in A\}$.

De plus, si G opère sur E et F, il opère sur l'ensemble des fonctions de E dans F.

Définition. Soit G un groupe opérant sur E. Un élément $x \in E$ est dit invariant quand : $\forall g \in G, gx = x$.

Si on se donne un espace homogène (G, E), un ensemble K et qu'on fait opérer G sur K de manière triviale, on cherche le plus petit entier p et une (ou plusieurs) fonction invariante $f : E^p \to K$. Cette recherche est la recherche d'invariant pour notre action de groupe et dans ce cas précis pour la géométrie que l'on considère.

Cette recherche d'invariant permet la classification des figures. Si on se donne une géométrie par un espace homogène (G, E). On considère l'espace des orbites $\mathcal{P}(E)/G$ (définit par l'action de G sur $\mathcal{P}(E)$) et on cherche suffisamment d'invariant sur chaque orbite pour les caractériser (puisqu'une figure en géométrie correspond à une orbite de cette action).

Références

[1] M. Alessandri. *Thèmes de géométrie : groupe en situation géométrique*. Dunod, 1999.

[2] G. Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[3] J. Calais. *Éléments de la théorie des groupes*. puf, 1984.

[4] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries, tome 1*. Calvage et Mounet, 2013.

[5] G. Laville. *Géométrie pour le capes et l'agrégation*. ellipse, 1998.

[6] F. Ulmer. *Théorie des groupes*. ellipses, 2012.