QUELQUES EXEMPLES DE SOUS-GROUPES DE $\mathbf{GL}_n$

par

Yves Laszlo

Table des matières

1. Introduction

Le but de ces notes est de donner une idée de la complexité d'un groupe d'apparence aussi anodine que $\mathbf{GL}_2(\mathbf{R})$. En bref, ce n'est pas parce qu'on a un groupe de matrices (2,2) qu'on peut en dire grand chose en général. On va donner des résultats, bien classiques, sur les sous-groupes finis de $\mathbf{GL}_n$, les sous-groupes fermés, résolubles, libres. Pour comprendre l'importance de ces deux dernières notion, il peut être bon d'avoir en tête l'alternative de Tits (1972) : un sous-groupe de type fini de $\mathbf{GL}_n(\mathbf{R})$ qui ne contient pas de sous-groupe libre à deux générateurs possède un sous-groupe normal résoluble d'indice fini ([**11**])!!! Ce résultat serait difficilement exposable en 3 heures à ce niveau, mais serait un superbe sujet de mémoire!!!

Le lecteur qui aura suivi le cours de théorie de Galois saura l'importance de la notion de sous-groupe normal (ou distingué). Pour les autres, disons que H est normal si et seulement si l'ensemble quotient G/H est muni d'une

structure de groupe compatible à celle de G. Si en général, G ne s'identifie pas au produit $H \times G/H$, il n'en demeure pas moins qu'on peut espérer tirer des renseignements sur G des deux groupes plus petits H et G/H. En ce sens, les groupes sans sous-groupes normaux -appelés groupes simples- sont les briques élémentaires de la théorie des groupes.

On n'a en aucune manière chercher à faire un cours au sens strict du terme, se permettant d'admettre ça et là des résultats peu surprenants ou de preuve fastidieuse, mais plutôt de donner un aperçu de la richesse des résultats et des techniques mises en jeu.

2. Sous-groupes finis

Tout sous groupe fini se plonge dans $\mathbf{GL}_n(\mathbf{Z})$ avec $n = \mathrm{card}(G)$ comme on le voit en faisant opérer G sur les fonctions sur G à valeurs entières. Essayons de préciser ce qu'on peut dire sur les sous-groupes finis de $\mathbf{GL}_n(\mathbf{R}), \mathbf{GL}_n(\mathbf{C})$.

2.1. Sous-groupes abéliens finis. —

Proposition 2.1.1. — *Les sous groupes abéliens finis de* $\mathbf{GL}_n(\mathbf{C})$ *sont isomorphes à des produits de* k *groupes cycliques* $\mathbf{Z}/m\mathbf{Z}$ *avec* $k \leq n$.

Preuve : on observe que les matrices d'un tel groupe commutent et sont diagonalisables (d'après le théorème de Lagrange, elles sont annulées par le polynômes $X^{|G|} - 1$, qui est à racines simples dans $\mathbf{C}$). Ceci permet de les diagonaliser dans une même base, (ce qui est l'objet d'un exercice classique de taupe) prouvant que G est isomorphe à un sous-groupe de $(\mathbf{Z}/|G|\mathbf{Z})^n$. Si $|G| = p$ est premier, alors G est un $\mathbf{F}_p$-sous-espace vectoriel de $\mathbf{F}_p^n$ et on a terminé. Dans le cas général, on prouve également qu'un tel sous-groupe est isomorphe à un produit de $k \leq n$ groupes cycliques (utiliser qu'une matrice entière est équivalente (sous l'action de $\mathbf{GL}_n(\mathbf{Z}) \times \mathbf{GL}_n(\mathbf{Z})$) à une matrice diagonale).■

Exercice 2.1.2. — *Soit* m *un entier impair. Quel est le cardinal maximal d'un sous-groupe abélien de* $\mathbf{GL}_n(\mathbf{R})$ *annulé par* m *?*

Corollaire 2.1.3. — *Si les groupes* $\mathbf{GL}_n(\mathbf{C})$ *et* $\mathbf{GL}_m(\mathbf{C})$ *sont isomorphes, alors* $n = m$.

Preuve : Observer que $(\mathbf{Z}/2\mathbf{Z})^n$ est le plus grand sous-groupe de $\mathbf{GL}_n(\mathbf{C})$ isomorphe à une puissance de $\mathbf{Z}/2\mathbf{Z}$. ■

On peut par ce genre de méthodes que $\mathbf{GL}_n(k) \xrightarrow{\sim} \mathbf{GL}_m(k')$ si et seulement si $n = m$ et $k \xrightarrow{\sim} k'$, résultat dû à Van der Warden et Schreier, généralisé au cas des corps non commutatifs par Dieudonné. Sur ce sujet, on pourra aller regarder [**9**] et pour une généralisation considérable, mais nettement plus chère, [**1**] .

2.2. Sous-groupes d'exposant fini. — On peut se demander si la théorie des sous-groupes d'exposant donné m, *ie* dont tes les éléments sont d'ordre $\leq m$, est plus riche que celle des sous-groupes finis. Il n'en est rien.

Proposition 2.2.1 **(Burnside)**. — *Soit G un sous-groupe d'exposant m de $\mathbf{GL}_n(\mathbf{C})$. Alors G est fini.*

Preuve : On a déjà observé que les matrices $g \in G$ étaient diagonalisables de valeurs propres des racines m-ièmes de 1. En particulier, l'ensemble T des traces des éléments de G est fini. Soit $g_1, \cdots, g_d$ une famille génératrice de l'espace vectoriel engendré par G dans $M_n(\mathbf{C})$ et considérons l'application

$$t : \begin{array}{ccc} G & \to & T^d \\ g & \mapsto & \mathrm{Tr}(gg_i) \end{array}$$

Comme T est fini, il suffit de montrer que t est injectif. Si $t(h) = t(h')$, par linéarité de la trace, on $\mathrm{Tr}(hg) = \mathrm{Tr}(h'g)$ pour tout $g \in G$. Avec $g = h^{-1}$, on obtient $n = \mathrm{Tr}(\mathrm{Id}) = \mathrm{Tr}(h'h^{-1})$. Comme $h'h^{-1} \in G$, sa trace est une somme de n racines de l'unité. Cette somme étant égale à n, chacune vaut 1. Comme $h'h^{-1}$ est diagonalisable de surcroît, on a bien $h' = h$.■

Remarque 2.2.2. — *Le lecteur connaissant un minimum de géométrie algébrique donnera une démonstration plus naturelle : l'adhérence de Zariski de G est encore d'exposant fini. Un développement limité en l'identité prouve que ce groupe est de caractéristique nulle) et donc cette adhérence est finie. Remarquons que le sous groupe des matrices*

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \bar{\mathbf{F}}_p$$

est un sous groupe infini de $\mathbf{SL}_2(\bar{\mathbf{F}}_p)$ d'exposant p : on ne peut remplacer l'énoncé précédent $\mathbf{C}$ par un corps quelconque. En revanche, le résultat est encore vrai si $\mathbf{C}$ est remplacé par un corps de caractéristique nulle quelconque.

2.3. Sous groupes finis de $\mathbf{GL}_n(\mathbf{R}), n \leq 3$. — Soit G un sous-groupe fini de $\mathbf{GL}_n(\mathbf{R})$ et q une forme quadratique définie positive sur $\mathbf{R}^n$. La forme quadratique sur $\mathbf{R}^n$ q_G définie par $q_G(x) = \sum_{g \in G} q(gx)$ est euclidienne et invariante par G de sorte que G est contenu dans le groupe orthogonal euclidien $\mathbf{O}(q_H)$. Dans le cas complexe, on prendrait une forme hermitienne et on tomberait dans un groupe unitaire.

L'avantage est que ces groupes orthogonaux (unitaires) sont *compacts*, ce qui n'est pas le cas du groupe linéaire général. Donc, si on ne s'intéresse qu'à la classe de conjugaison de G, *a fortiori* à son cardinal, on peut supposer $G \subset \mathbf{O}_n(\mathbf{R})$ ($U_n(\mathbf{C})$ dans le cas complexe).

Le cas $n = 2$ est très facile. L'intersection H de G et de $\mathbf{SO}_2(\mathbf{R})$ est au pire d'indice 2. Mais alors H est un sous-groupe du groupe abélien $\mathbf{SO}_2(\mathbf{R})$. Si m est l'ordre de H, tous les rotations de H ont donc un angle $2k\pi/m, k \in \mathbf{Z}$. On déduit un isomorphisme $H \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$ et se réalise par exemple comme le groupe des rotations laissant stable un polygone régulier à m côtés. Si on H d'indice 2 et est engendré par r d'ordre m, choisissons n'importe quel $s \in G \setminus H$. Comme s est une symétrie droite, $srs = r^{-1}$ et on G est le groupe *diédral* D_m, qui se réalise comme le groupe des isométries laissant stable un polygone régulier à m côtés.

Le cas $n = 3$ est plus subtil. Cherchons simplement les cardinaux des sous-groupes finis de $\mathbf{SO}_3(\mathbf{R})$. Soit X l'ensemble des points de la sphère unité S_2 de $\mathbf{R}^3$ qui sont fixés par des éléments non triviaux de G. Soit

$$Y = \{(g, x) \in G \setminus 1 \times S_2 \text{ tels que } gx = x\}.$$

Projetant sur $G \setminus 1$, on trouve

$$\text{card}(Y) = 2(\text{card}(G) - 1)$$

(une rotation $\neq 1$ a deux points fixes sur la sphère S_2, les intersections de son axe et de la sphère).
L'image de la projection sur S_2 est visiblement X. Bien entendu G opère sur X : en effet, si x est un point fixe de $g \neq 1$, alors hx est un point fixe de $hgh^{-1} \neq 1$ si $h \in G$. On découpe alors X en orbites

$$X = \sqcup_{x \in A} \omega(x)$$

où A partie de X telle que $A \to X/G$ bijectif, *ie* on choisit un élément dans A par orbites. Au dessus de $\xi = hx \in \omega(x)$, on a les rotations non triviales fixant ξ, autrement dit

$$G_\xi = hG_x h^{-1}$$

de sorte que G_x et G_ξ ont même cardinal qu'on notera ν_x (la discussion prouve que ν_x est bien défini si $x \in X/G$). Du coup, on a aussi

$$\text{card}(Y) = \sum_{x \in X/G} \text{card}(G_x - 1)\text{card } \omega(x) = \sum_{x \in X/G} \text{card}(G_x - 1)\text{card}(G)/\nu_x.$$

On a alors

$$2(\text{card}(G) - 1) = \sum_{x \in X/G} (\nu_x - 1)\text{card}(G)/\nu_x$$

autrement dit

$$2 - 2/\text{card}(G) = \sum_{x \in X/G} (1 - 1/\nu_x).$$

Cette formule permet de classifier. Notons que $\nu_x \geq 2$ (car $x \in X$ est fixé par un élément non trivial) ce qui prouve que X/G est au plus de cardinal 3. En observant que si ν_x devient grand, la somme de droite augmente, on trouve alors les cas suivants :

	ν_1	ν_2	ν_3	card(G)	G	polyèdre
I	n	n		n	$\mathbf{Z}/n\mathbf{Z}$	μ_n
II	2	2	n	n	D_n	μ_n
III	2	3	2	12	A_4	tétraèdre
IV	2	3	4	24	S_4	cube (octaèdre)
IV	2	3	5	60	A_5	dodécaèdre (icosaèdre)

La colonne polyèdre indique qu'on peut obtenir ces groupes comme des groupes d'isométrie laissant stable une figure. Dans le cas I, on a les n rotations laissant stables un polygone régulier à n côtés. Dans les cas II (diédral), on rajoute à ces rotations les symétries droites (demi-tours) d'axes les droites joignant les milieux (respectivement sommets) du polygone.

2.4. Sous-groupes finis de $\mathbf{GL}_n(\mathbf{Z})$. — On trouve déjà des groupes finis aussi grand qu'on veut dans $\mathbf{GL}_n(\mathbf{R}), n \leq 3$. Observons qu'ils sont « presque abéliens », au sens qu'ils contiennent un sous-groupe *abélien normal* d'indice petit, ici ≤ 60. On verra plus bas (2.5.1) que c'est toujours le cas. D'une certaine manière, si on veut plonger un groupe gros et compliqué dans un $\mathbf{GL}_n$, il y a un prix à payer : n sera grand. Pour l'instant, montrons que les sous-groupes de $\mathbf{GL}_n(\mathbf{Z})$ sont « petits ».

***Proposition 2.4.1* (Lemme de Serre).** — *Soit p un entier plus grand que 3. Alors, la restriction du morphisme*

$$\mathbf{GL}_n(\mathbf{Z}) \to \mathbf{GL}_n(\mathbf{Z}/p\mathbf{Z})$$

à un sous-groupe fini G est injectif.

Preuve : Les matrices de G sont d'ordre fini donc diagonalisables sur $\mathbf{C}$ (cf. preuve de 2.1.1). Leurs valeurs propres λ sont des racines de l'unité. Supposons que $g \in G$ soit dans le noyau, *ie* $g = \mathrm{Id} + pM$ avec $M \in M_n(\mathbf{Z})$. On a donc

$$\chi_g(X) = p^n \chi_M(\frac{X-1}{p})$$

où $\chi_B(X) = \det(X\mathrm{Id} - B)$ désigne le polynôme caractéristique. On va montrer qu'une écriture

$$P_n(X =)p^n Q_n(\frac{X-1}{p})$$

avec P_n, Q_n unitaires de degré n, P_n de racines des complexes λ de module 1 et Q_n à coefficients entiers force l'égalité $P_n = (X-1)^n$. En effet, $P_n(1) = \prod(1-\lambda) = p^n \times (entier)$. Le module du membre de gauche est plus petit que 2^n et $p \geq 3$ et donc l'entier en question est plus petit que $(2/3)^n$ en valeur absolu : il est nul. Ceci montre que 1 est racine de P_n, et règle au passage le cas $n = 1$. Divisant P_n par $X - 1$ et Q_n par X, on trouve une nouvelle relation du même type sur les quotients : tous les λ valent donc 1 et donc $g = 1$.■

Corollaire 2.4.2. — *Le cardinal d'un sous-groupe fini de $\mathbf{GL}_n(\mathbf{Z})$ est majoré*

$$\text{card } \mathbf{GL}_n(\mathbf{Z}/3\mathbf{Z})) = (3^n - 1) \cdots (3^n - 3^{n-1}).$$

2.5. Le théorème de Jordan. — Comme convenu, on va montrer un résultat dû à Jordan affirmant peu ou prou qu'un sous-groupe fini d'un $GL_n(\mathbf{C})$ n'est pas trop compliqué.

***Théorème 2.5.1* (Jordan,Schur).** — *Soit G un sous-groupe fini de $\mathbf{GL}_n(\mathbf{C})$. Alors, G a un sous-groupe abélien normal d'indice $\leq (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$.*

Preuve : L'astuce de la moyenne permet de supposer $G \subset U_n(\mathbf{C})$. On va voir que les matrices de G proches de Id forment un sous-groupe abélien normal. Prouvons quelques (jolis) lemmes élémentaires sur les matrices unitaires. On rappelle que deux matrices unitaires qui commutent sont simultanément *unitairement semblables* à des matrices diagonales de valeurs propres des racines de l'unité. On munit $M_n(\mathbf{C})$ de la norme L^2 définie par

$$|A| = \sqrt{\mathrm{Tr}(AA^*)}, \tag{2.5.a}$$

qui est invariante par multiplication à gauche ou à droite par des matrices unitaires. C'est une norme sous-multiplicative. Si A est unitaire, $|A| = \sqrt{n}$. On va montrer que si $A, B \in G$ sont assez proches de Id, alors

elles commutent. Le point est qu'essentiellement, si A, B assez voisines de Id, le commutateur est encore plus près de Id. Maintenant, comme les spectres possibles des éléments de G sont en nombre fini et que les matrices de G sont diagonalisables, ceci assure que si A, B sont proches de l'identité, le commutateur est trivial. On conclut alors facilement. Précisons tout cela.

Lemme 2.5.2. — *Soient A, B unitaires et supposons $|\mathrm{Id}-B|<2$. Alors si A commute avec $(A,B)=ABA^{-1}B^{-1}$ alors A et B commutent.*

Preuve : Par hypothèse, A commute avec $A(A,B)=BA^{-1}B^{-1}$, donc avec son inverse BAB^{-1} (dans un groupe si $xy=yx$, on a $y^{-1}x^{-1}=x^{-1}y^{-1}$ d'où $x^{-1}y=yx^{-1}$). Comme A et BAB^{-1} ont même spectre, on peut donc supposer sans nuire à la généralité qu'elles sont diagonales. Si on note $a_i, i=1\cdots r$ les valeurs propres distinctes de A, on a donc une décomposition en espaces propres

$$\mathbf{C}^n=\bigoplus_{i=1}^{r}\bigoplus_{j\in J_i}\mathbf{C}e_j$$

où e_j propre de valeur propre a_i pour $j\in J_i$. Ainsi,

$$A=\mathrm{diag}(a_i\mathrm{Id}_i)$$

avec Id_i l'identité de taille card J_i.
Il existe une matrice de permutation

$$P=(\delta_{j,\sigma(i)})_{i,j}, \sigma\in S_n$$

(en particulier P est unitaire) telle que

$$P^{-1}AP=BAB^{-1}$$

(car A et BAB^{-1} diagonales de même spectre) et donc $R=PB$ et A commutent. Un calcul standard prouve que R est diagonale par blocs

$$R=\mathrm{diag}(R_i)$$

avec R_i de taille $\mathrm{card}(J_i)$.
-Si pour tout i, on a $\sigma(J_i)\subset J_i$, la matrice P s'écrit

$$\mathrm{diag}(P_{\sigma_i}) \text{ avec } \sigma_i\in S_{\mathrm{card}(J_i)}$$

et donc commute à A. Ainsi, $A=BAB^{-1}$ et c'est terminé.
-Sinon, il existe au moins *deux* indices $i\neq k$ tels que

$$\sigma(J_i)\not\subset J_i \text{ et } \sigma(J_k)\not\subset J_k.$$

En particulier, il existe deux indices

$$\iota\in J_i \text{ et } \kappa\in J_k \text{ tels que } R_{\iota,\sigma(\iota)}=R_{\kappa,\sigma(\kappa)}=0$$

(on a simplement écrit qu'il y a des blocs de zéros à côté des blocs R_i, R_k et en particulier les colonnes d'indice $\sigma(\iota),\sigma(\kappa)$ sont nulles).
Mais alors

$$|\mathrm{Id}-B|^2=|P-R|^2\geq\sum_l(|P_{\iota,l}-R_{\iota,l}|^2+|P_{\kappa,l}-R_{\kappa,l}|^2)=1+\sum_l(|R_{\iota,l}|^2)+1+\sum_l(|R_{\kappa,l}|^2)=4$$

puisque $R_{\iota,\sigma(\iota)} = R_{\kappa,\sigma(\kappa)} = 0$. Ce cas ne se produit donc pas.■

Lemme 2.5.3. — *Soient A, B unitaires. Alors,*

$$|\mathrm{Id} - (A, B)| \leq \sqrt{2}|\mathrm{Id} - A||\mathrm{Id} - B|.$$

Preuve : On peut supposer $A = \mathrm{diag}(a_i)$. On a

$$|\mathrm{Id} - (A, B)|^2 = |BA - AB|^2 = \sum |(a_i - a_j)b_{i,j}|^2 = \sum |(a_i - a_j)(\delta_{i,j} - b_{i,j})|^2$$

(en effet $(a_i - a_j)(\delta_{i,j} - b_{i,j})$ est nul si $i = j$!).
Or, on a

$$|a_i - a_j|^2 = |(1 - a_i) - (1 - a_j)|^2 \leq (|1 - a_i| + |1 - a_j|)^2 \leq 2(|1 - a_i|^2 + |1 - a_j|)^2) \leq 2|\mathrm{Id} - A|^2.$$

En reportant, on ce qu'on voulait.■

Lemme 2.5.4. — *Soient $A, B \in G$. Si $|\mathrm{Id} - A| < 1/\sqrt{2}$ et $|\mathrm{Id} - B| < 2$, alors A et B commutent.*

Preuve : C'est très joli. On définit la suite de matrices B_i par

$$B_0 = B \text{ et } B_{i+1} = (A, B_i).$$

D'après le lemme 2.5.3, on a

$$|\mathrm{Id} - B_i| \leq (\sqrt{2}|\mathrm{Id} - A|)^i |\mathrm{Id} - B_0|$$

et donc $\lim B_i = \mathrm{Id}$. Comme B_i varie dans G qui est fini, donc discret, on a $B_i = \mathrm{Id}$ si $i >> 0$. Montrons par récurrence descendante que B_i et A commutent pour tout i. Si $i >> 0$, c'est vrai. Supposons que $B_{i+1} = (A, B_i)$ et A commutent. Comme les matrices A et B_i sont unitaires et que $|I - B_i| < |I - B_0| < 2$, le lemme 2.5.3 assure que B_i et A commutent.■

Notons alors H le sous groupe engendré par

$$\{A \in G \text{ tels que } |I - A| < 1/\sqrt{2}\}.$$

Le lemme 2.5.4 assure que les éléments de H commutent deux à deux et donc H est abélien et visiblement normal (la norme unitaire est certainement invariante par conjugaison unitaire).
Reste à évaluer son indice. Soit A_i un système de représentant de G/H. Ils sont comme on l'a vu sur la sphère de rayon $\sqrt{n}$ de $M_n(\mathbf{C}) = \mathbf{R}^{2n^2}$. D'autre part, si $i \neq j$, on a

$$|R_i - R_j| \geq 1/\sqrt{2}$$

car sinon $R_i^{-1} R_j \in H$. Notons B_i la boule de centre R_i et de rayon $1/(2\sqrt{2})$. On a donc $B_i \cap B_j = \emptyset$. Autrement dit, on a une réunion *disjointe* des B_i toutes contenues dans la couronne

$$C(\sqrt{n} - 1/(2\sqrt{2}), \sqrt{n} + 1/(2\sqrt{2})).$$

Si v est le volume de la boule unité, on a donc

$$\sum_i v(B_i) = [G : H](1/2\sqrt{2})^{2n^2} v \leq (C(\sqrt{n} - 1/(2\sqrt{2}), \sqrt{n} + 1/(2\sqrt{2})) = (\sqrt{n} + 1/(2\sqrt{2}))^{2n^2} v - (\sqrt{n} - 1/(2\sqrt{2}))^{2n^2} v,$$

qui donne l'inégalité annoncée.■

Par exemple, ceci donne une borne pour les cardinaux des groupes finis simples contenus dans $\mathbf{GL}_n(\mathbf{C})$. Notons que ce théorème reste valable remplaçant $\mathbf{C}$ par un corps de caractéristique positive p pourvu qu'on se limite à des groupes d'ordre premier à p. La démonstration est tout autre, et nettement plus technique. Pour des généralisations, on pourra aller regarder le livre [**7**] , livre dont est servilement tiré la preuve précédente.

3. Sous-groupes résolubles

On trouve partout (et il est facile de prouver) que le groupe $\mathbf{PGL}_n(k) = \mathbf{GL}_n(k)/k^*$ est simple, au moins si k est un corps de cardinal ≥ 3 ou $n \geq 3$. Ceci signifie que les sous-groupes normaux non triviaux sont centraux, ce qui en limite l'intérêt. Par exemple, le groupe dérivé de $\mathbf{GL}_n(k)$ est $\mathbf{SL}_n(k)$ (dans le cas $k \neq \mathbf{F}_2$, observer qu'une transvection est semblable à son carré) et celui de $\mathbf{SL}_n$ est lui-même : $G = \mathbf{GL}_n$ n'est pas résoluble (ceci signifie que la série dérivée $D^0 = G, D^{i+1} = [D^i, D^i]$ n'est pas réduite à l'identité si $i >> 0$, ou, plus géométriquement, que G n'est pas extension successive de sous-groupes normaux abéliens -cf. le cours de théorie de Galois-). On peut caractériser les sous-groupes résolubles de $\mathbf{GL}_n(\mathbf{C})$, à condition qu'ils soient connexes.

3.1. Le théorème de Lie-Kolchin. —

Exercice 3.1.1. — *Montrer que T_n le sous-groupe de $\mathbf{GL}_n$ des matrices triangulaires supérieures est résoluble.*

En fait, $T_n(\mathbf{C})$ est le sous-groupe résoluble connexe maximal de $\mathbf{GL}_n(\mathbf{C})$.

Théorème 3.1.2 **(Lie-Kolchin)**. — *Soit G un sous-groupe résoluble connexe de $\mathbf{GL}_n(\mathbf{C})$. Alors, G est conjugué à un sous-groupe de $T_n(\mathbf{C})$.*

Preuve : On identifie matrices et endomorphismes de $V = k^n$. On veut montrer l'existence d'un *drapeau*

$$0 = V_0 \subset V_i \cdots \subset V_n = V$$

de sous-espaces vectoriels V_i de dimension i stables par G. On fait une récurrence sur $s = \dim V + l$ où l est la longueur de la série des groupes dérivés itérés (le cas $s = 0$ étant laissé au lecteur...).
On suppose donc $s > 0$ (et donc $n > 0$) et le théorème prouvé si $s < n$. Si $V \neq 0$ a un sous-espace stable W *non trivial* par G, la récurrence appliqué à V et V/W permet de conclure. On peut donc supposer qu'un tel espace n'existe pas (on dit que la représentation de G sur V est *irréductible*).
Si $l = 0$ (*ie* G abélien), alors on a une suite de matrices trigonalisables qui commutent, et donc ont un vecteur propre en commun (bien classique...). Comme V est irréductible, on a donc $\dim V = 1$ et c'est terminé.
On peut donc désormais supposer $l > 0$. Soit $H = [G, G]$ le groupe dérivé de G : c'est un sous-groupe normal, non trivial car $l > 0$. Il est connexe : c'est l'image des applications continues « produit de commuateurs »

$$G^2 \times G^2 \cdots \times G^2 \to G$$

qui toutes ont l'identité en commun. Le groupe H est bien entendu résoluble comme G (car $D^i(H) \subset D^i(G)$). Comme $s(H) = s(G) - 1$, l'hypothèse de récurrence assure que les éléments $h \in H$ admettent un vecteur propre commun v *non nul* de valeur propre $\lambda(h) \in \mathbf{C}$. Notons que $\lambda \in H^*$, ensemble des *caractères continus* de H. Soit

$$W = \bigoplus_{\chi \in H^*} V_\chi$$

où

$$V_\chi = \{v \in V \text{ tels que } hv = \chi(h)v \text{ pour tout } h \in H\}.$$

On a $gV_\chi \subset V_{g\chi}$ avec $g\chi(h) = \chi(g^{-1}hg)$ de sorte que W est *non nul* ($v \in W$) et *stable* par G. Comme V est irréductible, on a

$$V = W = \bigoplus_{\chi \in H^*} V_\chi.$$

Une autre manière de dire est que dans une base convenable, on a

$$h = \begin{pmatrix} \lambda_1(h) & & \\ & \ddots & \\ & & \lambda_n(h) \end{pmatrix} \text{ et } g^{-1}hg = \begin{pmatrix} \lambda_1(g^{-1}hg) & & \\ & \ddots & \\ & & \lambda_n(g^{-1}hg) \end{pmatrix}.$$

Comme h et $g^{-1}hg$ sont semblables, elles ont même spectre. Aussi, à h fixé, $g^{-1}hg$ prend un nombre fini de valeurs. Par connexité de G et continuité du produit matriciel, on déduit $h = ghg^{-1}$ pour tout g. Mais alors $\mathrm{Ker}(h - \lambda_1(h))$ est non nul et stable par G tout entier : c'est donc V. Donc h est une homotéthie de déterminant 1 (c'est un commutateur), donc de rapport une racine de 1. Par connexité de H, ce rapport est 1, une contradiction car H non trivial.■

Rappelons que Tits a montré qu'un sous-groupe de type fini de $\mathbf{GL}_n(\mathbf{R})$ qui ne contient pas de sous-groupe libre à deux générateurs possède un sous-groupe normal résoluble d'indice fini Regardons à quoi peuvent ressembler les sous-groupes libres du groupe linéaire.

Remarque 3.1.3. — *Le groupe des permutations S_3 est visiblement résoluble et non connexe. O peut le faire opérer sur $\mathbf{C}$ grâce à la signature où sur $\mathbf{C}^3$ grâce aux matrices de permutation. On peut facilement montrer que l'action d'un sous-groupe G de $\mathbf{GL}_n(\mathbf{C})$ isomorphe à S_3 sur $\mathbf{C}^n$ est nécessairement isomorphe à la somme directe de $\mathbf{C}$ ou de $\mathbf{C}^3$ avec l'action précédente sur chaque facteur et d'un facteur $\mathbf{C}^m$ avec action triviale. On déduit que G n'admet pas de drapeau stable : l'hypothèse de connexité dans le théorème de Lie-Kolchin est cruciale.*

4. Sous-groupes libres

On dira qu'un G groupe est produit libre de deux sous-groupes G_1, G_2 si l'application de restriction

$$\mathrm{Hom}(G, H) \to \mathrm{Hom}(G_1, H) \times \mathrm{Hom}(G_2, H)$$

est un isomorphisme pour tout groupe H. Moralement, ceci signifie qu'on a le moins de relations possibles entre éléments de G_1, G_2.

On montre sans peine que $G = G_1 * G_2$ si et seulement si G_1, G_2 engendrent G et si les produits de termes successifs d'éléments de G_1 et G_2 différents de 1 est encore différent de 1 (cf. [**2**]).

Étant donné deux groupes G_1, G_2, on en déduit facilement la construction d'un groupe G produit libre de G_1 et G_2, unique à isomorphisme près d'après la proposition universelle précédente (exercice).
Un groupe libre à n générateurs est simplement le produit libre de n copies de $\mathbf{Z}$. Le lecteur vérifier à titre d'exercice qu'un groupe libre à n générateurs n'est isomorphe à un groupe libre à m générateurs que si $m = n$.
On montre (théorème de Nielsen-Schreier) que tout sous-groupe d'un groupe libre est libre, mais pas forcément avec une famille finie de générateurs ([**2**] ou mieux, pour une preuve topologique, [**10**]).
On va construire une famille de sous-groupes libres à deux générateurs et discrets de $\mathbf{GL}_2(\mathbf{R})$, en fait de $\mathbf{SL}_2(\mathbf{R})$. On en déduira une famille de sous-groupes libres à deux générateurs et... denses!!!

4.1. Une famille explicite. — Soient a, b deux réels. Posons

$$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

On se donne des entiers relatifs non nuls $n_i, m_i, i \geq 0$. On définit par récurrence les matrices M_i par

$$M_0 = \mathrm{Id}, M_{2i+1} = M_{2i}A^{n_i} \text{ et } M_{2i+2} = M_{2i+1}B^{m_i}.$$

Autrement dit, on fait un produit « du type »

$$M_i = A^{n_1}B^{m_1}A \cdots B^{m_{k-1}}A^{n_k} \cdots$$

avec i facteurs.
Le lemme suivant est dû à Jean Lannes. On définit le réel $c(n)$ comme étant le terme d'indice $(1,1)$ de M_n si n pair et d'indice $(1,2)$ si n impair. On a $c(0) = 1, c(1) = a$.

Lemme 4.1.1. — *Supposons* a et $b \geq 2$. *Alors,* $|c(n)| \geq n+1$ *pour tout* n.

Preuve : On a

$$M_{2t} = \begin{pmatrix} * & c(2t-1) \\ * & * \end{pmatrix} \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} = \begin{pmatrix} c(2t) & * \\ * & * \end{pmatrix}$$

de sorte que

$$M_{2t} = \begin{pmatrix} c(2t) & c(2t-1) \\ * & * \end{pmatrix}.$$

et de même

$$M_{2t+1} = \begin{pmatrix} c(2t) & c(2t+1) \\ * & * \end{pmatrix}.$$

Utilisant alors la relation $M_{2t+1} = M_{2t}A^{n_t}$, on trouve la relation

$$c(2t+1) = n_t a c(2t) + c(2t-1).$$

Utilisant alors la relation $M_{2t+2} = M_{2t+1}B^{m_t}$, on trouve la relation

$$c(2t+2) = m_t b c(2t+1) + c(2t).$$

Donc, on déduit immédiatement l'inégalité

$$|c(n+1)| \geq 2|c(n)| - |c(n-1)| \text{ } ie \text{ } |c(n+1)| - |c(n)| \geq |c(n)| - |c(n-1)|$$

pour tout $n > 0$. Comme $|c(1)| - |c(0| = a - 1 \geq 1$, le lemme suit.■

Si on veut traiter des produits qui commencent par B et non par A, on conjugue par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ce qui ramène au cas précédent (avec a changé en b). Dans tous les cas, un produit de n puissances d'exposants non nuls des matrices A ou B a au moins un coefficient de valeur absolue $\geq n+1$. En particulier, il est $\neq \mathrm{Id}$.

Corollaire 4.1.2. — *Si $a, b \geq 2$, le sous-groupe $L_{a,b}$ de $\mathbf{SL}_2(\mathbf{R})$ engendré par A et B est libre et discret.*

Rappelons qu'un espace topologique est discret si chaque point est ouvert. Attention toutefois à ne pas faire de confusion car on regarde ici la topologie induite par la topologie de $M_n(\mathbf{R})$ sur $\mathbf{GL}_n(\mathbf{R})$. Prenons le cas $n = 1$ et $G = \{2^k, k \in \mathbf{Z}\}$. C'est bien un sous-groupe discret : la suite des 2^{-k} s'approche bien de 0 dans $\mathbf{R}$ quand k devient grand mais $0 \notin G$!

Exercice 4.1.3. — *Montrer que si $a, b = 1$, le groupe engendré par a, b n'est pas libre.*

4.2. Exemples, suite. — La propriété d'être libre est très « instable ».

Lemme 4.2.1. — *Soit $a \in \mathbf{R}$ un nombre transcendant sur $\mathbf{Q}$. Alors, le groupes $L_a = L_{a,a}$ est libre à deux générateurs A, B.*

Preuve : Considérons le morphisme

$$\mathbf{GL}_2(\mathbf{Z}[T]) \to \mathbf{GL}_2(\mathbf{R})$$

déduit de la flèche $T \to a$. Ce morphisme est injectif car a est transcendant. Supposons qu'on ait un produit non trivial du « type $ABAB...$ » qui vaut l'identité dans L_a. Le produit correspondant dans L_T serait aussi l'identité dans $\mathbf{GL}_2(\mathbf{Z}[T])$. Si on envoie maintenant T sur 2, on déduit que le produit correspondant dans L_2 serait nul, ce qui n'est pas car $L_2 = \mathbf{Z}A * \mathbf{Z}A$ dans ce cas, une contradiction.■

Remarquons qu'on a des nombres transcendants t aussi proches qu'on veut de 1. Les groupes L_t sont des groupes libres à deux générateurs A, B mais pas L_1. A priori, on peut se demander si L_1 ne serait pas un groupe libre avec d'autres générateurs. Il n'en n'est rien comme le montre la section suivante.

4.3. Ping-pong. — On va donner un critère bien commode pour reconnaître qu'un produit est libre. Ceci va permettre par exemple de prouver que le produit libre de deux groupes très petit peut être très gros.

***Proposition 4.3.1* (Lemme du ping-pong)**. — *Soit G un groupe opérant sur un ensemble E. Soient H, H' deux sous-groupes de G. On suppose qu'il existe deux parties non vides X, X' de X tels que*

$$hX' \subset X \text{ si } h \in H \setminus 1 \text{ et } h'X \subset X' \text{ si } h' \in H \setminus 1.$$

Alors, si H' n'est pas réduit à 2 éléments et $X' \not\subset X$, alors, le morphisme canonique

$$H * H' \to < H, H' >$$

est un isomorphisme.

Preuve : on peut supposer $H \neq 1$.

-Considérons d'abord un produit « impair »

$$p = h_0 h'_1 h_1 \cdots h'_k h_k$$

avec $h_i \in H \setminus 1$ et $h'_i \in H' \setminus 1$. Si $p = 1$, on a

$$X' = h_0 h'_1 h_1 \cdots h'_k h_k X' \subset h_0 h'_1 h_1 \cdots h'_k X \cdots \subset h_0 X' \subset X,$$

ce qui n'est pas.

-Si on a un produit « impair »

$$p = h'_0 h_1 h'_1 \cdots h_k h'_k$$

avec $h_i \in H \setminus 1$ et $h'_i \in H' \setminus 1$, choisissons $h \in H \setminus 1$. Alors,

$$hph^{-1} = hh'_0 h_1 h'_1 \cdots h_k h'_k h^{-1}$$

est différent de 1 d'après ce qui précède et donc $p \neq 1$.

-Si on a un produit « pair »

$$p = h_1 h'_1 \cdots h_k h'_k$$

avec $h_i \in H \setminus 1$ et $h'_i \in H' \setminus 1$, choisissons $h' \in H' \setminus \{1, h'_k\}$. Alors

$$h'ph'^{-1} = h' h_1 h'_1 \cdots h_k (h'_k h'^{-1})$$

est un « produit impair » comme plus haut et donc $p \neq 1$.

-Si enfin on a un produit « pair »

$$p = h'_1 h_1 \cdots h'_k h_k$$

avec $h_i \in H \setminus 1$ et $h'_i \in H' \setminus 1$, alors

$$h_k p h_k^{-1} = h_k h'_1 h_1 \cdots h'_k$$

est un « produit pair » du type précédent et donc $p \neq 1$.■

Corollaire 4.3.2. — *Le sous-groupe de* $G = \mathbf{PSL}_2(\mathbf{R})$ *engendré par*

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ et } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

est le produit libre de $H =< S > \tilde{\to} \mathbf{Z}/2\mathbf{Z}$ *et de* $H' =< TS > \tilde{\to} \mathbf{Z}/3\mathbf{Z}$.

Preuve : On fait opérer G sur $\hat{\mathbf{R}} = \mathbf{R} \sqcup \infty$ par la formule usuelle

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .t = \frac{at+b}{ct+d}.$$

On a $St = -1/z$ et $Tt = z + 1$. Posons

$$X' = \mathbf{R}_{>0} \sqcup \infty \text{ et } X = \mathbf{R}_{\leq 0}.$$

On a visiblement $S(X') = X$. Par ailleurs, on a $h' = TS = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ qui agit par $t \mapsto -1/t + 1$. C'est un élément d'ordre 3. L'image de $X = R_{\leq 0}$ par cette transformation est $\mathbf{R}_{>1} \cup \infty \subset X'$ et l'image par le carré de h' est

$$h'(\mathbf{R}_{>1} \cup \infty) =]0, 1] \subset X'.$$

On conclut par le lemme du ping-pong.■

Lemme 4.3.3. — *Le groupe $\mathbf{SL}_2(\mathbf{Z})$ est engendré par S et T.*

Preuve : On a

$$T' = S^{-1}TS = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Ainsi, si on se permet de multiplier à droite ou à gauche $A \in \mathbf{SL}_2(\mathbf{Z})$ par des puissances de T ou de T', on ne fait qu'ajouter un multiple entier d'une ligne (colonne) de A à l'autre ligne (colonne) de A. Multiplier à gauche ou à droite par S échange, aux signe près, ligne et colonne ou vice versa. On va faire du pivot de Gauss à coefficients entiers.

Deux matrices obtenues par un tel procédé seront simplement dites équivalentes. Soit A une matrice de $\mathbf{SL}_2(\mathbf{Z})$. On note $m(A)$ la plus petite valeur absolue de ses coefficients non nuls. Dans l'ensemble des matrices qui lui sont équivalentes, choisissons A' tel que le maximum des valeurs absolues de ses coefficients non nuls soit minimal (un tel A' existe). On peut supposer $A = A'$. Par permutation de ligne et de colonne, on peut supposer $a_{1,1} = m(A)$. Si $a_{1,2}$ est non nul par exemple, on fait la division $a_{1,2} = qa_{1,1} + r, 0 \leq r < |a_{1,1}$ et on ajoute $-q$ fois la première colonne à la seconde. Le coefficient $a_{1,2}$ est remplacé par r et donc r est nul par minimalité. Le même argument sur les lignes prouve que nécessairement A est diagonale avec $|a_{2,2}| \geq |a_{1,1}|$. En ajoutant la première ligne à la seconde, on se ramène à

$$\begin{pmatrix} a_{1,1} & 0 \\ a_{1,1} & a_{2,2} \end{pmatrix}.$$

L'argument précédent (en divisant $a_{2,2}$ par $a_{1,1}$ prouve $a_{1,1}|a_{2,2}$). Un argument de déterminant prouve $A = \pm\mathrm{Id}$.■

Corollaire 4.3.4. — *Le morphisme précédent induit un isomorphisme*

$$\mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/3\mathbf{Z} \xrightarrow{\sim} \mathbf{PSL}_2(\mathbf{Z}).$$

Remarque 4.3.5. — *On ne peut faire marcher cet argument dans $SL_2(\mathbf{R})$. En effet, $S^2 = -\mathrm{Id} \neq 1$ mais agit trivialement : on n'a pas de ping-pong. On aurait, pour le lecteur savant, un produit amalgamé $\mathbf{Z}/4\mathbf{Z} *_{\mathbf{Z}/2\mathbf{Z}} \mathbf{Z}/6\mathbf{Z} = \mathbf{SL}_2(\mathbf{Z})$. Notre groupe $L_1 = \mathbf{SL}_2(\mathbf{Z})$ n'est donc certainement pas libre à n générateurs, car par exemple*

$$\mathrm{Hom}(\mathbf{SL}_2(\mathbf{Z}), \mathbf{Z}) = 1$$

(ce qu'on peut voir facilement à la main d'ailleurs).

Toutes ces choses sont bien connues et sont racontées en de nombreux endroits. On pourra consulter pour approfondir le joli livre [**8**].

Un sous groupe discret n'est autre qu'un sous-groupe qui est aussi une sous-variété fermée de dimension zéro de $\mathbf{GL}_n(\mathbf{R})$. Les sous-groupes fermés connexes de $\mathbf{GL}_n(\mathbf{R})$ sont assez bien compris, en tout cas sont codés par un objet bilinéaire : leur algèbre de Lie. C'est l'objet du théorème de Cartan.

5. Sous-groupes fermés

On se donne un sous-groupe connexe fermé non trivial de G, en particulier non discret. On va voir, grâce à l'exponentielle, que c'est une sous-variété de $\mathbf{GL}_n(\mathbf{R})$ et qu'il est bien déterminé par un sous espace vectoriel de $M_n(\mathbf{R})$: son algèbre de Lie. Commençons par quelques rappels sur l'exponentielle de matrice.

5.1. Exponentielle. — On fixe une norme sous-multiplicative sur $M_n(\mathbf{R})$, par exemple la norme L^2 (2.5.a). Si $|H| < 1$, on définit

$$\ln(\mathrm{Id} - H) = \sum_{k=0}^{\infty} \frac{H^{k+1}}{k+1}$$

(la série converge absolument). On a

$$\exp(\ln(\mathrm{Id} + H)) = \mathrm{Id} + H \text{ pour tout } H \text{ tel que } |H| < 1$$

(argument formel ou changer H en tH et dériver par rapport à $t \in \mathbf{R}$). On dispose donc d'un application analytique de la boule unité ouverte autour de Id dans $M_n(\mathbf{C})$ dans $\mathbf{GL}_n(\mathbf{C})$ définie par $M \to \ln(M - \mathrm{Id})$. Inversement, observons qu'on a

$$|\exp(H) - \mathrm{Id}| < \exp(|H| - 1) < 1 \text{ et } \ln\exp(H) = H \text{ si } |H| < 1/2.$$

En particulier, l'exponentielle réalise un homéomorphisme analytique d'inverse L entre la boule ouverte V de centre 0 et de rayon $1/2$ dans $M_n(\mathbf{C})$ et le voisinage ouvert de Id $W = \exp(V) = L^{-1}(V)$ de $\mathbf{GL}_n(\mathbf{C})$: c'est une version explicite du théorème d'inversion locale. Ce phénomène est général.

5.2. Algèbre de Lie d'un sous-groupe fermé. — Soit G un sous-groupe fermé connexe de $\mathbf{GL}_n(\mathbf{R})$. Soit

$$\mathfrak{g} = \{M \in M_n(\mathbf{R}) \text{ tels que } \exp(tM) \in G \text{ pour tout } t \in \mathbf{R}\}.$$

On note $[A, B] = AB - BA$ le crochet de Lie de deux matrices.

Proposition 5.2.1. — *Avec les notations précédentes,* $\mathfrak{g}$ *est une sous-algèbre de Lie de* $M_n(\mathbf{R})$.

Preuve : La proposition est un conséquence immédiate du lemme suivant.

Lemme 5.2.2. — *Soit* $X, Y \in M_n(\mathbf{C})$. *Alors on a*

i) $\lim_{k\to\infty}(\exp(\frac{-X}{k})\exp(\frac{-Y}{k}))^k = \exp(X+Y)$;

ii) $\lim_{k\to\infty}(\exp(\frac{X}{k})\exp(\frac{Y}{k})\exp(\frac{-X}{k})\exp(\frac{-Y}{k}))^{k^2} = \exp([X,Y])$;

Preuve : Prenons *ii*) par exemple. On a

$$\exp(\frac{X}{k})\exp(\frac{Y}{k})\exp(\frac{-X}{k})\exp(\frac{-Y}{k}) = \mathrm{Id} + \frac{[X,Y]}{k^2} + o(1/k^2),$$

en particulier cette suite tend vers l'identité. On a alors,

$$k^2 L(\exp(\frac{X}{k})\exp(\frac{Y}{k})\exp(\frac{-X}{k})\exp(\frac{-Y}{k})) = [X,Y] + o(1).$$

Pour k assez grand, en prenant l'exponentielle, on déduit

$$(\exp(\frac{X}{k})\exp(\frac{Y}{k})\exp(\frac{-X}{k})\exp(\frac{-Y}{k}))^{k^2} = \exp([X,Y] + o(1)) = \exp([X,Y]) + o(1),$$

ce qu'on voulait. Le point i) est analogue. Remarquons qu'on n'a pas pris le log de l'expression, mais plutôt pris l'exponentielle de ce qui formellement est le log : ceci tient au fait que le log n'est défini que localement.■

Si maintenant $X, Y \in \mathfrak{g}$, le point i) prouve que $\exp(t(X+Y))$ est limite d'éléments de G, donc est dans G car G est fermé, de même pour $\exp(t[X,Y])$. Comme $\mathfrak{g}$ contient zéro et est stable par passage à l'opposé, on a gagné. ■

Par exemple, l'algèbre de Lie $\mathfrak{sl}_n(\mathbf{R})$ de $SL_n(\mathbf{R})$ est l'ensemble des matrices de trace nulle.
Bien entendu, si G est discret, alors $\mathfrak{g} = 0$ (sinon $\exp(X/k)$ est une suite d'éléments non triviaux de G convergeant vers l'identité pour $0 \neq X \in \mathfrak{g}$). La réciproque est vraie.

Lemme 5.2.3. — *Un sous-groupe fermé G de $\mathbf{GL}_n(\mathbf{R})$ est discret si et seulement si $\mathfrak{g} = 0$. Précisément, si g_k est une suite g_k d'éléments non triviaux de G convergeant vers l'identité, toute valeur d'adhérence de « la suite des log » $\frac{L(g_k)}{|L(g_k)|}$ est un élément non nul de $\mathfrak{g}$.*

Preuve : Supposons que G est non discret. On a donc une suite d'éléments distincts γ_k convergeant vers $\gamma \in \mathbf{GL}_n(\mathbf{R})$. Comme G est fermé, on a $\gamma \in G$. Posant $g_k = \gamma_k \gamma^{-1}$, on obtient une suite g_k d'éléments $\neq \mathrm{Id}$ de G convergeant vers l'identité. Pour k assez grand, $X_k = L(g_k)$ est bien défini et est non nul convergeant vers 0. Par compacité, on peut supposer $X = X_k/|X_k|$ converge vers X sur la sphère unité de $M_n(\mathbf{R})$.
Montrons qu'on a $X \in \mathfrak{g}$. En effet, soit $t \in \mathbf{R}$ et notons $e_k = \left[\frac{t}{|X_k|}\right]$ la partie entière de $\frac{t}{|X_k|}$. La suite $e_k X_k$ converge vers tX car X_k tend vers zéro . Ainsi, la suite d'éléments de G

$$\exp(e_k X_k) = (g_k)^{e_k}$$

converge vers $\exp(tX)$ ce qui prouve $X \in \mathfrak{g}$. ■

Cet énoncé se généralise comme suit.

5.3. Le théorème de Cartan. — Le théorème de Cartan caractérise les sous-groupes fermés connexes par leur algèbre de Lie.

***Théorème 5.3.1* (Cartan)**. — *Soit G un sous-groupe fermé de $\mathbf{GL}_n(\mathbf{R})$ d'algèbre de Lie $\mathfrak{g}$. Alors on a*
– *l'exponentielle réalise un homéomorphisme local $(\mathfrak{g}, 0) \xrightarrow{\sim} (G, \mathrm{Id})$;*
– *Si G est connexe, $\exp(\mathfrak{g})$ engendre G.*

En fait, la preuve donnera un peu mieux : l'exponentielle permet de montrer que G est une sous-variété de $GL_n(\mathbf{R})$, autrement dit il existe un homéomorphisme d'un voisinage V de Id dans $GL_n(\mathbf{R})$ *sur* un voisinage U de $(0,0)$ dans l'espace linéaire $\mathbf{R}^d \times \mathbf{R}^c$ induisant un homéomorphisme $G \cap V \xrightarrow{\sim} \mathbf{R}^d \cap U$. Une autre manière de dire (projeter sur $\mathbf{R}^c$) est qu'il existe (*localement* au voisinage de Id) une submersion (différentielle surjective) $s : \mathbf{GL}_n(\mathbf{R}) \to \mathbf{R}^c$ telle que (localement), on ait $G = s^{-1}(0)$, *ie* G est *localement* donné par $c = n^2 - \dim(\mathfrak{g})$ équations transverses.
Preuve : Soit $\mathbf{R}^c$ un supplémentaire de $\mathfrak{g}$ dans $M_n(\mathbf{R})$ et considérons l'application

$$\phi : \begin{cases} \mathfrak{g} \times \mathbf{R}^c & \to & \mathbf{GL}_n(\mathbf{R}) \\ (X,Y) & \mapsto & \exp(X)\exp(Y) \end{cases}$$

Sa différentielle en 0 est $(X,Y) \mapsto X+Y$ qui est un isomorphisme. Le théorème d'inversion local assure l'existence de voisinages ouverts U de 0 et V de Id tels que ϕ soit un homéomorphisme (en fait analytique) de U sur V. On peut supposer U que est une boule ouverte centrée en 0, en particulier stable par homotéthie de rapport < 1. La projection linéaire

$$p : \mathfrak{g} \times \mathbf{R}^c \to \mathbf{R}^c$$

est certainement une submersion en zéro (en fait partout). Autrement dit, on a une submersion en Id

$$s = p \circ \phi^{-1} : V \to \mathbf{R}^c.$$

Pour $k > 0$, posons $V_k = \exp(U/k)$: c'est un voisinage ouvert de Id. On va montrer qu'il existe $k >> 0$ tel que

$$s^{-1}(0) \cap V_k = G \cap V_k.$$

Bien entendu, on a $s^{-1}(0) \cap V_k \subset G \cap V_k$.
Supposons par l'absurde que pour tout $k > 0$, il existe $g_k \in G \cap V_k$ avec $s(g_k) = p(\phi^{-1}(g_k)) \neq 0$ Autrement dit, on a

$$g_k = \exp(X_k)\exp(Y_k) \text{ avec } X_k \in \mathfrak{g} \text{ et } Y_k = s(g_k) \in \mathbf{R}^c \setminus 0.$$

Par continuité de la projection sur $\mathbf{R}^c$, la suite Y_k converge vers zéro dans $\mathbf{R}^c$ et par ailleurs

$$\exp(Y_k) = \exp(-X_k)g_k \in G.$$

Mais d'après 5.2.3, toute valeur d'adhérence de $Y_k/|Y_k|$ est un élément de $\mathfrak{g}$. Comme $\mathbf{R}^c$ est fermé (dimension finie), cette valeur d'adhérence est dans $\mathbf{R}^c$, une contradiction car $\mathbf{R}^c \cap \mathfrak{g} = \{0\}$. Ceci achève la preuve du premier point. Si maintenant H est le sous groupe de G engendré par l'exponentielle, il contient donc un voisinage de Id dans G : par homogénéité, H est ouvert. Mais alors,

$$G = H \sqcup_{H' \neq H \in G/H} H'$$

de sorte que par connexité de G, on a $G = H$. ■

Corollaire 5.3.2. — *Deux sous-groupes fermés connexes de* $\mathbf{GL}_n(\mathbf{R})$ *sont égaux si et seulement si ils ont les mêmes algèbres de Lie.*

On comprend alors l'importance de l'étude des algèbres de Lie. On ne saurait trop conseiller la lecture des superbes volumes de Bourbaki dédiés à ce sujet ([**3**],[**4**],[**5**],[**6**]).

5.4. En guise de conclusion. — Le théorème de Cartan joint avec ce que l'on a fait permet de construire des sous-groupes libres à deux générateurs de $\mathbf{SL}_2(\mathbf{R})$ qui sont... denses. En effet, on a

Proposition 5.4.1. — *Le sous-groupe L_t (cf. 4.2.1) est libre de générateurs A, B dense dès que $0 < t < 1/4$ et t transcendant par exemple.*

Preuve : Notons $\mathfrak{g}$ l'algèbre de lie de l'adhérence de L_a dans $\mathbf{SL}_2(\mathbf{R})$ (qui est certainement un sous-groupe).

a) . — Montrons déjà que L_a n'est pas discret. On calcule alors le commutateur (A, M) avec $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{R})$ et on trouve

$$(A, M) - \mathrm{Id} = \begin{pmatrix} tac + t^2c & t(1-a^2) - t^2ac \\ tc^2 & -tac \end{pmatrix}.$$

Désignons par $\|M\|$ est la norme sup de M. Supposons qu'on a $\|M - \mathrm{Id}\| \leq 1/2$. On a alors

$$|tac + t^2c| \leq (7/16)\ \|M - \mathrm{Id}\|, |t(1-a^2) - t^2ac| \leq 15/32\ \|M - \mathrm{Id}\|, |tc^2| \leq \|M - \mathrm{Id}\|\ /8 \text{ et } |-tac| \leq 3/8\ \|M - \mathrm{Id}\|,$$

et on obtient

$$\|(A, M) - \mathrm{Id}\| \leq 1/2\ \|M - \mathrm{Id}\|\ .$$

Par récurrence, on construit donc une suite de commutateurs en partant de $M_0 = B$ qui tend vers l'identité. Comme t est transcendant et donc L_t libre, aucun des termes n'est l'identité, prouvant bien que L_t non discret. Soit alors G l'adhérence de L_t. C'est un sous-groupe fermé non discret de G de sorte que son algèbre de Lie $\mathfrak{g}$ est non nulle. Observons ensuite que $\mathfrak{g}$ est invariante par conjugaison par les éléments de L_t.

b) . — Montrons que la seule sous algèbre de Lie non nulle de $\mathfrak{sl}_2(\mathbf{R})$ invariante par conjugaison sous L_t est $\mathfrak{sl}_2(\mathbf{R})$, ce qui prouvera la proposition.

On part d'une matrice non nulle

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathfrak{g}.$$

Maple affirme alors que

$$A_j = 1/j(\mathrm{Ad}(A^j).M - M) = \begin{pmatrix} c & -2a - jtc \\ 0 & c \end{pmatrix} \text{ et } B_j = 1/j(\mathrm{Ad}(B^j).M - M) = \begin{pmatrix} -b & 0 \\ 2a - jtb & b \end{pmatrix}$$

sont des éléments de $\mathfrak{g}$ pour tout $j \in \mathbf{Z}$

0. Comme $\mathfrak{g}$ est donnée par des équations polynômiales (de degré 1), c'est encore vrai si $j = 0$ (adhérence de Zariski si on veut).

En faisant $A_{j+1} - A_j$ et $B_{j+1} - B_j$, on déduit $cE_{1,2}$ et $bE_{2,1}$ dans $\mathfrak{g}$.

– Si $bc \neq 0$, on a $E_{1,2}, E_{2,1}$ et $H = E_{1,1} - E_{2,2} \in \mathfrak{g}$ et donc $\mathfrak{g} = \mathfrak{sl}_2$.

– Si $b = 0$ par exemple. Comme $A_j \in \mathfrak{g}$ pour tout j et a ou b non nul, on a $E_{1,2} \in \mathfrak{g}$. Par ailleurs $B_j = aE_{2,1} \in \mathfrak{g}$.

  – Si a est non nul, c'est terminé comme plus haut.

  – Si $a = 0$, on a $M = cE_{2,1}$ et $cE_{1,2} \in \mathfrak{g}$ et c'est terminé comme plus haut.

■

Références

[1] Armand Borel and Jacques Tits. Homomorphismes "abstraits" de groupes algébriques simples. *Ann. of Math. (2)*, 97 :499–571, 1973.

[2] N. Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 1 à 3*. Hermann, Paris, 1970.

[3] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVII : Groupes et algèbres de Lie. Chap. II : Algèbres de Lie libres. Chap. III : Groupes de Lie.* Actualites scientifiques et industrielles 1349. Paris : Hermann. 320 p. , 1972.

[4] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVIII : Groupes et algèbres de Lie. Chap. VII : Sous-algèbres de Cartan, éléments réguliers. Chap. VIII : Algèbres de Lie semi-simples deployees.* Actualites scientifiques et industrielles, 1364. Paris : Hermann. 271 p. , 1975.

[5] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres 4, 5 et 6*. Elements de Mathematique. Paris etc. : Masson. 288 p. , 1981.

[6] N. Bourbaki. *Éléments de mathématique. Groupes et algèbres de Lie, Chapitre 9 : Groupes de Lie réels compacts*. Paris etc. : Masson. 144 p., 1982.

[7] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[8] Pierre de la Harpe. *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.

[9] Jean Dieudonné. *Sur les groupes classiques*. Hermann, Paris, 1973. Troisième édition revue et corrigée, Publications de l'Institut de Mathématique de l'Université de Strasbourg, VI, Actualités Scientifiques et Industrielles, No. 1040.

[10] Claude Godbillon. *Éléments de topologie algébrique*. Hermann, Paris, 1971.

[11] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20 :250–270, 1972.

Yves Laszlo, Université Paris VI, Institut de Mathématiques, 175 boulevard du Chevaleret, 75013 Paris, France
E-mail : laslo@math.jussieu.fr