Sous-groupes finis des groupes linéaires complexes

Sergio Vega, sous la direction d'Odile Garotta

15 mai 2015

Table des matières

Introduction

Un des premiers résultats en théorie des représentations est que tout groupe fini peut, à l'aide de la représentation régulière, être réalisé comme groupe d'endomorphismes d'un k-espace vectoriel, quelque soit le corps commutatif k. Dans ce mémoire on aborde le problème inverse : étant donné un k-espace vectoriel V de dimension finie, quels sont les sous-groupes finis de $\mathrm{GL}(V)$?

Il est difficile de donner une réponse complète à cette question, c'est-à-dire d'établir une classification des sous-groupes finis de $\mathrm{GL}(V)$ pour un V fixé. Il est cependant possible dans certains cas de borner la taille de ces sous-groupes : si $k = \mathbb{Q}$ un théorème de Minkowski affirme que le cardinal des sous-groupes finis de V est borné par une constante dépendant de la dimension de V uniquement.

Si $k = \mathbb{C}$ il n'y a plus de borne sur la taille des sous-groupes finis de $\mathrm{GL}(V)$, mais ils restent soumis à une exigence de structure : un théorème de Jordan affirme que chacun de ces sous-groupes possède un sous-groupe abélien distingué d'indice borné par une constante dépendant uniquement de la dimension n de V (voir Théorème 1.1 ici pour un énoncé formel). C'est à ce théorème que nous nous intéressons dans ce mémoire.

Depuis le mémoire de 1878 où il a été énoncé et démontré par Camille Jordan, plusieurs preuves de ce théorème ont été proposées. Dans la Section 1 nous en présentons une proche de celle donnée par Frobenius dans [4], qui utilise la structure d'espace hermitien dont V peut être doté. Quelques idées de la preuve originelle de Jordan sont exposées dans la Section 3.

Encore aujourd'hui le théorème de Jordan est l'objet de recherches, celles-ci portant notamment sur la valeur optimale de la borne sur l'indice. A l'aide de la classification des groupes finis simples, M. Collins [3] a donné en 2007 une réponse définitive au problème pour $n \geqslant 71$. Les cas restants n'ont pas encore été totalement traités. Nous présentons ici, en Section 2, le cas $n = 2$.

Le lecteur a sans doute remarqué que $\mathrm{GL}(V)$ est déterminé à isomorphisme près par la dimension de V ; plus précisément, on a $\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{C})$. Le théorème de Jordan est le plus souvent énoncé pour les sous-groupes de $\mathrm{GL}_n(\mathbb{C})$. Nous prenons cependant le parti de travailler dans le cadre d'un espace vectoriel abstrait V, pour mettre en avant les propriétés géométriques des objets étudiés.

1 Structure des sous-groupes de $\mathrm{GL}(V)$

Nous commençons par montrer que tout sous-groupe fini de $\mathrm{GL}(V)$ est isomorphe à un sous-groupe (fini) du groupe unitaire $\mathrm{U}(V)$. La preuve présentée ci-dessous relève de ce qu'on appelle parfois l'astuce unitaire de Weyl.

Proposition 1.1. *Soit G un groupe fini d'endomorphismes d'un $\mathbb{C}$-espace vectoriel V de dimension finie. V peut être muni d'un produit hermitien pour lequel les éléments de G sont unitaires.*

Démonstration. Soit $\langle ., . \rangle$ un produit hermitien quelconque sur V. En posant

$$\langle x, y \rangle_G = \sum_{g \in G} \langle g(x), g(y) \rangle \quad \forall x, y \in V,$$

on définit un nouveau produit hermitien vérifiant, pour tout $h \in G$,

$$\langle h(x), h(y) \rangle_G = \sum_{g \in G} \langle gh(x), gh(y) \rangle = \sum_{g' \in G} \langle g'(x), g'(y) \rangle = \langle x, y \rangle_G.$$

□

Une conséquence de cette proposition est que les éléments d'un sous-groupe fini de $\mathrm{GL}(V)$ sont diagonalisables, car une transformation unitaire est diagonalisable dans une base orthonormée. On rappelle que des endomorphismes diagonalisables commutent deux à deux si et seulement si ils peuvent tous être diagonalisés dans une même base. Ce résultat d'algèbre linéaire — démontré en annexe, cf. Corollaire 4.1 — permet de classifier complètement les sous-groupes abéliens finis de $\mathrm{GL}(\mathbb{C}^n)$.

Proposition 1.2. *Soit V un espace vectoriel complexe de dimension n. Un groupe abélien fini G peut être plongé dans $\mathrm{GL}(V)$ si et seulement si G est un produit d'au plus n groupes cycliques.*

Démonstration. On commence par remarquer que si $e_1, e_2, \ldots, e_n$ est une base de V, le groupe des endomorphismes inversibles diagonalisables dans cette base est isomorphe à $(\mathbb{C}^*, \times)^n$: un isomorphisme est donné par $f \mapsto (f_{|\mathbb{C}e_1}, \ldots, f_{|\mathbb{C}e_n})$, en identifiant les $f_{|\mathbb{C}e_i}$, qui sont des applications linéaires sur des droites, à des scalaires.

Soit G un produit de n groupes cycliques d'ordres $m_1, m_2, \ldots, m_n$. Pour tout $k \in \mathbb{N}^*$, le groupe $\mathbb{U}_k$ des racines k-èmes de l'unité dans $\mathbb{C}$ est un groupe cyclique d'ordre k, donc G est isomorphe à $\mathbb{U}_{m_1} \times \mathbb{U}_{m_2} \times \cdots \times \mathbb{U}_{m_n}$. Ce dernier est un sous-groupe du groupe multiplicatif $(\mathbb{C}^*)^n$, qui peut être plongé dans $\mathrm{GL}(V)$ en choisissant une base $e_1, e_2, \ldots, e_n$ de V et en considérant le groupe des endomorphismes inversibles diagonalisables dans cette base.

Résumons : G est isomorphe à $\mathbb{U}_{m_1} \times \mathbb{U}_{m_2} \cdots \times \mathbb{U}_{m_n}$ qui s'injecte canoniquement dans $(\mathbb{C}^*)^n$, qu'on peut plonger à son tour dans $\mathrm{GL}(V)$. G peut donc être réalisé comme sous-groupe de $\mathrm{GL}(V)$.

Montrons que réciproquement, tout sous-groupe abélien fini de $\mathrm{GL}(V)$ est un produit d'au plus n groupes cycliques. Si G est un tel groupe les éléments de G sont simultanément diagonalisables, donc G est isomorphe à un sous-groupe de $(\mathbb{C}^*)^n$. Il nous suffit donc de montrer que les sous-groupes finis de $(\mathbb{C}^*)^n$ s'écrivent comme produit d'au plus n groupes cycliques.

Nous utiliserons pour cela résultat suivant, qui découle du théorème de la base adaptée pour les modules libres sur des anneaux principaux : tout sous-groupe de $(\mathbb{Z}^n, +)$ est de la forme $m_1\mathbb{Z}e_1 \times m_2\mathbb{Z}e_2 \times \cdots \times m_n\mathbb{Z}e_n$, avec des m_i entiers et des $e_i \in \mathbb{Z}^n$ choisis tels que $\mathbb{Z}^n = \mathbb{Z}e_1 \times \mathbb{Z}e_2 \times \cdots \times \mathbb{Z}e_n$, le produit direct étant interne. On aura surtout besoin des deux corollaires suivants : tout sous-groupe de $\mathbb{Z}^n$ est isomorphe à un certain $\mathbb{Z}^m$ avec $m \leqslant n$, et tout quotient de $\mathbb{Z}^n$ par un de ses sous-groupes est de la forme $\prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$ (certains m_i pouvant éventuellement être nuls).

Soit donc G un sous-groupe de $(\mathbb{C}^*)^n$. Comme tous les éléments de G sont d'ordre $|G|$, on a $G \subset (\mathbb{U}_{|G|})^n$. G est donc inclus dans l'image du morphisme surjectif

$$\begin{array}{rccc} \rho : & \mathbb{Z}^n & \longrightarrow & (\mathbb{U}_{|G|})^n \\ & (a_1, a_2, \ldots, a_n) & \longmapsto & (e^{2i\pi a_1/|G|}, \ldots, e^{2i\pi a_n/|G|}). \end{array}$$

L'image réciproque de G par ρ est un sous-groupe du groupe abélien libre $\mathbb{Z}^n$, et est donc isomorphe à $\mathbb{Z}^k$ pour un $k \leqslant n$. Il existe donc (quitte à composer avec la projection canonique $\mathbb{Z}^n \hookrightarrow \mathbb{Z}^k$) un morphisme surjectif

$$\rho' : \mathbb{Z}^n \to G.$$

Son noyau $\operatorname{Ker} \rho'$ est un sous-groupe additif de $\mathbb{Z}^n$: comme $G \simeq \mathbb{Z}^n / \operatorname{Ker} \rho'$, G est isomorphe à un certain $\prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$. Les m_i sont tous non nuls, puisque G est fini — mais ils peuvent être éventuellement égaux à 1, le $\mathbb{Z}/m_i\mathbb{Z}$ correspondant est alors trivial — donc G s'écrit comme un produit d'au plus n groupes cycliques. □

Remarque. On sait qu'un même groupe peut, grâce au théorème des restes chinois, s'écrire de plusieurs manières comme produit de groupes cycliques, par exemple $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Le nombre minimal de facteurs qu'il faut pour écrire un groupe abélien G est en fait le nombre de facteurs invariants donnés par le théorème de structure des groupes abéliens finis ; c'est aussi le nombre minimal de générateurs de G vu en tant que $\mathbb{Z}$-module. La proposition que nous venons de démontrer peut alors se reformuler comme suit : un groupe abélien fini G peut-être plongé dans $\mathrm{GL}(V)$ si et seulement si G a au plus n facteurs invariants.

Voici maintenant le théorème principal de cette section, dû à Camille Jordan.

Théorème 1.1 (Jordan, 1878)**.** *Soit V un $\mathbb{C}$-espace vectoriel de dimension n. Il existe un entier $D(n)$ tel que tout sous-groupe fini G de $\mathrm{GL}(V)$ admette un sous-groupe distingué et abélien H d'indice inférieur à $D(n)$, c'est-à-dire vérifiant $[G : H] \leqslant D(n)$.*

Démonstration. On commence par choisir une norme hermitienne sur V telle que les éléments de G soient unitaires, ce qui est possible en vertu de la Proposition 1.1. On munit alors $\mathrm{End}(V)$ de la norme d'opérateur subordonnée à cette norme hermitienne. Autrement dit, pour tout $f \in \mathrm{End}(V)$ on pose

$$\|f\| = \sup_{x \neq 0} \frac{\|f(x)\|}{\|x\|}.$$

Cette norme est une norme d'algèbre, et les transformations unitaires ont norme 1, puisque ces transformations préservent la norme hermitienne. Il s'ensuit que la multiplication par une transformation unitaire ne change pas la norme d'opérateur : si f est une transformation quelconque et φ est unitaire on a

$$\|f\| = \|f\|.\|\varphi\| \geqslant \|f\varphi\| = \|f\varphi\|.\|\varphi^*\| \geqslant \|f\varphi\varphi^*\| = \|f\|$$

où φ^* désigne l'adjointe de φ pour le produit hermitien de V, de sorte que $\varphi\varphi^* = \mathrm{id}_V$. On a donc bien $\|f\varphi\| = \|f\|$, et on montre de même que $\|\varphi f\| = \|f\|$.

La démonstration à proprement parler peut maintenant commencer : à quelques détails près, il s'agit de celle donnée dans [6], et l'argument donnant une valeur explicite pour $D(n)$ est celui de [1]. On considère H le sous-groupe de G engendré par l'ensemble S défini par :

$$S = \{s \in G, \|s - \mathrm{id}_V\| < 1/2\}.$$

Nous allons montrer que H vérifie les propriétés énoncées dans le théorème, c'est-à-dire que H est abélien, distingué dans G et que $[G : H] \leqslant D(n)$ avec $D(n) = 5^{2n^2} - 3^{2n^2}$.

Pour tout élément s de S, on a

$$\|gsg^{-1} - \mathrm{id}_V\| = \|g(s - \mathrm{id}_V)g^{-1}\| = \|s - \mathrm{id}_V\| < 1/2$$

quelque soit $g \in G$. Autrement dit S est stable par conjugaison avec g. Comme S génère H, il s'ensuit que $gHg^{-1} \subset H$, ce qui prouve que H est un sous-groupe distingué, puisque g est arbitraire.

Dire que deux éléments g et g' de G ne sont pas dans la même classe modulo H revient à dire que $g^{-1}g' \notin H$. En particulier, $\|g^{-1}g' - \mathrm{id}_V\| \geqslant 1/2$. Donc si $\{g_k, k \in K\}$ est un système de représentants de G modulo H, on a $\|g_k - g_{k'}\| \geqslant 1/2$ pour tout $k \neq k'$. Les boules ouvertes $B(g_k, 1/4)$, $k \in K$ sont donc disjointes.

Identifions $\mathrm{End}(V)$ à $\mathbb{R}^{2n^2}$ par le choix d'une $\mathbb{R}$-base quelconque : comme nous sommes en dimension finie, les boules ouvertes de la norme d'opérateur sont des ouverts bornés pour la nouvelle norme euclidienne. En particulier elles ont un volume positif et fini, proportionnel à la puissance $2n^2$-ème de leur rayon d'après les propriétés de la mesure de Lebesgue : pour tout $x \in \mathrm{End}(V), r \in \mathbb{R}^+$ on a

$$\mathrm{Vol}(B(x, r)) = \mathrm{Vol}(h_r(B(x, 1))) = r^{2n^2}\mathrm{Vol}(B(x, 1)) = r^{2n^2}\mathrm{Vol}(B(0, 1)),$$

h_r désignant l'homothétie de centre x et rapport r.

On peut donc, en utilisant le fait que les boules $B(g_k, 1/4)$ sont disjointes, écrire l'inégalité suivante,

$$\begin{aligned}\kappa \mathrm{Card}(K)(1/4)^{2n^2} &= \sum_{k\in K} \mathrm{Vol}(B(g_k, 1/4)) \\ &= \mathrm{Vol}(\bigcup_{k\in K} B(g_k, 1/4)) \\ &\leqslant \mathrm{Vol}(B(0,5/4) \setminus B(0,3/4)) \\ &= \kappa(5/4)^{2n^2} - \kappa(3/4)^{2n^2},\end{aligned}$$

où κ est le volume de la boule unité pour la norme d'opérateur. Il s'ensuit que $[G : H] \leqslant 5^{2n^2} - 3^{2n^2}$, puisque $\mathrm{Card}(K) = [G : H]$.

Il reste encore à montrer que H est abélien. Voici une esquisse de la démarche suivie : d'abord nous nous ramenons au cas où H agit irréductiblement sur V, c'est-à-dire où H ne fixe aucun sous-espace propre non trivial de V, puis nous montrons que le centre de H est alors constitué d'homothéties. Une propriété des commutateurs multiplicatifs — à savoir que le commutateur de deux endormorphismes proches de l'identité est encore plus proche de l'identité — permet alors de conclure.

Procédons : grâce au théorème de Maschke, on peut décomposer V en somme directe d'espaces $V_i, i \in I$ stables par H, de telle sorte que H agit irréductiblement sur chacun des V_i. Puisque les V_i sont stables par H, on peut définir, pour tout $i \in I$, le morphisme de restriction

$$\begin{aligned} r_i \colon H &\longrightarrow \mathrm{GL}(V_i) \\ h &\longmapsto h_{|V_i}. \end{aligned}$$

Notons H_i l'image de H par r_i, qui est un groupe fini de transformations unitaires de V_i. Pour montrer que H est abélien il nous suffit de montrer que chaque H_i l'est. En effet, pour tout $h, h' \in H$

$$h = \bigoplus_{i\in I} r_i(h), \quad h' = \bigoplus_{i\in I} r_i(h'),$$

et donc

$$hh' = \bigoplus_{i\in I} r_i(h)r_i(h') = h'h$$

si les restrictions commutent [1].

Tout élément s de S vérifie $\|s(x) - x\| < \|x\|/2$ quelque soit $x \in V$, par définition de S et de la norme d'opérateur. En considérant cette inégalité seulement pour $x \in V_i$, on voit que $\|r_i(s) - \mathrm{id}_{V_i}\| < 1/2$. Pour tout $i \in I$, H_i est donc engendré par l'ensemble S_i défini par

$$S_i = \{s \in H_i, \|s - \mathrm{id}_{V_i}\| < 1/2\},$$

puisque S_i contient $r_i(S)$ et que $r_i(S)$ engendre H_i.

1. On rappelle que la somme directe de deux endomorphismes φ_E et φ_F définis sur E et F respectivement est l'endomorphisme de $E \oplus F$ donné par $(\varphi_E \oplus \varphi_F)(x_E + x_F) = \varphi_E(x_E) + \varphi_F(x_F)$.

Fixons i et considérons $Z(H_i)$ le centre de H_i. Un élément $z \in H_i$ appartient à $Z(H_i)$ si et seulement $zh = hz$ pour tout $h \in H_i$: autrement dit z appartient au centre de H_i si et seulement si z est un automorphisme de la représentation (V_i, r_i) de G. Comme cette représentation est irréductible, on peut appliquer le lemme de Schur : $Z(H_i)$ est l'ensemble des homothéties de $\mathrm{End}(V_i)$ appartenant à H_i.

Supposons par l'absurde que H_i ne coïncide pas avec son centre $Z(H_i)$. Il existe alors, puisque l'ensemble est fini, un élément $x \in H_i \setminus Z(H_i)$ pour lequel $\|x - \mathrm{id}_{V_i}\|$ est minimal. Regardons les commutateurs de x avec les éléments de S_i. On a, pour tout $s \in S_i$,

$$\begin{aligned}
\|xsx^{-1}s^{-1} - \mathrm{id}_{V_i}\| &= \|xs - sx\| \\
&= \|(x - \mathrm{id}_{V_i})(s - \mathrm{id}_{V_i}) - (s - \mathrm{id}_{V_i})(x - \mathrm{id}_{V_i})\| \\
&\leqslant \|(x - \mathrm{id}_{V_i})\|.\|(s - \mathrm{id}_{V_i})\| + \|(s - \mathrm{id}_{V_i})\|.\|(x - \mathrm{id}_{V_i})\| \\
&< \|x - \mathrm{id}_{V_i}\|.
\end{aligned}$$

Par choix de x, cela n'est possible que si $xsx^{-1}s^{-1}$ est une homothétie, dont on note le rapport λ. Mais alors

$$\lambda \,\mathrm{Tr}(s) = \mathrm{Tr}(xsx^{-1}) = \mathrm{Tr}(x^{-1}xs) = \mathrm{Tr}(s)$$

d'où $\mathrm{Tr}(s) = 0$ ou $\lambda = 1$. Mais comme $\|s - \mathrm{id}_{V_i}\| < 1/2$, les valeurs propres de s sont à distance au plus $1/2$ de 1 ; elles sont donc en particulier de partie réelle strictement positive. On ne peut donc pas avoir $\mathrm{Tr}(s) = 0$, et on a $\lambda = 1$, autrement dit $xsx^{-1}s^{-1} = \mathrm{id}_{V_i}$ et x et s commutent.

Ainsi x commute avec chacun des $s \in S_i$, donc x commute avec tous les éléments de H_i, ce qui contredit le choix $x \in H_i \setminus Z(H_i)$. On a donc $Z(H_i) = H_i$, les H_i sont tous abéliens (en fait $\dim V_i = 1$) et H l'est donc aussi. □

On peut se demander quelle est la valeur optimale $\underline{D}(n)$ de $D(n)$, c'est-à-dire quel est la plus petite valeur de $D(n)$ telle que la conclusion du théorème de Jordan soit vraie. Il est assez facile de voir que $\underline{D}(n) \geqslant (n+1)!$ pour $n \geqslant 4$, car le groupe symétrique S_{n+1} n'a pas de sous-groupes abéliens distingués non triviaux (Corollaire 4.2) et peut être représenté fidèlement dans $\mathbb{C}^n$ par la représentation standard. M. Collins a montré dans [3] qu'en fait $\underline{D}(n) = (n+1)!$ pour $n \geqslant 71$.

2 Le cas $n = 2$

Pour les petites valeurs de n il est possible d'avoir $(n+1)! < \underline{D}(n)$. Nous allons montrer que $\underline{D}(2) = 60$ en utilisant la classification des sous-groupes de $\mathrm{SO}(\mathbb{R}^3)$ pour obtenir des informations sur les sous-groupes finis de $\mathrm{GL}(\mathbb{C}^2)$.

Proposition 2.1. *Soit V un $\mathbb{C}$-espace vectoriel de dimension 2 et G un sous-groupe fini de $\mathrm{GL}(V)$. L'ensemble Z des homothéties appartenant à G forme un sous-groupe distingué de G et G/Z est soit :*

- *un groupe cyclique*
- *un groupe diédral d'ordre $2m$ pour $m \geqslant 2$*
- *le groupe des isométries directes d'un polyèdre régulier, c'est à dire A_4, S_4 ou A_5.*

Réciproquement, tous les groupes décrits ci-dessus sont réalisés comme quotient d'un sous-groupe fini G de $\mathrm{GL}(V)$ par le groupe Z de ses homothéties. On peut montrer à partir de ces résultats que $\underline{D}(2) = 60$.

Démonstration. On admet la classification des sous-groupes finis de $\mathrm{SO}(\mathbb{R}^3)$: ce sont exactement les groupes cycliques, diédraux et les groupes des rotations d'un polyèdre régulier. La démonstration se base sur l'étude de l'action de ces groupes sur les droites vectorielles de $\mathbb{R}^3$: nous renvoyons le lecteur à [7]. Précisons tout de même quels groupes correspondent à quels polyèdres réguliers : A_4 est le groupe des rotations du tétraèdre, S_4 celui du cube et de l'octaèdre (qui sont duaux l'un de l'autre), et A_5 est celui de l'icosaèdre et du dodécaèdre.

Le premier sujet d'agrégation de 2003, dont nous nous sommes inspirés pour cette preuve, montre que $\underline{D}(2) = 60$ en évitant d'utiliser cette classification. A la place on raisonne sur l'action des éléments de G sur les droites de V, mais cette méthode donne moins d'informations sur G/Z.

Soit G un sous-groupe fini de $\mathrm{GL}(V)$ et Z le sous-groupe de ses homothéties : comme dans la preuve du théorème de Jordan, on choisit un produit hermitien sur V pour lequel les éléments de G sont unitaires. C'est possible, on le rappelle, grâce à la Proposition 1.1. Soit $\mathrm{U}(V)$ le groupe unitaire de V. On note $\mathrm{PU}(V)$ le groupe projectif unitaire, c'est-à-dire le groupe quotient de $\mathrm{U}(V)$ par le sous-groupe $Z(V)$ de ses homothéties : $Z(V)$ est bien un sous-groupe distingué car il est inclus dans le centre de $\mathrm{U}(V)$. Puisque V est de dimension 2, $\mathrm{U}(V)$ est isomorphe à $U_2(\mathbb{C})$, comme on le voit en fixant une base orthonormée de V et en associant à $f \in \mathrm{U}(V)$ sa représentation matricielle dans cette base. On peut donc appliquer la Proposition 4.2 de l'annexe : $\mathrm{PU}(V)$ est isomorphe à $\mathrm{SO}(\mathbb{R}^3)$.

L'image de G par le morphisme quotient $\varphi : \mathrm{U}(V) \to \mathrm{PU}(V)$ s'identifie à G/Z par factorisation du morphisme $\varphi_{|G}$. Le quotient G/Z est donc isomorphe à un sous-groupe fini de $\mathrm{SO}(\mathbb{R}^3)$.

Réciproquement, soit H un sous-groupe fini quelconque de $\mathrm{SO}(\mathbb{R}^3)$: montrons que H est isomorphe au quotient d'un sous-groupe fini G de $\mathrm{SU}(V)$ par le groupe de ses homothéties. Soit $\rho : \mathrm{SU}(V) \to \mathrm{SO}(\mathbb{R}^3)$ le morphisme de noyau $\{\pm \mathrm{id}_V\}$ décrit par la Proposition 4.2. Alors $G = \rho^{-1}(H)$ est un sous-groupe fini de cardinal $2|H|$, car $\operatorname{Ker}\rho = \{\pm \mathrm{id}_V\}$. De plus le sous-groupe Z des homothéties de G est exactement $\operatorname{Ker}\rho$, donc par le premier théorème d'isomorphisme $G/Z \simeq H$, ce qu'on voulait démontrer.

Intéressons-nous au cas où H est le groupe des isométries directes de l'icosaèdre régulier : $\rho^{-1}(H)$ est alors un sous-groupe à 120 éléments de $\mathrm{SU}(V)$. L'image de tout sous-groupe distingué de $\rho^{-1}(H)$ est un sous-groupe distingué de H, or celui-ci est simple car isomorphe à A_5 (voir Théorème 4.1 pour la simplicité de A_5), donc le seul sous-groupe non trivial, abélien et distingué de $\rho^{-1}(H)$ est $\{\pm \mathrm{id}_V\}$. L'exemple de ce groupe $\rho^{-1}(H)$ montre que $\underline{D}(2)$ vaut au moins 60.

Il reste à montrer que G admet un sous-groupe abélien distingué d'indice au plus 60, pour pouvoir conclure que $\underline{D}(2) = 60$. C'est le cas si G/Z est isomorphe au groupe des rotations d'un polyèdre régulier, car alors Z est un sous-groupe distingué abélien de G et $[G : Z]$ vaut 12,24 ou 60 (selon le polyèdre dont il s'agit). On peut donc supposer que G/Z est un groupe cyclique ou diédral.

G/Z contient alors un sous-groupe distingué cyclique d'indice au plus 2, que nous notons H' : posons $G' = \varphi^{-1}_{|G}(H')$, φ désignant toujours le morphisme quotient $\mathrm{U}(V) \to \mathrm{PU}(V)$. Comme G' contient Z, le troisième théorème d'isomor-

phisme nous dit que G'/Z est un sous-groupe distingué de G/Z et que G/G' est isomorphe à $(G/Z)/(G'/Z)$. Puisque $G'/Z = \varphi_{G'}(G') = H'$, on a $[G : G'] \leqslant 2$.

Il suffit maintenant de montrer que G' est abélien. Soit $a \in H'$ un générateur de H' et $b \in G'$ un de ses antécédents par $\varphi_{|G}$. Alors $\varphi(b^k) = a^k$ pour tout $k \in \mathbb{N}$. On a donc

$$G' = \varphi_{|G}^{-1}(H') = \bigcup_{k\in\mathbb{N}} b^k Z,$$

Z étant le noyau de $\varphi_{|G}$. Deux éléments quelconques g'_1, g'_2 de G' peuvent donc toujours s'écrire sous la forme $g'_1 = b^{k_1} z_1$ et $g'_2 = b^{k_2} z_2$: on a alors $g'_1 g'_2 = b^{k_1+k_2} z_1 z_2 = g'_2 g'_1$, car Z est inclus dans le centre de G. Le groupe G' est donc abélien. □

Remarque. Il était important pour la fin de la preuve que le sous-groupe distingué abélien H' de $\varphi(G)$ fût cyclique, car il se peut en général que l'image réciproque d'un groupe abélien par $\varphi_{|G}$ ne soit pas abélienne. C'est instructif d'essayer de le démontrer pour voir où se situe l'obstruction à la preuve, puis de construire un exemple, comme celui donné par le sous-groupe de $\mathrm{U}_2(\mathbb{C})$ à 8 éléments

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\}$$

qui n'est pas commutatif (il est isomorphe à D_4) mais dont l'image par quotient dans $\mathrm{PU}(V)$ est isomorphe au groupe de Klein $D_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remarque. On rappelle que G est une extension de N par H s'il existe une suite exacte

$$1 \to N \to G \to H \to 1$$

ou de manière équivalente si G admet un sous-groupe distingué N_G isomorphe à N tel que G/N_G est isomorphe à H. Le problème de l'extension consiste à trouver toutes les extensions de N par H. Il est possible qu'une telle extension G ne soit ni le produit direct, ni même le produit semi-direct de N et H, comme le montre encore l'exemple de D_4.

En effet, la restriction du morphisme canonique $\mathrm{U}(V) \to \mathrm{PU}(V)$ au groupe de matrices présenté dans la remarque précédente est un morphisme $D_4 \to D_2$ dont le noyau est isomorphe à $\mathbb{Z}/2\mathbb{Z}$: D_4 est donc par définition une extension de $\mathbb{Z}/2\mathbb{Z}$ par D_2. Mais D_4 ne peut pas s'écrire comme produit semi-direct $\mathbb{Z}/2\mathbb{Z} \rtimes D_2$: le groupe d'automorphismes de $\mathbb{Z}/2\mathbb{Z}$ étant trivial, un tel produit est nécessairement direct, et D_4 n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times D_2$ puisque D_4 n'est pas abélien.

A cause de ce problème d'extension, la proposition 2.1 s'avère insuffisante telle quelle pour classifier tous les sous-groupes de $\mathrm{GL}(\mathbb{C}^2)$.

Un autre exemple d'extension non-directe de $\mathbb{Z}/2\mathbb{Z}$ par D_2 est donné par le groupe des quaternions $\mathbb{H}_8$, qui peut être défini comme le groupe de matrices

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\},$$

et est donc réalisé comme sous-groupe de $\mathrm{GL}(\mathbb{C}^2)$. Le groupe $\mathbb{H}_8$ est une extension de D_2 par $\mathbb{Z}/2\mathbb{Z}$, qui n'est pas isomorphe à $D_2 \times \mathbb{Z}/2\mathbb{Z}$, ni à D_4, comme

on peut le voir en comptant le nombre d'éléments d'ordre 2 dans chacun de ces trois groupes.

Remarquons que, d'après la Proposition 1.2, $\mathbb{Z}/2\mathbb{Z} \times D_2 \simeq (\mathbb{Z}/2\mathbb{Z})^3$ ne peut pas être plongé dans $\mathrm{GL}_2(\mathbb{C})$, puisqu'il ne peut pas s'écrire comme produit de deux groupes cycliques. Parmi les trois extensions de $\mathbb{Z}/2\mathbb{Z}$ par D_2 que nous avons vues (ce sont en réalité toutes les extensions possibles), seules les extensions non-directes peuvent être réalisées comme sous-groupes de $\mathrm{GL}_2(\mathbb{C})$.

3 La preuve originelle de Jordan

Dans cette section nous présentons quelques idées de la preuve que Jordan avait initialement donnée de son théorème, qu'on peut trouver présentée en un langage moderne dans [2]. Elle repose sur la notion de M-faisceau et de tore de racines. ces termes ne sont pas utilisés ailleurs dans la littérature contemporaine ; le premier est celui qu'avait employé Jordan et n'a pas ici le sens qu'il a en géométrie algébrique.

Définition 3.1 (Tore de racines, faisceau)**.** Soit V un espace vectoriel complexe et A un sous-groupe abélien fini de $\mathrm{GL}(V)$ d'espaces propres $V_i, i \in I$. Sur les *espaces propres d'un ensemble fini d'endomorphismes*, nous invitons le lecteur à regarder la Définition 4.1 et la Proposition 4.1.

Le *tore de racines* S des V_i est le groupe des endomorphismes de $\mathrm{GL}(V)$ dont les restrictions aux V_i sont des homothéties. Pour tout $i \in I$ et $s \in S$, on note $\lambda_i(s)$ l'unique scalaire tel que $\lambda_i(s)\,\mathrm{id}_{V_i} = s_{|V_i}$.

Soit $M \geqslant 2$ un entier. On dit que A est *un M-faisceau* lorsque, pour tout $i, j \in I$, $i \neq j$, l'ensemble $\{\lambda_i(a)/\lambda_j(a) \mid a \in A\}$ a au moins M éléments.

Il est utile pour l'étude des M-faisceaux d'introduire (en gardant les notations employées ci-dessus) les morphismes de groupes

$$\begin{aligned} \varphi_{i,j} \colon A &\to \mathbb{C}^* \\ a &\mapsto \lambda_i(a)/\lambda_j(a). \end{aligned}$$

On remarque que A est un M-faisceau si et seulement si $\mathrm{Im}\,\varphi_{i,j}$ a au moins M éléments pour tous indices $i, j \in I$ distincts. On peut penser aux $\varphi_{i,j}$ de la manière suivante : A agit sur les droites de V, c'est-à-dire sur l'espace projectif $\mathbb{P}V$, et les $\varphi_{i,j}$ décrivent cette action de A en termes de coordonnées projectives. Ce point de vue se trouve illustré dans la démonstration des deux lemmes suivants, qui proposent des caractérisations alternatives des M-faisceaux.

Lemme 3.1. *Un groupe abélien fini d'endomorphismes A est un M-faisceau si et seulement si l'orbite d'une droite de V par action de A contient, ou bien un seul élément, ou bien au moins M éléments.*

Démonstration. On commence par montrer le sens suivant : si A est un M-faisceau, l'orbite de toute droite d de $\mathbb{P}V$ est soit réduite à d, soit contient au moins M éléments. Si $v \in V$ est un vecteur directeur de d, on peut écrire v sous la forme $v = \sum v_i$ avec des $v_i \in V_i$, de sorte que $a(v) = \sum \lambda_i(a) v_i$ pour tout $a \in A$. Par unicité de cette écriture, on voit que pour $a, a' \in A$, $a(v)$ et $a'(v)$ ne peuvent être colinéaires que si le quotient $\lambda_i(a)/\lambda_i(a')$ ne dépend pas de $i \in I_1$,

I_1 étant l'ensemble des $i \in I$ tels que v_i soit non nul. En particulier, on doit avoir $\varphi_{i,j}(a) = \varphi_{i,j}(a')$ pour tous $i, j \in I_1$.

Deux cas peuvent donc se présenter : ou bien deux vecteurs v_i, v_j sont non nuls, et $\{a(v) \mid a \in A\}$ contient au moins $\varphi_{i,j}(A)$ vecteurs deux à deux non-colinéaires, ou bien v est un vecteur propre de A et la droite dirigée par v est stable par action de A. Mais comme A est un M-faisceau, $|\operatorname{Im}\varphi_{i,j}| \geqslant M$ pour tous $i \neq j$: l'orbite de d contient donc plus M éléments dans le premier cas, et un seul dans le second.

Réciproquement, montrons que si l'orbite de chaque droite non fixée par action de A contient au moins M éléments, A est un M-faisceau. Si v_i, v_j sont deux vecteurs non-nuls de deux espaces propres distincts V_i, V_j, $v_i + v_j$ n'est pas un vecteur propre de A et par hypothèse l'orbite de $\mathbb{C}(v_i + v_j)$ contient au moins M vecteurs pour tous $i, j \in I$ différents. On vérifie facilement que $a(v_i + v_j)$ et $a'(v_i + v_j)$ sont colinéaires si et seulement si $\varphi_{i,j}(a) = \varphi_{i,j}(a')$, donc $\varphi_{i,j}(A)$ a au moins M éléments. Ainsi pour tous i, j distincts $\operatorname{Im}\varphi_{i,j}$ contient au moins M éléments, et A est donc bien un M-faisceau. □

Lemme 3.2. *Un sous-groupe abélien fini A de $\mathrm{GL}(V)$ est un M-faisceau si et seulement si les groupes $A^m, m < M$ ont les mêmes espaces propres, A^m désignant le groupe $\{a^m \mid a \in A\}$.*

Démonstration. Rappelons d'abord pourquoi A^m est un groupe : l'application $a \mapsto a^m$ est un morphisme car A est abélien, et A^m est l'image de A par ce morphisme.

On note toujours $V_i, i \in I$ les espaces propres de A. Supposons que A soit un M-faisceau. Soit v un vecteur et $m < M$: montrons que v est un vecteur propre de G^m si et seulement si v appartient à l'un des V_i. Comme dans la preuve du lemme précédent, on écrit v sous la forme $\sum v_i$ avec $v_i \in V_i$ pour tout i. Si v appartient à l'un des V_i, alors v est un vecteur propre de A et donc de A^m. Sinon, au moins deux vecteurs v_i, v_j de la somme sont non nuls. Comme $\operatorname{Im}\varphi_{i,j}$ a au moins M éléments il existe un $a \in A$ tel que $\varphi_{i,j}(a)^m \neq 1$. $a^m(v)$ ne peut pas être alors colinéaire à v, car on aurait

$$a^m(v) = \sum \lambda v_i = \sum \lambda_i(a^m) v_i,$$

pour un certain $\lambda \in \mathbb{C}$, d'où, par unicité de cette écriture, $\lambda = \lambda_i(a^m) = \lambda_j(a^m)$ ce qui contredit $\varphi_{i,j}(a^m) \neq 1$. Donc si v n'appartient pas à l'union des V_i, v n'est pas un vecteur propre de A^m.

Réciproquement, montrons que si A n'est pas un M-faisceau il existe m et v tels que v soit un vecteur propre de A^m, mais v n'appartienne à aucun des V_i. Puisque A n'est pas un M-faisceau il existe $i, j \in I$ distincts tels que $\operatorname{Im}\varphi_{i,j}$ ait moins de M éléments. Posons $m = |\operatorname{Im}\varphi_{i,j}|$: par théorème de Lagrange, $\varphi_{i,j}(a^m) = \varphi_{i,j}(a)^m = 1$ pour tout $a \in A$. Soit v_i, v_j deux vecteurs non nuls de V_i et V_j respectivement. Leur somme v n'appartient à aucun des $V_i, i \in I$, mais pourtant

$$a^m(v) = \lambda_i(a)^m(v_i) + \lambda_j(a)^m(v_j) = \lambda_i(a)^m(v),$$

quelque soit $g \in G$. □

Ces deux caractérisations des M-faisceaux ont l'avantage de ne pas faire intervenir leurs espaces propres. Ils permettent par exemple de prouver le corollaire suivant, plus difficile à obtenir avec la définition initiale des M-faisceaux.

Corollaire 3.1. *Si deux M-faisceaux F et F' commutent alors FF' est aussi un M-faisceau.*

Démonstration. Comme F et F' commutent, FF' est un groupe. D'après le Lemme 3.1 il nous suffit de vérifier que l'orbite d'une droite d non stable par action de FF' a au moins M éléments. Une telle droite ne peut pas être stable à la fois par F et F', sans restreindre la généralité, on peut donc supposer que d n'est pas stable par F. Comme F est un M-faisceau, l'orbite de cette droite a au moins M éléments par action de F, donc au moins M éléments par action de FF'. □

Dans la suite on s'intéresse aux faisceaux contenus dans un sous-groupe fini G de $\mathrm{GL}(V)$ fixé : on dira que F est un M-faisceau de G si F est à la fois un M-faisceau et un sous-groupe de G. Remarquons que G possède toujours un M-faisceau, quelque soit $M \geqslant 2$, à savoir le faisceau trivial.

C'est la version suivante du Théorème 1.1 que Jordan a énoncée et démontrée dans son *Mémoire sur les équations différentielles linéaires à intégrale algébrique*.

Théorème 3.1. *Pour tout $n \in \mathbb{N}^*$ il existe des entiers M, N ayant la propriété suivante. Pour tout espace vectoriel complexe V de dimension n et tout sous-groupe fini G de $\mathrm{GL}(V)$, G admet un unique M-faisceau maximal (au sens de l'inclusion) et celui-ci est d'indice au plus N dans G.*

Le M-faisceau maximal H du Théorème 3.1 est nécessairement distingué, car pour tout $g \in G$ gHg^{-1} est aussi un M-faisceau maximal (d'espaces propres $g(V_i), i \in I$) donc $gHg^{-1} = H$ par unicité de H. Comme H est aussi abélien, en prenant $D(n) = N$ on voit que le théorème précédent implique le Théorème 1.1, avec une précision supplémentaire sur la forme du sous-groupe abélien distingué, mais sans borne explicite pour son indice.

Dans le cas où G est abélien, l'unique M-faisceau maximal ne coïncide pas forcément avec G. On a cependant le résultat suivant.

Lemme 3.3. *Soit A un sous-groupe abélien fini de $\mathrm{GL}(V)$, $M \geqslant 2$ un entier et F un M-faisceau maximal de A. Alors $[A : F] \leqslant (M-1)^{n-1}$, n étant la dimension de V.*

Démonstration. On garde les notations en vigueur dans cette section ; en particulier les espaces propres de A sont notés $V_i, i \in I$. Nous allons procéder par récurrence sur k le cardinal de I, l'hypothèse de récurrence étant que $[A : F] \leqslant (M-1)^{k-1}$. Si $k = 1$ alors A est un groupe d'homothéties et en particulier A est un M-faisceau : tout M-faisceau maximal F de A est donc égal à A tout entier et on a bien $[A : F] = 1 = (M-1)^{k-1}$.

On suppose la propriété vraie pour $k \leqslant l$; supposons que I ait $l+1$ éléments et soit F un M-faisceau maximal de A.

Si pour tous $i, j \in I$ distincts on a $|\varphi_{i,j}(A)| \geqslant M$, A est par définition un M-faisceau : on a alors $F = A$ et $[A : F] \leqslant (M-1)^l$ pour tout M-faisceau maximal F.

Sinon, il existe i, j distincts dans I tels que $|\varphi_{i,j}(A)| \leqslant M-1$. Pour tout M-faisceau maximal F on a alors $|\varphi_{i,j}(F)| = 1$: autrement pour tout couple de vecteurs non nuls $(v_i, v_j) \in V_i \times V_j$ l'orbite de la droite $\mathrm{Vect}(v_i + v_j)$ par action de F aurait moins de M éléments sans pour autant être un point fixe, ce qui contredirait le Lemme 3.1. Ainsi $F \subset \mathrm{Ker}\,\varphi_{i,j}$. Le groupe abélien $\mathrm{Ker}\,\varphi_{i,j}$ a au

plus l sous-espaces propres, à savoir $V_i \oplus V_j$ et les autres espaces propres de A, certains d'entre-eux éventuellement regroupés. Par hypothèse de récurrence on a donc $[\operatorname{Ker} \varphi_{i,j} : F] \leqslant (M-1)^{l-1}$ et comme $A/\operatorname{Ker} \varphi_{i,j} \simeq \varphi_{i,j}(A)$, on a aussi $[A : \operatorname{Ker} \varphi_{i,j}] \leqslant M-1$ et par conséquent $[A : F] \leqslant (M-1)^l$. □

On ne donnera pas la preuve directe du Théorème 3.1, et on renvoie de nouveau le lecteur intéressé à [2]. En voici tout de même la trame : on raisonne par récurrence sur n ; on montre avec l'hypothèse de récurrence que pour M assez grand les centralisateurs des éléments de G contiennent chacun un unique M-faisceau maximal ; on écrit alors une équation de classe pour les éléments de G selon les propriétés du M-faisceau associé, puis l'analyse de cette équation montre que si M est assez grand elle ne peut admettre de solutions que si G admet un unique M-faisceau maximal.

On se contentera ici de déduire le Théorème 3.1 du Théorème 1.1 : il nous suffit pour cela de démontrer la proposition suivante.

Proposition 3.1. *Soit V un espace vectoriel complexe de dimension finie, G un sous-groupe fini de $\mathrm{GL}(V)$ et H un sous-groupe abélien distingué de G d'indice N. Alors pour tout $M > N$, G contient un unique M-faisceau maximal F pour lequel $[G : F] \leqslant N(M-1)^{n-1}$.*

Démonstration. Gardons les notations de l'énoncé : on note de plus $V_i, i \in I$ les espaces propres de H et S le tore des racines associé aux V_i.

Pour montrer qu'il existe un unique M-faisceau maximal, il suffit de montrer que tous les M-faisceaux de G commutent. En effet, si tel est le cas et F, F' sont deux M-faisceaux maximaux, FF' est également un M-faisceau et on a $F = FF' = F'$ par maximalité.

Nous allons montrer que tout M-faisceau est inclus dans $S \cap G$, il s'ensuivra que tous les M-faisceaux commutent comme sous-groupes du groupe abélien $S \cap G$.

Soit F un M-faisceau de G. Comme H est distingué dans G, le deuxième théorème d'isomorphisme nous dit que $H \cap F$ est distingué dans F et que

$$F/(F \cap H) \simeq FH/H.$$

Soit m l'ordre du groupe $F/(F \cap H)$ et π le morphisme quotient $F \to F/(F \cap H)$. On a $f^m \in H$ pour tout $f \in F$: en effet, $f \in H$ si et seulement si $f \in \operatorname{Ker} \pi$, et par théorème de Lagrange on a $\pi(f^m) = \pi(f)^m = 1_{F/(F \cap H)}$ quelque soit $f \in F$. Par ailleurs,

$$m = [F : F \cap H] = [FH : H] \leqslant [G : H] = N < M.$$

Ces deux propriétés mises ensemble permettent de prouver que $F \subset S$: le Lemme 3.2 appliqué au groupe F^m montre qu'il a les mêmes espaces propres que F. Comme F^m est inclus dans H, chaque V_i est inclus dans un espace propre de F^m, donc dans un espace propre de F. Il s'ensuit que les restrictions des éléments de F aux V_i sont des homothéties, c'est-à-dire que F est inclus dans le tore de racines S.

Désormais F désigne l'unique M-faisceau maximal de G : il nous reste à borner l'indice $[G : F]$. On peut écrire

$$[G : F] = [G : S \cap G][S \cap G : F].$$

Comme $H \subset S \cap G$, on a $[G : S \cap G] \leqslant N$; comme $S \cap G$ est abélien et F y est encore maximal, on peut appliquer le Lemme 3.3 qui donne $[S \cap G : F] \leqslant (M-1)^{n-1}$. Il s'ensuit bien $[G : F] \leqslant N(M-1)^{n-1}$, ce qui conclut la démonstration. □

Le Théorème 3.1 s'obtient alors à l'aide du Théorème 1.1 en prenant $N = D(n)$ et $M = N + 1$ dans l'énoncé précédent : tout sous-groupe abélien fini de $\mathrm{GL}(V)$ contient un unique $D(n)$-faisceau maximal d'indice au plus $D(n)^n$.

4 Annexe

4.1 Espaces propres d'un ensemble fini d'endomorphismes

Soit V un espace vectoriel de dimension finie, sur un corps commutatif quelconque k. On rappelle que l'espace propre d'un endomorphisme f associé au scalaire $\lambda \in k$ est $\mathrm{Ker}(f - \lambda \,\mathrm{id}_V)$. Les espaces propres non triviaux de f sont toujours en nombre fini et en somme directe, et f est diagonalisable si et seulement si leur somme est l'espace V tout entier.

Etant donné un ensemble fini F d'endomorphismes, un vecteur $v \in V$ est un vecteur propre de chacun des endomorphismes de F si et seulement si v appartient à une intersection de la forme $\bigcap_{f \in F} \mathrm{Ker}(f - \lambda_f \,\mathrm{id}_V)$, ce qui justifie la définition suivante.

Définition 4.1. On appelle espaces propres d'un ensemble fini F d'endomorphismes les espaces non triviaux de la forme $\bigcap_{f \in F}(\mathrm{Ker}\, f - \lambda_f \,\mathrm{id}_V)$. Leur réunion est exactement l'ensemble des $v \in V$ qui sont des vecteurs propres de tous les $f \in F$.

Comme dans le cas d'un endomorphisme seul, les espaces propres de F sont en nombre fini. Ils sont aussi en somme directe, comme le montre une récurrence aisée que nous ne détaillerons pas, la Proposition 4.1 traitant le seul cas envisagé dans le corps du mémoire.

On peut se demander quand est-ce que la somme de ces espaces propres est V. Pour que cela soit possible, il faut déjà que chacun des endomorphismes de V soit diagonalisable, car la somme des espaces propres de chaque $f \in F$ contient la somme des espaces propres de F. Si on suppose que les éléments de F sont diagonalisables, la proposition suivante donne une condition nécessaire et suffisante pour que V soit engendré par les espaces propres de F.

Proposition 4.1. *Soit F un ensemble fini d'endomorphismes diagonalisables : la somme des espaces propres de F est V si et seulement si les éléments de F commutent deux à deux. Cette somme est alors directe.*

Le lecteur familier avec la théorie des représentations linéaires de groupes finis peut remarquer que, dans le cas où F est un groupe abélien fini, les espaces propres de F sont exactement les composantes isotypiques de la représentation $F \hookrightarrow \mathrm{GL}(V)$.

Pour la preuve de la proposition nous aurons besoin d'un résultat assez connu sur les projections. On rappelle qu'un endomorphisme f est une projection si et seulement si $f^2 = f$, et que f est alors la projection sur $\operatorname{Im} f$ le long de $\operatorname{Ker} f$.

Lemme 4.1. *Soit $p, q \in \operatorname{End}(V)$ deux projections. Si p et q commutent alors pq est la projection sur $\operatorname{Im} p \cap \operatorname{Im} q$ le long de $\operatorname{Ker} p + \operatorname{Ker} q$.*

Démonstration. Commençons par rappeler une propriété des projecteurs : $\operatorname{Im} p$ est l'ensemble des points fixes de p. En effet, si $x = p(y)$, alors $p(x) = p^2(y) = p(y) = x$, et réciproquement $x = p(x)$ implique $x \in \operatorname{Im} p$.

Comme p et q commutent, on a $(pq)^2 = pqpq = ppqq = p^2q^2 = pq$, donc pq est bien une projection.

Déterminons son image : si $x \in \operatorname{Im} p \cap \operatorname{Im} q$ alors $pq(x) = p(q(x)) = p(x) = x$ donc x appartient à l'image de pq. Réciproquement si $x \in \operatorname{Im} pq$ alors $x = pq(x) = p^2q(x) = p(pq(x)) = p(x)$ donc x appartient à $\operatorname{Im} p$ et aussi à $\operatorname{Im} q$ par un raisonnement semblable.

Montrons maintenant que le noyau de pq est $\operatorname{Ker} p + \operatorname{Ker} q$. Si $x \in \operatorname{Ker} pq$ alors $p(q(x)) = 0$ donc $q(x)$ appartient à $\operatorname{Ker} p$. Mais $x = q(x) + (x - q(x))$ avec $x - q(x) \in \operatorname{Ker} q$, donc x s'écrit bien comme somme d'un vecteur de $\operatorname{Ker} p$ et d'un vecteur de $\operatorname{Ker} q$. Réciproquement, si $x = x_p + x_q$ avec $x_p \in \operatorname{Ker} p$ et $x_q \in \operatorname{Ker} q$, on a $pq(x) = pq(x_p) + pq(x_q) = qp(x_p) + pq(x) = q(0) + p(0) = 0$. □

Remarquons que des applications successives du lemme à un ensemble fini de projections $\{p_i, i \in I\}$ commutant deux à deux montrent que $\prod_i p_i$ est la projection sur $\bigcap_i \operatorname{Im} p_i$ le long de $\sum_i \operatorname{Ker} p_i$.

Preuve de la Proposition 4.1. Soit F un ensemble fini d'endomorphismes diagonalisables. Montrons d'abord que si la somme des espaces propres $V_k, k \in K$ de F est V, alors les éléments de F commutent deux à deux.

Comme les éléments de V_k sont stables par action de F, on peut définir le morphisme de restriction

$$\begin{aligned} r_k \colon F &\longrightarrow \operatorname{End}(V_k) \\ f &\longmapsto f_{|V_k}. \end{aligned}$$

Pour tous $k \in K$ et $f, f' \in F$, les restrictions $r_k(f), r_k(f')$ commutent entre-elles, puisque ce sont des homothéties. On a donc $V_k \subset \operatorname{Ker}(ff' - f'f)$ d'où, puisque les $V_k, k \in K$ engendrent V, $\operatorname{Ker}(ff' - f'f) = V$ et $ff' = f'f$. Comme f et f' sont arbitraires, on en conclut bien que les éléments de F commutent deux à deux.

Réciproquement, supposons que les éléments de F commutent deux à deux, et montrons que la somme des espaces propres de F est V. Pour éviter la multiplication des indices, nous supposerons que F contient seulement deux éléments, la preuve présentée ci-dessous s'adaptant sans mal au cas général.

Nous aurons besoin de la caractérisation suivante des endomorphismes diagonalisables : un endomorphisme f est diagonalisable si et seulement si il existe des projections non nulles $p_i, i \in I$ et des scalaires $\lambda_i, i \in I$ deux à deux distincts tels que

i) $\sum_{i \in I} p_i = \mathrm{id}_V$

ii) $p_{i_1} p_{i_2} = p_{i_2} p_{i_1} = 0$ pour tout $i_1 \neq i_2$

iii) $\sum_{i \in I} \lambda_i p_i = f$.

Cette caractérisation des endomorphismes diagonalisables pourrait être utilisée comme définition, elle est employée dans [5] dont nous nous sommes inspirés pour cette démonstration. C'est un exercice facile de démontrer qu'elle est équivalente aux autres définitions en remarquant que des $p_i, i \in I$ vérifient les conditions ci-dessus si et seulement si, pour tout $i \in I$, $\operatorname{Im} p_i$ est l'espace propre de f associé à λ_i, et $\operatorname{Ker} p_i$ contient les autres espaces propres.

La décomposition de f donnée dans le dernier point est appelée décomposition spectrale de f. Elle a la propriété agréable suivante :

$$Q(f) = Q\left(\sum_{i\in I} \lambda_i p_i\right) = \sum_{i\in I} Q(\lambda_i) p_i,$$

pour tout polynôme $Q \in k[X]$. En particulier, il existe pour tout $i_0 \in I$ un polynôme Q tel que $Q(f) = p_{i_0}$: il suffit de choisir Q tel que $Q(\lambda_{i_0}) = 1$ et $Q(\lambda_i) = 0$ pour $i \neq i_0$, ce qui est possible en posant

$$Q(X) = \prod_{i\neq i_0} \frac{X - \lambda_i}{\lambda_{i_0} - \lambda_i}.$$

Ces préliminaires étant faits, nous pouvons finir la démonstration de la Proposition 4.1. On note f et g les deux éléments de F, $p_i, i \in I$ les projections intervenant dans la décomposition spectrale de f et $p'_j, j \in J$ les décompositions intervenant dans la décomposition spectrale de g. Comme f et g commutent, $Q(f)$ et $R(g)$ commutent pour tous polynômes $Q, R \in k[X]$: les p_i commutent donc avec les p'_j.

Nous savons grâce au Lemme 4.1 que, pour tout $(i, j) \in I \times J$, $p_i p'_j$ est la projection sur

$$V_{i,j} = \operatorname{Ker}(f - \lambda_i \operatorname{id}_V) \cap \operatorname{Ker}(g - \lambda'_j \operatorname{id}_V).$$

Comme $\sum_i p_i = \sum_j p'_j = \operatorname{id}_V$, on a en composant les deux égalités $\sum_{i,j} p_i p'_j = \sum p'_j p_i = \operatorname{id}_V$. Il s'ensuit que les images des $p_i p'_j$ engendrent V, autrement dit $\sum V_{i,j} = V$. La somme des espaces propres de F est donc V, puisque les $V_{i,j}$ non triviaux sont exactement les espaces propres de F.

Les projections $p_i p'_j$ permettent aussi de montrer que la somme des $V_{i,j}$ est directe. En effet, on a $p_i p'_j p_{i'} p'_{j'} = 0$ dès que $i \neq i'$ ou $j \neq j'$. Il s'ensuit que, pour tous vecteurs $v_{i,j} \in V_{i,j}, i \in I, j \in J$, on a

$$p_{i_0} p'_{j_0}(\sum v_{i,j}) = v_{i_0,j_0}$$

quelques soient i_0, j_0, de sorte $\sum v_{i,j} = 0$ implique $v_{i,j} = 0$ pour tous i, j. □

Corollaire 4.1. *Des endomorphismes diagonalisables en nombre fini sont simultanément diagonalisables si et seulement si ces endomorphismes commutent deux à deux.*

Démonstration. Il suffit de montrer que les éléments de F sont simultanément diagonalisables si et seulement si la somme des espaces propres de F est V. Si $e_i, i \in I$ est une base de V qui diagonalise tous les éléments de F, alors chacun des e_i appartient à un des espaces propres de F et donc la somme de ceux-ci fait V ; si réciproquement la somme des espaces propres de F est V, il suffit de choisir une base pour chacun d'eux et de faire la réunion de ces bases pour obtenir une base de V dans laquelle les éléments de F sont diagonalisables. □

4.2 L'isomorphisme $\mathrm{SU}(\mathbb{C}^2)/\{\pm \mathrm{id}\} \simeq \mathrm{SO}(\mathbb{R}^3)$

Rappelons que $\mathrm{SU}(\mathbb{C}^n)$ (resp. $\mathrm{SO}(\mathbb{R}^n)$) désigne le groupe des endomorphismes unitaires de $\mathbb{C}^n$ (resp. isométries linéaires de $\mathbb{R}^n$) ayant déterminant 1. Le groupe des transformations unitaires de déterminant quelconque est noté $\mathrm{U}(\mathbb{C}^n)$.

Proposition 4.2. *Il existe un morphisme de groupes surjectif de* $\mathrm{U}(\mathbb{C}^2)$ *dans* $\mathrm{SO}(\mathbb{R}^3)$ *dont le noyau est exactement l'ensemble des homothéties. Sa restriction à* $\mathrm{SU}(\mathbb{C}^2)$ *est un morphisme surjectif de noyau* $\{\pm \mathrm{id}\}$.

Démonstration. Nous suivons la preuve proposée dans le sujet d'agrégation de 2003.

Considérons l'ensemble E des endomorphismes de $\mathbb{C}^2$ de trace nulle et auto-adjoints pour le produit hermitien canonique. E est stable par addition et par multiplication avec un scalaire réel, donc E est un $\mathbb{R}$-espace vectoriel. On peut aussi voir E comme l'ensemble des endomorphismes diagonalisables dans une base orthonormée ayant des valeurs propres réelles opposées, ou comme les endomorphismes de $\mathbb{C}^2$ dont la représentation matricielle a la forme

$$\begin{pmatrix} \alpha & \beta \\ \bar{\beta} & -\alpha \end{pmatrix}, \quad \alpha \in \mathbb{R}, \quad \beta \in \mathbb{C},$$

ce qui montre au passage que E est de dimension 3, et est donc isomorphe à $\mathbb{R}^3$ en tant qu'espace vectoriel. On dote E d'un produit scalaire en posant, pour tout $f, g \in E$, $\langle f, g\rangle = \mathrm{Tr}(fg^*) = \mathrm{Tr}(fg)$: il s'agit bien d'une forme bilinéaire symétrique, et on peut voir qu'elle est définie positive en remarquant que si $f \in E$ a λ et $-\lambda$ pour valeurs propres, $ff^* = f^2 = \lambda^2 \,\mathrm{id}_{\mathbb{C}^2}$.

A toute transformation unitaire $u \in \mathrm{U}(\mathbb{C}^2)$ on peut associer l'application φ_u définie sur E par $\varphi_u \colon f \mapsto ufu^*$. L'application φ_u est à valeurs dans E, car si f est auto-adjointe de trace nulle, ufu^* l'est aussi. On vérifie de même que φ_u est $\mathbb{R}$-linéaire et que

$$\begin{aligned} ||ufu^*||_E &= \mathrm{Tr}(ufu^*(ufu^*)^*) \\ &= \mathrm{Tr}(ufu^*uf^*u^*) \\ &= \mathrm{Tr}(uff^*u^*) \\ &= \mathrm{Tr}(u^*uff^*) \\ &= \mathrm{Tr}(ff^*) \\ &= ||f||_E \end{aligned}$$

de sorte que φ_u est une isométrie de E. Enfin, remarquons que $\rho : u \mapsto \varphi_u$ est un morphisme de groupes.

On peut expliciter φ_u à l'aide d'une base de vecteurs propres de u : en écrivant f et u dans cette base on constate que ufu^* s'écrit

$$\begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & -\alpha \end{pmatrix} \begin{pmatrix} \bar{\omega_1} & 0 \\ 0 & \bar{\omega_2} \end{pmatrix} = \begin{pmatrix} \alpha & \beta\omega_1\bar{\omega_2} \\ \bar{\beta}\bar{\omega_1}\omega_2 & -\alpha \end{pmatrix}.$$

Si u est une homothétie $\varphi_u = \mathrm{id}_E$, et sinon φ_u fixe la droite des éléments de E qui commutent avec u et tourne l'orthogonal de cette droite d'un angle $\arg(\omega_1\bar{\omega_2})$ ou $\arg(\omega_2\bar{\omega_1})$ selon l'orientation que l'on donne à E. Ainsi φ_u est toujours un élément de $\mathrm{SO}(\mathbb{R}^3)$ — on identifie désormais E à $\mathbb{R}^3$ — et réciproquement, tous

les éléments de $\mathrm{SO}(\mathbb{R}^3)$ ont la forme décrite ci-dessus, donc l'image de ρ est $\mathrm{SO}(\mathbb{R}^3)$.

Nous avons bien construit un morphisme de groupes surjectif $\rho : u \mapsto \varphi_u$ de $\mathrm{U}(\mathbb{C}^2)$ dans $\mathrm{SO}(\mathbb{R}^3)$, et nous avons aussi montré que le noyau de cette application est constitué des homothéties de $\mathrm{U}(\mathbb{C}^2)$. Le fait que la restriction de ρ à $\mathrm{SU}(\mathbb{C}^2)$ reste surjective vient du fait que toute transformation unitaire peut s'écrire $u = \lambda u'$ avec $\lambda \in \mathbb{C}$ et $u' \in \mathrm{SU}(\mathbb{C}^2)$, et il est évident que le noyau de cette restriction est précisément $\{\pm \mathrm{id}\}$. □

Le groupe $\mathrm{U}(\mathbb{C}^2)$ peut être vu comme le groupe des quaternions — ceux-ci peuvent être définis comme une sous-algèbre de matrices — de norme unité : l'isomorphisme de la proposition nous permet donc d'associer une rotation de l'espace à tout quaternion unitaire. Dans certaines branches de la physique il est courant de représenter les rotations de l'espace par des matrices complexes de taille 2×2.

Il y a encore une autre manière d'interpréter ce morphisme : à chaque matrice unitaire complexe il est possible d'associer une homographie du plan complexe, et à ces homographies du plan complexe il est possible d'associer une rotation de la sphère de $\mathbb{R}^3$ via la projection stéréographique : on obtient ainsi le morphisme de groupes de $\mathrm{U}(\mathbb{C}^2)$ dans $\mathrm{SO}(\mathbb{R}^3)$ dont il est question.

On peut trouver une exposition plus détaillée de ces deux approches dans [8].

4.3 Simplicité du groupe alterné

On rappelle qu'un groupe G est dit simple s'il n'a pas de sous-groupe distingué propre, c'est-à-dire non trivial et différent de G.

Théorème 4.1 (Jordan, 1870)**.** *Le groupe alterné A_n est simple pour $n \geqslant 5$.*

Pour la démonstration du théorème nous aurons besoin du résultat suivant, bien connu, sur les classes de conjugaison du groupe symétrique. Puisqu'il est de niveau L3, nous n'en donnons pas de démonstration : le lecteur peut en trouver une dans [7].

Lemme 4.2. *La classe de conjugaison dans S_n d'une permutation π est l'ensemble des permutations ayant la même structure de cycles.*

Ce résultat ne suffit pas pour déterminer les classes de A_n : il se peut que deux permutations ayant la même structure de cycles ne soient pas conjuguées dans A_n. Il permet tout de même de montrer le lemme suivant.

Lemme 4.3. *Les 3-cycles sont tous conjugués dans A_n dès que $n \geqslant 5$.*

Démonstration. D'après le lemme précédent, pour tous 3-cycles $(abc), (a'b'c')$ il existe $\sigma \in S_n$ telle que $\sigma(a'b'c')\sigma^{-1} = (abc)$. Si σ est paire, alors $(a'b'c')$ et (abc) sont bien conjugués dans A_n. Sinon, on peut choisir d, e distincts de a, b et c, on a alors $(de)\sigma \in A_n$ et

$$((de)\sigma)(a'b'c')((de)\sigma)^{-1} = (de)\sigma(a'b'c')\sigma^{-1}(de) = (de)(abc)(de) = (abc).$$

Dans tous les cas, $(a'b'c')$ et (abc) sont conjugués dans A_n. □

Nous avons maintenant tous les outils nécessaires pour montrer que A_n est simple. Nous reprenons la preuve de [7].

Démonstration de la simplicité de A_n. On commence par vérifier que A_5 est simple. Les 3-cycles engendrent A_n pour tout $n \geqslant 3$ (un fait connu que l'on admet) donc il suffit de montrer que tout sous-groupe distingué H non-trivial de A_5 contient un 3-cycle. Soit $\sigma \in H$ une permutation non triviale qui n'est pas un 3-cycle : σ est alors de la forme $(ab)(cd)$ ou de la forme $(abcde)$. Dans le premier cas on pose $\pi = (abe)$ de sorte que $\pi\sigma\pi^{-1} \in H$ et

$$(\pi\sigma\pi^{-1})\sigma^{-1} = (be)(cd)(ab)(cd) = (aeb)$$

donc H contient un 3-cycle. Dans le second cas on pose $\pi = (abc)$ et là encore

$$\pi\sigma\pi^{-1}\sigma^{-1} = (abd).$$

Dans tous les cas H contient un 3-cycle, ce qui conclut la preuve.

On passe maintenant au cas général. Soit H un sous-groupe distingué non trivial de A_n avec $n \geqslant 5$, montrons que $H = A_n$. Il nous suffit pour cela de montrer que H contient un 3-cycle.

Soit π un élément non trivial de H, et $\sigma = (abc)$ un 3-cycle. On s'intéresse au commutateur $\rho = \sigma\pi\sigma^{-1}\pi^{-1}$. Comme $\rho = (\sigma\pi\sigma^{-1})\pi^{-1}$ il appartient à H, et comme $\rho = \sigma(\pi\sigma^{-1}\pi^{-1})$ et $\sigma, (\pi\sigma^{-1}\pi^{-1})$ sont deux 3-cycles, ρ a au moins $n-6$ points fixes.

On peut choisir σ de sorte que ρ soit non triviale et ait au au moins $n-5$ points fixes : si i est tel que $\pi(i) \neq i$ il suffit de prendre $b = i$, $c = \pi(i)$ et $a \notin \{i, \pi(i), \}$, ce qui est toujours possible dès que $n \geqslant 4$. On a alors $\pi\sigma^{-1}\pi^{-1}(c) = \pi(a) \neq c$ puisque $a \neq i$. Les supports de $\pi\sigma^{-1}\pi^{-1}$ et σ ne sont donc pas disjoints et leur union, qui contient le support de ρ, a 5 éléments au plus.

Soit A le groupe des permutations de A_n fixant ces mêmes $n-5$ nombres (si ρ a plus de points fixes on en choisit $n-5$ arbitrairement). A est isomorphe à A_5, $A \cap H$ est un sous-groupe distingué de A, et $A \cap H$ est non trivial car il contient ρ. Par simplicité de A_5, $A \cap H = A$ et en particulier H contient un 3-cycle, donc $H = A_n$. □

Corollaire 4.2. *Pour $n \geqslant 5$, le seul sous-groupe distingué propre de S_n est A_n.*

Démonstration. Soit H un sous-groupe distingué de S_n. Comme A_n est simple et $H \cap A_n$ est distingué dans A_n, ou bien $A_n \subset H$, ou bien $H \cap A_n = 1$. Dans le premier cas, puisque A_n est d'indice 2 on a forcément $H = A_n$ ou $H = S_n$. Dans le second cas, le deuxième théorème d'isomorphisme nous dit que $H/(H \cap A_n) \simeq HA_n/A_n$ d'où $|H| \leqslant 2$. Si H contient un élément non trivial h, l'hypothèse que H est distingué s'écrit $ghg^{-1} = h$ pour tout $g \in S_n$, ce qui est absurde car le centre de S_n est réduit à l'identité pour $n \geqslant 3$: H doit donc être trivial. Ainsi S_n n'admet que trois sous-groupes distingués dont un seul, à savoir A_n, est propre. □

Références

[1] Richard Antetomaso. Autour du théorème de Jordan sur les sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$. *RMS*, 124, 2014.

[2] Emmanuel Breuillard. An exposition of Jordan's original proof of his theorem on finite subgroups of $\mathrm{GL}_n(\mathbb{C})$, 2011. Disposible sur sa page personnelle.

[3] Michael Collins. On Jordan's theorem for complex linear groups. *Journal of Group Theory*, 2007.

[4] Georg Frobenius. Uber den von L. Bieberbach gefundenen Beweis eines Satzes von C.Jordan. *Sitzber. Preuss. Akad. Wiss.*, 1911.

[5] Paul R. Halmos. *Finite Dimensional Vector Spaces*. Springer, 1958.

[6] Geoffrey R. Robinson. On linear groups. *Journal of Algebra*, 131, 1990.

[7] Aviva Szpirglas. *Algèbre L3*. Pearson Education, 2009.

[8] Romain Vidonne. *Groupe circulaire, rotations et quaternions*. éditions Ellipses, 2001.