Groupe linéaire, groupe affine

Dans tout ce chapitre, E désigne un espace vectoriel de dimension finie n sur un corps commutatif $\mathbb{K}$.

1 Groupe linéaire, groupe spécial linéaire

Le *groupe linéaire de E*, noté $GL(E)$, est le groupe formé par les transformations bijectives et linéaires de E sur lui-même. La donnée d'une base quelconque $\mathscr{B}$ de E permet de construire un isomorphisme entre $GL(E)$ et le groupe $GL(n, \mathbb{K})$ des matrices carrées $n \times n$, inversibles et à coefficients dans $\mathbb{K}$: celui qui à $u \in GL(E)$ associe la matrice de u dans la base $\mathscr{B}$. Cet isomorphisme fournit un outil pratique pour l'étude de $GL(E)$: le calcul matriciel. Mais attention, ce n'est pas un isomorphisme canonique, car il dépend de la base choisie. Rappelons ici que deux matrices sont conjuguées dans $GL(n, \mathbb{K})$ si et seulement si elles représentent le même élément de $GL(E)$ dans deux bases de E. De même, deux éléments u et u' de $GL(E)$ sont conjugués dans $GL(E)$ si et seulement si on peut trouver deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E telles que la matrice de u dans la base $\mathscr{B}$ soit aussi la matrice de u' dans la base $\mathscr{B}'$.

La loi de groupe de $GL(E)$, qui est la loi de composition des applications, sera ici notée multiplicativement uv à la place de $u \circ v$, afin d'alléger l'écriture ; de plus, cette notation a l'avantage de s'accorder avec celle utilisée pour la multiplication des matrices.

L'application déterminant : $GL(E) \longrightarrow \mathbb{K}^*$ est un morphisme surjectif de $GL(E)$ sur le groupe multiplicatif des scalaires non nuls. Son noyau s'appelle le *groupe spécial linéaire de E*, et se note $SL(E)$. Ainsi,

$$SL(E) \overset{\text{déf}}{=} \{u \in GL(E) \ / \det u = 1\}$$

est un sous-groupe distingué de $GL(E)$, et on a la suite exacte

$$1 \longrightarrow SL(E) \longrightarrow GL(E) \xrightarrow{\det} \mathbb{K}^* \longrightarrow 1.$$

Le sous-groupe $SL(E)$ est bien sûr isomorphe au sous-groupe de $GL(n, \mathbb{K})$ formé des matrices de déterminant 1, et noté $SL(n, \mathbb{K})$.

Proposition 1.1 *$GL(E)$ est un produit semi-direct de $SL(E)$ par $\mathbb{K}^*$.*

Preuve — On montre ce résultat pour le groupe $GL(n, \mathbb{K})$. Il suffit pour cela de trouver un sous-groupe H de $GL(n, \mathbb{K})$ tel que la restriction à H de l'application déterminant soit un isomorphisme entre H et $\mathbb{K}^*$. Pour tout $\lambda \in \mathbb{K}^*$, considérons la matrice

$$A_\lambda \overset{\text{déf}}{=} \begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ & & & \lambda \end{pmatrix}.$$

Il est immédiat que l'ensemble H des matrices A_λ quand λ décrit $\mathbb{K}^*$ forme un sous-groupe de $GL(n, \mathbb{K})$; et comme $\det A_\lambda = \lambda$, la restriction à H de l'application déterminant est un isomorphisme entre H et $\mathbb{K}^*$. ❑

Exercice 1.1 *Pour tout entier q de la forme p^α, avec p premier et $\alpha \in \mathbb{N}^*$, on désigne par $\mathbb{F}_q$ le corps fini de cardinal q. Vérifier que les ordres des groupes $GL(n, \mathbb{F}_q)$ et $SL(n, \mathbb{F}_q)$ sont donnés par*

$$\begin{aligned} |GL(n, \mathbb{F}_q)| &= (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}), \\ \text{et} \qquad |SL(n, \mathbb{F}_q)| &= |GL(n, \mathbb{F}_q)|/(q-1) = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})q^{n-1}. \end{aligned}$$

2 Générateurs

A l'instar du groupe symétrique $\mathbf{S}_n$, pour lequel les transpositions forment une famille génératrice particulièrement intéressante car elles ont un grand nombre de points fixes, on cherche pour $GL(E)$ des générateurs ayant le plus de points fixes possibles. Or, le plus “gros” ensemble de points fixes possibles pour un élément de $GL(E)$ différent de Id est un hyperplan. On s'intéresse donc aux éléments de $GL(E)$ qui laissent invariants tous les points d'un hyperplan de E.

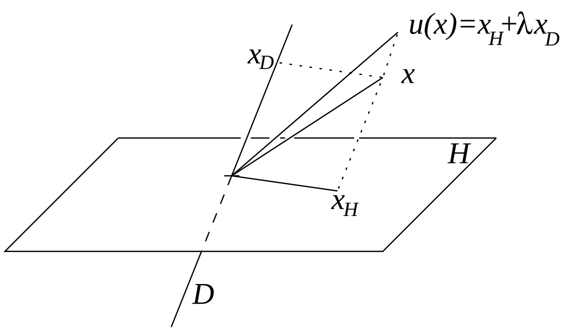
2.1 Les dilatations

Proposition 2.1 *Soit H un hyperplan de E, et $u \in GL(E)$ laissant fixes tous les points de H. Les propriétés suivantes sont équivalentes.*

1. $\det u \neq 1$,
2. *u admet une valeur propre $\lambda \neq 1$,*
3. *$\mathrm{Im}\,(u - \mathrm{Id}) \not\subset H$,*
4. *il existe $\lambda \in \mathbb{K} \setminus \{0, 1\}$, et une base de E dans laquelle la matrice de u est*

$$\begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ & & & \lambda \end{pmatrix}.$$

Preuve — laissée en exercice.



Lorsque $u \in GL(E)$ vérifie les conditions décrites dans la proposition 2.1, l'hyperplan H est le sous-espace propre associé à la valeur propre 1 (d'ordre $n-1$) de u, et le sous-espace propre associé à la valeur propre $\lambda \neq 1$ est une droite D supplémentaire de H. On dit alors que *u est une dilatation d'hyperplan H, de droite D, et de rapport λ.*

Exercice 2.1 *Prouver que deux dilatations sont conjuguées si et seulement si elles ont le même rapport.*

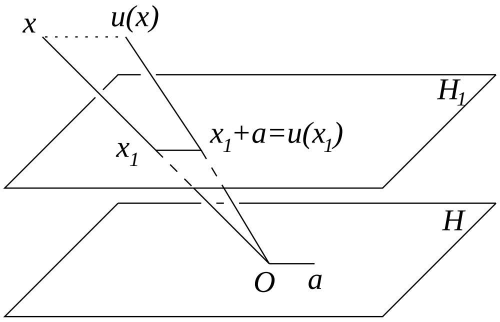
2.2 Les transvections

Proposition 2.2 *Soit H un hyperplan de E, d'équation $f(x) = 0$ où $f \in E^*$, et $u \in GL(E)$, $u \neq Id$, laissant fixes tous les points de H. Les propriétés suivantes sont équivalentes.*

1. $\det u = 1$ *(i.e. $u \in SL(E)$),*
2. *u n'est pas diagonalisable,*
3. *$\mathrm{Im}\,(u - Id)$ est une droite $D \subset H$,*
4. *il existe $a \in H$ tel que pour tout $x \in E$, $u(x) = x + f(x)a$*
5. *il existe une base de E dans laquelle la matrice de u est*

$$\begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & 1 \\ & & & 1 \end{pmatrix}.$$

Preuve — laissée en exercice.



Si $u \in GL(E)$ vérifie les conditions décrites dans la proposition 2.2, on dit que *u est une transvection d'hyperplan H et de droite D*. Notons que $D = \mathrm{Im}\,(u - \mathrm{Id})$ est la droite vectorielle engendrée par a, et que dans l'hyperplan affine H_1 parallèle à H, d'équation $f(x) = 1$, u coïncide avec la translation $x \longmapsto x + a$. Attention, la donnée de l'hyperplan H et de la droite D ne suffit pas à déterminer u, car f étant fixée, chaque choix d'un vecteur non nul $a \in D$ donne une transvection d'hyperplan H et de droite D. Aussi, la donnée de la seule transvection u ne détermine a qu'à un scalaire près (car la forme linéaire f n'est elle-même déterminée qu'à un scalaire près par la donnée de H). Dans la suite, on notera $\tau_{f,a}$ la transvection définie par $\tau_{f,a}(x) \stackrel{\text{déf}}{=} x + f(x)a$, où f est une forme linéaire non nulle sur E telle que $f(a) = 0$.

Exercice 2.2 *Soit H un hyperplan de E. On considère*

$$F(H) \overset{\text{déf}}{=} \left\{u \in GL(E) \Big/ u_{|_H} = Id_H\right\}, \quad \text{et } T(H) \overset{\text{déf}}{=} F(H) \cap SL(E).$$

Montrer que ce sont des sous-groupes de $GL(E)$, et préciser leurs éléments. Prouver que $T(H)$ est un sous-groupe distingué de $F(H)$, isomorphe au groupe additif H. Montrer que $F(H)$ est isomorphe à un produit semi-direct $H \rtimes \mathbb{K}^*$.

2.3 Conjugaison des transvections

Exercice 2.3 *Soit τ une transvection d'hyperplan H et de droite D. Prouver que, pour tout $u \in GL(E)$, $u\tau u^{-1}$ est une transvection d'hyperplan $u(H)$ et de droite $u(D)$.*

Proposition 2.3 *Deux transvections u et v sont toujours conjuguées dans $GL(E)$. Si $n \geq 3$, elles sont aussi conjuguées dans $SL(E)$.*

Preuve — D'après la propriété 5 de la proposition 2.2, si u et v sont deux transvections il existe deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E telles que la matrice de u dans $\mathscr{B}$ et celle de v dans $\mathscr{B}'$ soient égales à

$$\begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & 1 \\ & & & 1 \end{pmatrix}.$$

On en déduit immédiatement que u et v sont conjuguées dans $GL(E)$, *i.e.* il existe $w \in GL(E)$ vérifiant $v = wuw^{-1}$.

Supposons maintenant $n \geq 3$, et montrons que u et v sont aussi conjuguées dans $SL(E)$. Il suffit pour cela de trouver $s \in GL(E)$ tel que $sw \in SL(E)$ (*i.e.* $\det s = 1/\lambda$, où $\lambda = \det w$), et $v = svs^{-1}$ (car on aura alors $v = (sw)u(sw)^{-1}$). Il est immédiat que s de matrice diagonale

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & \lambda & & \\ & 0 & & & 1/\lambda & \\ & & & & & 1/\lambda \end{pmatrix}$$

dans la base $\mathscr{B}'$ convient. ❑

Dans le cas $n = 2$, l'argument employé ci-dessus n'est plus utilisable. La classe de conjugaison d'une transvection dans $SL(E)$ dépend alors du corps $\mathbb{K}$ considéré.

Proposition 2.4 *Soit E de dimension 2 sur $\mathbb{K}$, et $\mathscr{B} = (e_1, e_2)$ une base fixée de E, permettant d'identifier chaque $u \in GL(E)$ à sa matrice dans cette base. Pour $\lambda \in \mathbb{K}^*$, les transvections*

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad v = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

sont conjuguées dans $SL(E)$ si et seulement si λ est un carré dans le corps $\mathbb{K}$.

Preuve — S'il existe $w = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ dans $SL(E)$ vérifiant $v = wuw^{-1}$, on a alors

$$vw = \begin{pmatrix} \alpha+\gamma\lambda & \beta+\delta\lambda \\ \gamma & \delta \end{pmatrix} = wu = \begin{pmatrix} \alpha & \alpha+\beta \\ \gamma & \delta \end{pmatrix},$$

d'où $\gamma = 0$ puisque $\lambda \neq 0$, puis $\delta = 1/\alpha$ car on a supposé $w \in SL(E)$. Comme on a aussi $\alpha = \delta\lambda$, on en déduit $\lambda = \alpha^2$.

Réciproquement, s'il existe $\alpha \in \mathbb{K}$ tel que $\lambda = \alpha^2$, alors $w = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$ est dans $SL(E)$ et vérifie $v = wuw^{-1}$. ❏

2.4 Générateurs de $SL(E)$ et $GL(E)$

Théorème 2.5 *Les transvections engendrent $SL(E)$; les transvections et les dilatations engendrent $GL(E)$.*

Preuve — Remarquons tout d'abord que la seconde partie du théorème est une conséquence immédiate de la première. En effet, tout $u \in GL(E)$ s'écrit sous la forme $u = vs$ où v est une dilatation de rapport $\det u$, et $s \in SL(E)$. Il reste donc à montrer que tout élément de $SL(E)$ peut s'écrire comme un produit de transvections, ce que l'on va montrer par récurrence sur la dimension n de E. Lorsque $n = 1$, c'est immédiat puisque dans ce cas, $SL(E) = \{\mathrm{Id}\}$. Puis, supposant que le théorème est démontré en dimension inférieure ou égale à $n-1$ ($n \geq 2$), on s'y ramène en utilisant le lemme qui suit.

Lemme 2.6 *Soit $u \in GL(E)$, H un hyperplan de E et $x_0 \in E \setminus H$. Alors il existe un produit s de transvections de E tel que $su(x_0) = x_0$ et $su(H) = H$.*

Admettant ce lemme provisoirement, on voit que tout $u \in GL(E)$ s'écrit sous la forme $u = s^{-1}v$, où s^{-1} est un produit de transvections, et v vérifie $v(x_0) = x_0$, $v(H) = H$. Si de plus u est dans $SL(E)$, v est aussi dans $SL(E)$ et sa restriction $\bar{v}$ à H est alors dans $SL(H)$ [...]. Par hypothèse de récurrence $\bar{v}$ s'écrit dans $SL(H)$ comme un produit de transvections $\bar{\tau}_1 \cdots \bar{\tau}_k$. Or, il est facile de voir que si $\bar{\tau}_j$ est une transvection dans $SL(H)$, d'hyperplan $\bar{H}_j$, alors $\bar{\tau}_j$ est la restriction à H d'une transvection τ_j d'hyperplan $\bar{H}_j \oplus \mathbb{K}x_0$ (en particulier, $\tau_j(x_0) = x_0$). On en déduit que $v = \tau_1 \cdots \tau_k$, puis que u est un produit de transvections.

Pour établir le lemme 2.6, on a besoin de deux autres résultats intermédiaires.

Lemme 2.7 *Soient x_0 et x_1 deux éléments non nuls de E. Alors il existe un produit s_1 d'au plus deux transvections tel que $s_1(x_1) = x_0$.*

Preuve — Supposons tout d'abord x_0 et x_1 non colinéaires, et soit $a \overset{\text{déf}}{=} x_0 - x_1$. On peut alors trouver une forme linéaire f sur E qui vérifie $f(a) = 0$ et $f(x_1) = 1$, d'où $\tau_{f,a}(x_1) = x_1 + a = x_0$. Si maintenant x_0 et x_1 sont colinéaires, on prend un troisième point x qui ne leur est pas colinéaire (ce qui est possible car $n \geq 2$), on trouve alors par l'argument précédent une première transvection qui envoie x_1 sur x, puis une seconde qui envoie x sur x_0.

Lemme 2.8 *Soient H et H_1 deux hyperplans distincts de E, et x_0 un point de E n'appartenant pas à $H \cup H_1$. Alors il existe une transvection τ telle que $\tau(x_0) = x_0$, et $\tau(H_1) = H$.*

Preuve — Définissons l'hyperplan $\bar{H} \stackrel{\text{déf}}{=} (H \cap H_1) \oplus \mathbb{K}x_0$, et cherchons la transvection τ d'hyperplan $\bar{H}$. Prenons $h \in H \setminus H_1$ (alors $h \notin \bar{H}$ [...]) ; comme $E = H_1 \oplus \mathbb{K}x_0$, il existe $h_1 \in H_1$ et $\lambda \in \mathbb{K}$ tels que $h = h_1 + \lambda x_0$. En posant $a \stackrel{\text{déf}}{=} \lambda x_0$, et en prenant une forme linéaire f telle que $\bar{H} = \operatorname{Ker} f$, et $f(h_1) = 1$ (ce qui est toujours possible car $h_1 \notin \bar{H}$), on a alors $\tau_{f,a}(h_1) = h$, puis $\tau_{f,a}(H_1) = H$.

Preuve du lemme 2.6 — Appliquons le lemme 2.7 avec $x_1 \stackrel{\text{déf}}{=} u(x_0)$: on obtient un produit s_1 de transvections tel que $s_1u(x_0) = x_0$. Soit ensuite $H_1 \stackrel{\text{déf}}{=} s_1u(H)$. Si $H_1 = H$, c'est terminé ; sinon, on peut appliquer le lemme 2.8 en remarquant que, puisque x_0 est fixe par s_1u et n'appartient pas à H, x_0 ne peut pas non plus appartenir à H_1. Le lemme 2.8 fournit alors une transvection τ qui vérifie $\tau s_1 u(x_0) = x_0$, et $\tau s_1 u(H) = H$. ❑

3 Centre, groupe projectif linéaire

3.1 Les homothéties

Soit $\lambda \in \mathbb{K}^*$. L'*homothétie de rapport* λ est l'élément h_λ de $GL(E)$ défini par

$$\forall x \in E, \quad h_\lambda(x) \stackrel{\text{déf}}{=} \lambda x.$$

Il est immédiat que l'ensemble de ces homothéties quand λ décrit $\mathbb{K}^*$ est un sous-groupe de $GL(E)$, isomorphe au groupe multiplicatif des scalaires non nuls, et que ce sous-groupe est inclus dans le centre $Z(GL(E))$. On veut maintenant établir qu'il n'y a pas d'autre élément dans $Z(GL(E))$.

Lemme 3.1 *Soit $u \in GL(E)$ laissant globalement invariante toute droite vectorielle. Alors u est une homothétie.*

Preuve — Prenons $x \neq 0$ dans E. Par hypothèse, il existe $\lambda \in \mathbb{K}^*$ tel que $u(x) = \lambda x$. Puis, pour tout $y \in E$, deux cas se présentent : ou bien y est colinéaire à x, et on a aussi $u(y) = \lambda y$, ou bien y n'est pas colinéaire à x. Dans ce second cas, il existe $\mu \in \mathbb{K}^*$ tel que $u(y) = \mu y$, et $\nu \in \mathbb{K}^*$ tel que $u(x+y) = \nu(x+y)$. Mais la famille (x, y) étant libre, de l'égalité

$$u(x+y) \;=\; \nu(x+y) \;=\; u(x) + u(y) \;=\; \lambda x + \mu y$$

on déduit $\mu = \nu = \lambda$. Ainsi, u est l'homothétie de rapport λ. ❑

Exercice 3.1 *Soit $r \in \{1, \ldots, n-1\}$, et $u \in GL(E)$ laissant globalement invariant tout sous-espace vectoriel de dimension r. Montrer que u est une homothétie.*

Théorème 3.2 *Le centre de $GL(E)$ est l'ensemble des homothéties ; le centre de $SL(E)$ est l'ensemble des homothéties dont le rapport λ vérifie $\lambda^n = 1$.*

Preuve — Il suffit de vérifier que si u commute avec tous les éléments de $SL(E)$, alors u est une homothétie. Or, d'après l'exercice 2.3, si τ est une transvection de droite D, $u\tau u^{-1}$ est une transvection de droite $u(D)$. Mais si u commute avec τ, $\tau = u\tau u^{-1}$, et donc $D = u(D)$. Ainsi, si u commute avec toutes les transvections, on a $u(D) = D$ pour toute droite vectorielle D, et le lemme 3.1 prouve alors que u est une homothétie. ❑

Dans la suite, on notera Z le centre de $GL(E)$.

3.2 Le groupe projectif linéaire

Soit $P(E)$ l'ensemble des droites vectorielles de E, également appelé *l'espace projectif associé à E*. Le groupe $GL(E)$ opère de façon naturelle sur $P(E)$ [...] ; autrement dit, on a un morphisme naturel φ de $GL(E)$ dans le groupe symétrique $\mathbf{S}(P(E))$. Le lemme 3.1 dit exactement que le noyau de ce morphisme est le sous-groupe Z constitué des homothéties de E. On a donc une opération *fidèle* du groupe quotient $GL(E)/Z$ sur $P(E)$. Le groupe quotient $GL(E)/Z$ est appelé le *groupe projectif linéaire de E*, et noté $PGL(E)$. Ce groupe est, par ce qui précède, isomorphe à un sous-groupe de $\mathbf{S}(P(E))$: l'image du morphisme φ. On note $PGL(n, \mathbb{K})$ le groupe matriciel correspondant.

On note aussi $PSL(E)$ le quotient de $SL(E)$ par son centre $Z \cap SL(E)$, et $PSL(n, \mathbb{K})$ le groupe matriciel correspondant. Comme $Z \cap SL(E)$ est aussi le noyau de $\varphi|_{SL(E)}$, (morphisme de $SL(E)$ dans $\mathbf{S}(P(E))$ correspondant à l'opération par restriction de $SL(E)$ sur $P(E)$), le groupe $PSL(E)$ opère lui aussi fidèlement sur $P(E)$, et il est aussi isomorphe à un sous-groupe de $\mathbf{S}(P(E))$: $\operatorname{Im} \varphi|_{SL(E)}$. Ce dernier étant un sous-groupe de $\operatorname{Im} \varphi$, on en déduit l'existence d'une injection "naturelle" de $PSL(E)$ dans $PGL(E)$, décrite plus précisément ci-après.

Pour tout $u \in GL(E)$, notons $\dot{u}$ la classe de u dans le groupe quotient $PGL(E)$; si de plus $u \in SL(E)$, notons aussi $\bar{u}$ la classe de u dans le groupe quotient $PSL(E)$. Prenons u et v dans $SL(E)$ tels que $\bar{u} = \bar{v}$. C'est donc qu'il existe $h \in Z \cap SL(E)$ tel que $u = vh$. En particulier $h \in Z$, et donc on a aussi $\dot{u} = \dot{v}$. Cette remarque permet de définir un morphisme "naturel" de $PSL(E)$ dans $PGL(E)$: l'application $\bar{u} \longmapsto \dot{u}$. Il est immédiat que ce morphisme est injectif [...]. Voyons quelle est son image. Pour $u \in GL(E)$, $\dot{u}$ est l'image d'une classe $\bar{v}$ de $PSL(E)$ si et seulement si il existe $v \in SL(E)$ et $h \in Z$ tels que $u = vh$; mais ceci équivaut à l'existence d'un $\lambda \in \mathbb{K}^*$ (le rapport de l'homothétie h) tel que $\det u = \lambda^n$, soit encore à $\det u \in \mathbb{K}^{*n}$, où $\mathbb{K}^{*n}$ est le sous-groupe multiplicatif de $\mathbb{K}^*$ défini par

$$\mathbb{K}^{*n} \stackrel{\text{déf}}{=} \{\mu \in \mathbb{K}^* \ / \ \exists \lambda \in \mathbb{K}^*, \ \mu = \lambda^n \} .$$

Remarquons par ailleurs que si u et v dans $GL(E)$ vérifient $\dot{u} = \dot{v}$, alors il existe $\mu \in \mathbb{K}^{*n}$ tel que $\det u = \mu \det v$. Ainsi, on peut définir le morphisme $\bar{\det}$ de $PGL(E)$ sur le groupe quotient $\mathbb{K}^*/\mathbb{K}^{*n}$, qui à $\dot{u}$ associe la classe du déterminant de u. Ce qui précède dit que l'image de $PSL(E)$ dans $PGL(E)$ par l'injection naturelle est précisément le noyau de $\bar{\det}$. En résumé, on a une suite exacte

$$1 \longrightarrow PSL(E) \longrightarrow PGL(E) \xrightarrow{\bar{\det}} \mathbb{K}^*/\mathbb{K}^{*n} \longrightarrow 1.$$

En particulier, lorsque le corps $\mathbb{K}$ est algébriquement clos on a $\mathbb{K}^{*n} = \mathbb{K}^*$, et les groupes $PSL(E)$ et $PGL(E)$ sont isomorphes.

Le théorème qui suit est admis ici ; on en trouve une démonstration dans [3].

Théorème 3.3 *Le groupe $PSL(E)$ est simple sauf dans les deux cas ($n = 2$, $\mathbb{K} = \mathbb{F}_2$) et ($n = 2$, $\mathbb{K} = \mathbb{F}_3$).*

Voici en exercice l'étude des deux cas particuliers du théorème précédent.

Exercice 3.2 *1 – Montrer que si $\mathbb{K}$ est le corps fini $\mathbb{F}_q$, alors*

$$|P(E)| \ = \ 1 + q + \cdots + q^{n-1},$$

$$\text{et} \qquad |PGL(n,\mathbb{F}_q)| = |SL(n,\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}.$$

2 – Montrer que les groupes $GL(n,\mathbb{F}_2)$, $SL(n,\mathbb{F}_2)$, $PGL(n,\mathbb{F}_2)$ et $PSL(n,\mathbb{F}_2)$ sont tous isomorphes. Quel est leur cardinal ?

3 – Montrer que $GL(2,\mathbb{F}_2)$ est isomorphe à $\mathbf{S}_3$; en déduire que $PSL(2,\mathbb{F}_2)$ n'est pas simple.

4 – Montrer que $PGL(2,\mathbb{F}_3)$ est isomorphe à $\mathbf{S}_4$, et que $PSL(2,\mathbb{F}_3)$ est isomorphe au groupe alterné A_4 (indication : A_4 est le seul sous-groupe d'indice 2 de $\mathbf{S}_4$ [...]). En déduire que $PSL(2,\mathbb{F}_3)$ n'est pas simple.

4 Groupe dérivé

Intéressons-nous maintenant au groupe dérivé $D(GL(E))$, c'est-à-dire au sous-groupe engendré par les commutateurs $uvu^{-1}v^{-1}$. Il est clair que tout commutateur est de déterminant 1, ainsi on a toujours $D(GL(E)) \subset SL(E)$. Le but de ce qui suit est de voir qu'en général l'inclusion réciproque est vraie, sauf dans un cas particulier à préciser.

Pour obtenir l'inclusion $SL(E) \subset D(GL(E))$, il suffit de montrer que toute transvection est un commutateur, puique les transvections engendrent $SL(E)$. Or, comme toutes les transvections sont conjuguées dans $GL(E)$, il suffit de vérifier que l'une d'entre elles est un commutateur. En effet, si on a prouvé qu'une transvection τ s'écrit $uvu^{-1}v^{-1}$, et si τ' est une autre tranvection, on sait qu'il existe $g \in GL(E)$ tel que $\tau' = i_g(\tau) = i_g(u)i_g(v)i_g(u)^{-1}i_g(v)^{-1}$, (où i_g est l'automorphisme intérieur $w \longmapsto gwg^{-1}$), donc τ' est aussi un commutateur. Remarquons même que si u et v sont dans $SL(E)$, sous-groupe normal de $GL(E)$, on aura aussi $i_g(u)$ et $i_g(v)$ dans $SL(E)$, ce qui donnera finalement $SL(E) = D(SL(E))$.

Voyons tout d'abord un cas assez simple : celui où le corps $\mathbb{K}$ est de caractéristique différente de 2. Alors, si τ est une transvection quelconque, τ^2 est aussi une transvection [...], qui lui est donc conjuguée : il existe $g \in GL(E)$ tel que $\tau^2 = g\tau g^{-1}$, *i.e.* $\tau = g\tau g^{-1}\tau^{-1}$: τ est un commutateur de $GL(E)$. Si de plus $n \geq 3$, on peut même prendre $g \in SL(E)$ d'après la proposition 2.3, et τ est un commutateur de $SL(E)$.

Si le corps $\mathbb{K}$ est de caractéristique 2, mais différent de $\mathbb{F}_2$, il est possible de trouver $\lambda \in \mathbb{K}^*$ tel que $\lambda^2 \neq 1$. On considère alors les éléments suivants de $SL(E)$ (identifiés à leur matrice dans une base fixée) :

$$u \stackrel{\text{déf}}{=} \begin{pmatrix} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & 1 \\ & & & 1 \end{pmatrix} \quad ; \quad v \stackrel{\text{déf}}{=} \begin{pmatrix} 1 & & & 0 & \\ & \ddots & & & \\ & & 1 & & \\ 0 & & & \lambda & \\ & & & & \lambda^{-1} \end{pmatrix}.$$

Alors

$$\tau \stackrel{\text{déf}}{=} uvu^{-1}v^{-1} = \begin{pmatrix} 1 & & & 0 & \\ & \ddots & & & \\ & & 1 & & \\ 0 & & & 1 & \lambda^2-1 \\ & & & & 1 \end{pmatrix}$$

est une transvection, qui est un commutateur de $SL(E)$. On a donc encore dans ce cas $SL(E) = D(SL(E))$.

Enfin, pour $\mathbb{K} = \mathbb{F}_2$ et en dimension $n \geq 3$, on vérifie que la transvection

$$\tau \stackrel{\text{déf}}{=} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

s'écrit $\tau = uvu^{-1}v^{-1}$, où u et v sont définis par

$$u \stackrel{\text{déf}}{=} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad ; \quad v \stackrel{\text{déf}}{=} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Remarquons que lorsque le corps $\mathbb{K}$ est $\mathbb{F}_2$, $GL(E) = SL(E)$; ainsi u et v sont dans $SL(E)$ ici.

Dans le cas $(\mathbb{K} = \mathbb{F}_2, n = 2)$, $GL(E) = SL(E)$ est isomorphe à $\mathbf{S}_3$, et $D(GL(E))$ au groupe alterné A_3. On a donc $D(GL(E)) \subsetneq GL(E) = SL(E)$. En conclusion de ce qui précède, on a donc le théorème suivant.

Théorème 4.1 *On a $D(GL(E)) = SL(E)$ sauf dans le cas $(\mathbb{K} = \mathbb{F}_2, n = 2)$.*

De plus, on a pu voir que dans la plupart des cas, $SL(E)$ est même égal à son propre sous-groupe dérivé. En fait, il n'y a que deux cas dans lesquels ce n'est pas vrai.

Théorème 4.2 *On a $D(SL(E)) = SL(E)$ sauf dans les deux cas $(\mathbb{K} = \mathbb{F}_2, n = 2)$ et $(\mathbb{K} = \mathbb{F}_3, n = 2)$.*

Exercice 4.1 *Achever la preuve du théorème 4.2*

5 Groupe affine

5.1 Structure du groupe affine

Pour tout $a \in E$, on appelle *translation de vecteur a* l'application $t_a : E \longrightarrow E$ définie par $t_a(x) \stackrel{\text{déf}}{=} x + a$. Il est immédiat que l'ensemble $T(E)$ des translations t_a quand a décrit E forme un sous-groupe du groupe symétrique $\mathbf{S}(E)$, isomorphe au groupe additif $(E, +)$. En particulier, $T(E)$ est un groupe abélien. Par ailleurs, la seule translation qui soit aussi dans $GL(E)$ est la translation de vecteur nul, c'est-à-dire Id.

Proposition 5.1 *Le sous-groupe du groupe symétrique $\mathbf{S}(E)$ engendré par $T(E)$ et $GL(E)$ est constitué des applications f de la forme $t_a \circ u$, où $a \in E$ et $u \in GL(E)$.*

Preuve — Il suffit de vérifier que l'ensemble des f de la forme $t_a \circ u$ est un groupe pour la loi de composition des applications. Soient a et b dans E, u et v dans $GL(E)$. Il est facile de vérifier que

$$u \circ t_b \circ u^{-1} \;=\; t_{u(b)}.$$

On en déduit

$$(t_a \circ u) \circ (t_b \circ v) \;=\; t_a \circ (u \circ t_b \circ u^{-1}) \circ u \circ v \;=\; (t_a \circ t_{u(b)}) \circ (u \circ v). \tag{1}$$

Puis en appliquant ce qui précède,

$$(t_a \circ u)^{-1} \;=\; u^{-1} \circ t_{-a} \;=\; t_{u^{-1}(-a)} \circ u^{-1}. \tag{2}$$

La stabilité par composition et par passage à l'inverse étant établie, on a le résultat annoncé. ❏

Le groupe engendré par $T(E)$ et $GL(E)$ s'appelle le *groupe affine de* E, et se note $GA(E)$. Une application f de la forme $t_a \circ u$, où $a \in E$ et $u \in GL(E)$, s'appelle une *bijection affine de* E. Il est très facile de voir que a et u sont déterminés de manière unique par la donnée de $f \in GA(E)$. En effet, $a = f(0)$ et $u = t_{-a} \circ f$. On appelle u la *partie linéaire de* $f = t_a \circ u$.

Proposition 5.2 *L'application Λ qui à une bijection affine $f = t_a \circ u$ associe sa partie linéaire u est un morphisme surjectif du groupe affine $GA(E)$ sur $GL(E)$. Son noyau est le groupe des translations $T(E)$.*

Preuve — Immédiat en utilisant (1) et (2). ❏

On en déduit que $T(E)$ est un sous-groupe distingué de $GA(E)$, et que le groupe quotient $GA(E)/T(E)$ est isomorphe à $GL(E)$. On a donc une suite exacte

$$1 \longrightarrow T(E) \longrightarrow GA(E) \xrightarrow{\Lambda} GL(E) \longrightarrow 1.$$

Il est immédiat ici que Λ admet un relèvement, puisque $GL(E)$ est lui-même un sous-groupe de $GA(E)$, avec $\forall u \in GL(E),\ \Lambda(u) = u$. Ainsi, $GA(E)$ peut être vu comme un produit semi-direct de $T(E)$ (donc de E) par $GL(E)$. En fait, on explicite facilement ce produit semi-direct à l'aide de (1).

Proposition 5.3 *Le groupe affine $GA(E)$ est isomorphe au produit semi-direct $E \rtimes GL(E)$ dont la loi est donnée par*

$$(a, u).(b, v) \;=\; (a + u(b), u \circ v).$$

5.2 Quelques exemples

Les homothéties affines

Soit $\lambda \in \mathbb{K}^*$, $\lambda \neq 1$ et $c \in E$. On appelle *homothétie affine de rapport λ et de centre c* l'application $h_{\lambda,c}$ de E dans E définie par $h_{\lambda,c}(x) \stackrel{\text{déf}}{=} c + \lambda(x - c)$.

Exercice 5.1 *Vérifier que l'ensemble des homothéties affines $h_{\lambda,c}$ quand λ décrit $\mathbb{K} \setminus \{0,1\}$ et c décrit E coïncide avec l'ensemble des $f \in GA(E)$ dont la partie linéaire est une homothétie différente de Id.*

L'ensemble $HA(E)$ des homothéties affines ne constitue pas un sous-groupe de $GA(E)$, puisqu'une translation n'est jamais une homothétie affine ; or le produit de deux homothéties affines de rapports inverses l'un de l'autre est une translation [...].

Proposition 5.4 *Le sous-groupe de $GA(E)$ engendré par les homothéties affines est constitué des homothéties affines et des translations.*

Preuve — Laissée en exercice.

Le sous-groupe $D(E) \stackrel{\text{déf}}{=} HA(E) \cup T(E)$ engendré par les homothéties affines est appelé *groupe des homothéties-translations.* Attention ! Certains auteurs le nomment parfois le *groupe des dilatations de E*, mais ici le terme *dilatation* n'a pas le même sens qu'au paragraphe 2.1...

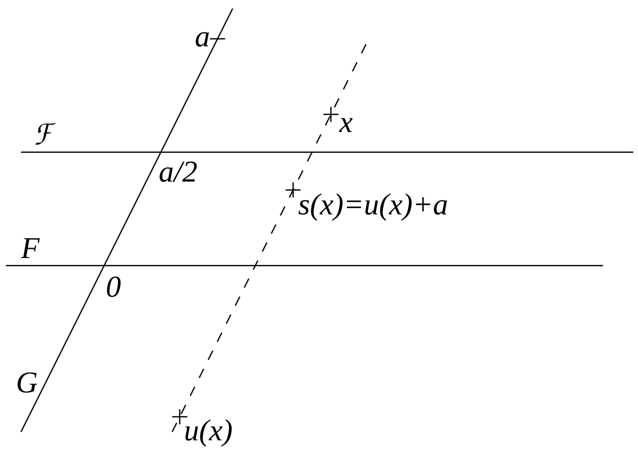
Ce sous-groupe est distingué dans $GA(E)$, puisqu'il s'écrit $D(E) = \Lambda^{-1}(Z)$, où Z est le centre de $GL(E)$.

Exercice 5.2 *Vérifier que $T(E) \lhd D(E)$, et que le groupe quotient $D(E)/T(E)$ est isomorphe au groupe multiplicatif $\mathbb{K}^*$. Montrer que $D(E)$ est isomorphe à un produit semi-direct $E \rtimes \mathbb{K}^*$.*

Les symétries affines

On suppose ici que le corps $\mathbb{K}$ n'est pas de caractéristique 2. On dit que $s \in GA(E)$ est une *symétrie affine* si s est involutive, c'est-à-dire si $s \circ s = \mathrm{Id}$.

Considérons une symétrie affine $s = t_a \circ u$. Alors u vérifie aussi $u^2 = \mathrm{Id}$, et il est classique que si F et G sont les sous-espaces propres définis par $F \stackrel{\text{déf}}{=} \mathrm{Ker}\,(u - \mathrm{Id})$ et $G \stackrel{\text{déf}}{=} \mathrm{Ker}\,(u + \mathrm{Id})$, alors $E = F \oplus G$. Écrivant $x \in E$ sous la forme $x_F + x_G$ où $x_F \in F$ et $x_G \in G$, on a alors $u(x) = x_F - x_G$, et $s(x) = a + x_F - x_G$. Le fait que $s \circ s(a) = a$ donne facilement $a \in G$, et l'ensemble des points fixes de s est constitué des $x \in E$ tels que $x_G = a/2$. C'est donc le sous-espace affine $\mathscr{F} \stackrel{\text{déf}}{=} F + a/2$. On appelle alors s la *symétrie par rapport à $\mathscr{F}$, parallèlement à la direction de G.*



Dans la cas particulier où F est réduit à $\{0\}$, ce qui correspond au cas où $u = -\mathrm{Id}$, on retrouve une homothétie affine de rapport -1, et de centre $a/2$. On l'appelle la *symétrie centrale de centre $a/2$.*

Remarque. Pour que $f = t_a \circ u$ soit une symétrie affine, il ne suffit pas que $u^2 = \mathrm{Id}$. En effet, si $u \in GL(E)$ est une involution et $a \notin \mathrm{Ker}\,(u + \mathrm{Id})$, $t_a \circ u$ n'a pas de point fixe...

Références

[1] Alain Bouvier et Denis Richard. *Groupes – observation, théorie, pratique.* Hermann, 1994.

[2] Encyclopædia Universalis. *Dictionnaire des Mathématiques – Algèbre, Analyse, Géométrie.* Albin Michel, 1997.

[3] Daniel PERRIN. *Cours d'Algèbre.* Ellipses, 1996.

[4] J.J. ROTMAN. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer-Verlag, 1995.