$\mathrm{H}^2\mathrm{M}^2$

Hitchhiker's Manual of Maths

Sommaire

Notations

« - Why don't they just speak English ?
- Yeah, well maybe because seventy percent of the planet speaks other languages.
Mathematics is the only truly universal language, Senator. »

Contact, Robert Zemeckis, 1997.

$:=$	par définition égal à
$\simeq$	isomorphisme
$\cong$	homéomorphisme
$\approx$	équivalence
$\sim$	similitude/conjugaison
$\equiv$	congruence
$\hookrightarrow$	injection
$\twoheadrightarrow$	surjection
$\hookrightarrow\!\!\!\!\twoheadrightarrow$	bijection
$\circlearrowleft$	action de groupe
$\bigsqcup$	réunion disjointe
id	application identité
$\mathbb{K}$	corps quelconque
I_k	matrice unité de $M_k(\mathbb{K})$
Id	endomorphisme identité (de matrice I_k)
χ_A	Polynôme caractéristique de l'endomorphisme A
π_A	Polynôme minimal de l'endomorphisme A
$\mathfrak{S}_X$	groupe symétrique de X ou automorphismes de l'ensemble X
$\mathrm{Aut}(G)$	automorphismes du groupe G. Inclu dans $\mathfrak{S}_G$
$\lvert X\rvert$	cardinal de l'ensemble X

Introduction

Née de l'étude des équations polynomiales par Évariste Galois (1811 - 1832), la théorie des groupes est devenue un outil central en mathématiques. En particulier, on retrouve les groupes de transformations continues et les algèbres du nom de leur inventeur [1] Sophus Lie (1842 - 1899) dans des domaines aussi variés que l'analyse et même la physique, en passant bien sûr par la géométrie, grâce notamment au *programme d'Erlangen* de Félix Klein (1849 - 1925) qui proposa d'étudier la géométrie non plus à travers les objets qui la composent, mais directement par les propriétés de l'espace géométrique lui-même et des structures algébriques que constituent les transformations qui n'altère pas l'espace. Hermann Weyl (1885 - 1955) étudia les groupes de Lie compacts et leurs représentations, notions qu'il rendit indispensables à la physique théorique.

Les groupes continus (p17), où même les groupes linéaires sur des corps divers - comme les corps finis ou celui des quaternions (p75) - sont les structures de base, les groupes dits classiques, dont il faut connaître les nombreuses formes et propriétés fondamentales.
Dans la notion de groupes classiques, nous entendrons les groupes linéaires $GL_n(\mathbb{K})$, où $\mathbb{K}$ est un corps, le groupe spécial linéaire $SL_n(\mathbb{K})$, ainsi que leur projectivisés $PGL_n(\mathbb{K})$ et $PSL_n(\mathbb{K})$, essentiels en géométrie projective, puis les groupes orthogonaux $O(n,\mathbb{K})$, $SO(n,\mathbb{K})$ et plus généralement les groupes orthogonaux laissant invariante une forme quadratique non dégénérée. Enfin, nous étudierons le groupe symplectique $Sp(n,\mathbb{K})$, laissant invariante une forme alternée non dégénérée en dimension $2n$.

L'intérêt de l'étude de ces groupes classiques est multiple, pour ne donner que ceux illustrés dans ce cours :

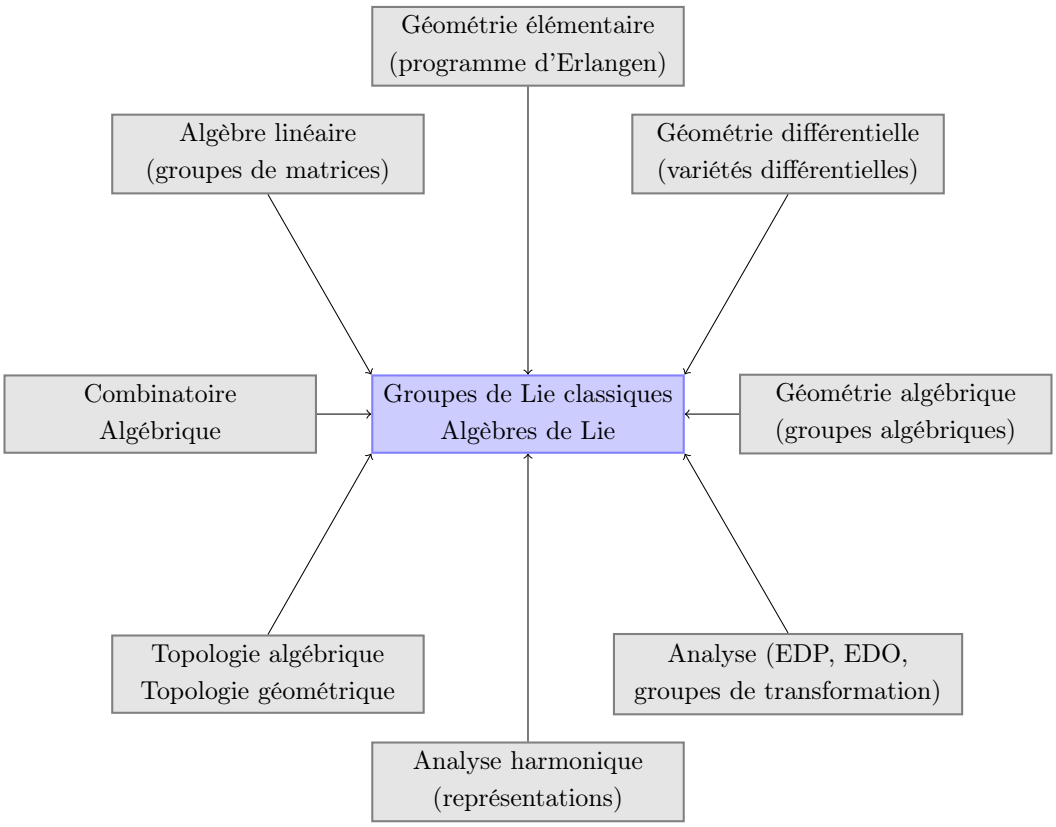
- *Applications à la géométrie.* En tant que groupes de transformations, ils permettent de ramener un problème géométrique en un autre plus simple à résoudre (p93). Nous y consacrons un chapitre entier où trois problèmes de géométrie plane sont résolus à l'aide de trois groupes différents. Il sera important de noter le type de géométrie utilisée (affine, projective réelle, projective complexe), l'étude des actions et des orbites associées, ainsi que leurs invariants.
- *Des groupes classiques pour l'étude des groupes.* Comme on le verra tout au long du cours, beaucoup de groupes obtenus naturellement pour la résolution de problèmes (groupes paraboliques, groupes affines...) se réalisent comme produits directs, semi-directs de groupes classiques. Les groupes classiques apparaissent alors comme les atomes constituant bon nombre de groupes rencontrés dans la nature. Leur étude systématique apparait alors comme essentielle.
- *Unification du programme d'algèbre et géométrie.* Enfin, nous verrons que les groupes classiques, à travers leurs actions, permettent de définir de facon naturelle des invariants d'action. Un des buts de ce cours est de donner à l'étudiant une vision des mathématiques à travers celle de l'action de groupe. Ainsi, les objets mathématiques étudiés les années précédentes en algèbre et en géométrie devraient apparaitre comme des invariants d'action de groupes classiques, voir le tableau p30.
- Quand le corps de base est $\mathbb{R}$ ou $\mathbb{C}$, certains problèmes de topologie se ramènent à des propriétés topologiques de groupes classiques. Il en sera question dans tous les chapitres, à l'exception de la combinatoire algébrique et des solides platoniciens.
- Quand on travaille sur des corps finis, ou sur des problèmes de configurations, les groupes classiques permettent de faire du dénombrement en les faisant agir sur un objet que l'on veut dénombrer. C'est l'objet du Chapitre VI p67. On en profitera pour faire de la géometrie discrète et pour observer les liens mysterieux entre le dénombrement et la topologie. Nous ne ferons qu'effleurer le problème en parlant de décomposition cellulaire, mais il faut savoir que ce lien aboutit à la fameuse "conjecture de Weil" et une célèbre médaille Field (Pierre Deligne, 1978).

[1] Les algèbres en question furent aussi développées par Wilhelm Karl Joseph Killing (1847 - 1923), indépendamment de Lie. Killing a essentiellement classifié les algèbres de Lie simples finies complexes, travail ensuite complété par Élie Cartan (1869 - 1951).

Après avoir étudié les groupes classiques, discrets ou topologiques, on introduira au Chapitre VIII (p83) la notion plus difficile de groupe de Lie. Il s'agit de groupes munis d'une structure de variété différentielle. L'utilité de cette structure réside dans le fait qu'une grande quantité d'information sur le groupe peut être lue dans un espace vectoriel : l'espace tangent au groupe en l'identité. Cet espace tangent est doté d'une structure supplémentaire appelée structure d'algèbre de Lie que nous étudierons assez peu malheureusement (un des buts avoués du cours étant de faire de la transversalité à l'intérieur du programme de l'agrégation). Il s'agit là d'une méthode générale puissante, la linéarisation, dont le théoreme des fonctions implicites fait partie. On montrera l'efficacité d'une telle méthode en exhibant des isomorphismes exceptionnels. On mettra ici en oeuvre une méthode typique de la théorie de Lie : on montre qu'un morphisme entre groupes de Lie est surjectif en se ramenant simplement à la surjectivité d'une application linéaire !

A chaque fin de chapitre, on donne quelques références dans la littérature. Afin de ne pas encombrer le lecteur avec un bibliographie surchargée, on citera parmi les livres suivants :

Introduction à la théorie des groupes classiques, Rached Mneimné, Frédéric Testard, **Hermann**
Cours d'algèbre, Daniel Perrin, **Ellipses**
Eléments de géométrie, actions de groupes, Rached Mneimné, **Cassini**
Géométrie, Michèle Audin, **Belin**
Algèbre linéaire, Rémi Goblot, **Ellipses**
Méthodes modernes en géométrie, Jean Fresnel, **Hermann**



Chapitre I

Actions et théorème du rang

« Everything begins with choice »

Matrix Reloaded, Andy & Larry Wachowski, 2003.

Le but de ce chapitre est de motiver l'étude des actions de groupes, qui seront introduites au chapitre suivant. Le théorème du rang, théorème bien connu de L1 et corollaire du théorème de la base incomplète, assure que deux matrices sont équivalentes si et seulement si elles ont même rang et il est valable dans n'importe quel corps. On revisite ce fameux théorème en terme d'invariant d'action de groupe.

1 Théorème du rang

Soit $\mathbb{K}$ un corps et $\varphi : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ une application linéaire. Soient $\underline{e}, \underline{f}$ des bases de $\mathbb{K}^n$ et $\mathbb{K}^m$ respectivement.
On note $A = \mathrm{mat}_{\underline{e},\underline{f}}(\varphi) = (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$ la matrice de φ dans les bases $\underline{e}, \underline{f}$, où a_{ij} est la i$^{\text{ème}}$ coordonnée de $\varphi(e_j)$ dans la base $\underline{f}$. C'est un élément du $\mathbb{K}$-espace vectoriel des matrices de taille $m \times n$ que l'on note $M_{m,n}(\mathbb{K})$.
Il est tentant d'associer un outil pratique (la matrice) à un objet théorique (l'application linéaire), mais cette association pose un problème de choix (la base), et on sait qu'en mathématiques, les choix finissent par se payer cher. Pour cela, on définit une relation :

Définition 1 :
Deux matrices A et B sont équivalentes $(A \approx B)$ $\iff$ *elles codent la même application linéaire*
$\iff \exists P, Q$ *inversibles telles que* $B = PAQ^{-1}$

D'où la question : à quelle condition deux matrices A et B sont-elles équivalentes ?

Rappel :
$\mathrm{rg}\, A = \mathrm{rg}\, \varphi = \dim \mathrm{Im}\, \varphi = \dim E$ où E est l'espace vectoriel engendré par les colonnes (ou les lignes) de A.

Théorème 1 (du rang):

$$A \approx B \iff \mathrm{rg}\, A = \mathrm{rg}\, B$$

Démonstration :

$\boxed{\Longrightarrow}$ $A \approx B \Longrightarrow \operatorname{rg} A = \operatorname{rg} \varphi = \operatorname{rg} B$ est clair.

$\boxed{\Longleftarrow}$ Montrons que si on note $r = \operatorname{rg} A$ alors $A \approx I_{r,0} = \left[\begin{smallmatrix} I_r \\ 0 \end{smallmatrix} \right] \in M_{m,n}(\mathbb{K})$. On aura alors $A \approx I_{r,0} \approx B$ d'où $A \approx B$.

Montrons que $I_{r,0}$ est la matrice de φ dans une certaine base (en fait un certain couple de bases).

$\dim \operatorname{Ker} \varphi = n - \dim \operatorname{Im} \varphi = n - r$. Soit $(e'_i)_{r+1 \leq i \leq n}$ une base de $\operatorname{Ker} \varphi$.

D'après le théorème de la base incomplète, $\exists \underline{e'} = (e'_i)_{1 \leq i \leq n}$ base de $\mathbb{K}^n$. On pose $f'_i = \varphi(e'_i) \quad \forall 1 \leq i \leq r$.

$(f'_i)_{1 \leq i \leq r}$ est un système libre car $(e'_i)_{1 \leq i \leq n}$ est libre et φ injective sur $< (e'_i)_{1 \leq i \leq r} >= (\operatorname{Ker} \varphi)^{\perp}$.

En effet, $\operatorname{Ker} \varphi \mid_{<(e'_i)_{1 \leq i \leq r}>} = \operatorname{Ker} \varphi \cap < (e'_i)_{1 \leq i \leq r} >= \{0\}$.

Toujours d'après le théorème de la base incomplète, on obtient une base $\underline{f'} = (f'_i)_{1 \leq i \leq m}$.

Ainsi $I_{r,0} = \operatorname{mat}_{\underline{e'}, \underline{f'}}(\varphi)$.

□

2 Action $GL_m(\mathbb{K}) \times GL_n(\mathbb{K}) \circlearrowleft M_{m,n}(\mathbb{K})$ par équivalence

La réponse à ce problème de choix des bases passe par une action de groupe particulière. On verra au chapitre suivant la définition d'une action, p20.

Notons G le produit direct $GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$.

$$\begin{array}{ccc} G \times M_{m,n}(\mathbb{K}) & \longrightarrow & M_{m,n}(\mathbb{K}) \\ (P, Q, A) & \longmapsto & (P, Q) \cdot A := PAQ^{-1} \end{array}$$

Remarques :

On vérifie qu'on a une "pseudo-associativité" : $[(P, Q)(P', Q')] \cdot A = (P, Q) \cdot [(P', Q') \cdot A]$

Avec $(I_m, I_n) \cdot A = A$

On comprend pourquoi il est naturel de mettre l'élément du groupe G à gauche de l'élément sur lequel il agit ; c'est une action à gauche. L'application définie par $A \cdot (P, Q) := P^{-1}AQ$ donnerait une action à droite.

$$\begin{aligned} \operatorname{Orb}(A) &= G \cdot A \\ &= \{B \in M_{m,n}(\mathbb{K}) \, : \, B = PAQ^{-1}\} \\ &= \{B \in M_{m,n}(\mathbb{K}) \, : \, B \text{ code la même application linéaire que } A\} \\ &= \{B \in M_{m,n}(\mathbb{K}) \, : \, B \approx A\} \\ &= \{B \in M_{m,n}(\mathbb{K}) \, : \, rg(B) = rg(A)\} \end{aligned}$$

A chaque application linéaire φ de matrice A on préfère donc associer toutes ses matrices équivalentes, c'est à dire $\operatorname{Orb}(A)$ qui ne dépend pas d'un choix de bases. C'est une classe d'équivalence pour la relation $\approx$:

Définition 2 :

Soit A une matrice de $M_{m,n}(\mathbb{K})$, on appelle orbite de A pour l'action de G l'ensemble $\operatorname{Orb}(A) := G \cdot A$. *Par construction, les orbites partitionnent $M_{m,n}(\mathbb{K})$.*

Théorème 2 (Autre formulation du théorème du rang):

$\operatorname{Orb}(A) = \operatorname{Orb}(B) \Longleftrightarrow \operatorname{rg}(A) = \operatorname{rg}(B)$

On notera dans la suite O_r l'orbite constituée des matrices de rang r.

Soit ϕ_A : $G \longrightarrow \mathrm{Orb}(A)$ $\quad g \longmapsto g \cdot A$ Elle est surjective par définition. Mais est-elle injective ?

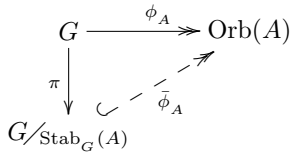
Alors $\phi_A(g') = \phi_A(g)$
$\iff g' \cdot A = g \cdot A$
$\iff g^{-1}(g' \cdot A) = g^{-1}(g \cdot A)$
$\iff (g^{-1}g') \cdot A = (g^{-1}g) \cdot A$
$\iff (g^{-1}g') \cdot A = A$

On note $\mathrm{Stab}_G(A) = \{h \in G : h \cdot A = A\} = \{(P,Q) \in GL_m(\mathbb{K}) \times GL_n(\mathbb{K}) : PAQ^{-1} = A\}$
Il est clair que $\mathrm{Stab}_G(A)$ est un sous-groupe de G, en général non distingué.
$g^{-1}g' \in \mathrm{Stab}_G(A) \iff g' \in g\ \mathrm{Stab}_G(A) \iff g$ et g' sont dans la même classe $\dot{g} \in G/_{\mathrm{Stab}_G(A)}$

Conclusion : On ne peut pas affirmer que ϕ_A soit injective : $\phi_A(g') = \phi_A(g) \iff \dot{g} = \dot{g}'$.

Théorème 3 :

Il existe une unique application $\bar{\phi}_A$ telle que le diagramme suivant commute :



De plus, $\bar{\phi}_A$ est bijective.

retour p21

Démonstration :

Si $\bar{\phi}_A$ existe, elle est clairement unique.
Si $g' \in \dot{g} = g\ \mathrm{Stab}_G(A)$ alors $g' = gh$ (avec $h \in \mathrm{Stab}_G(A)$)
Donc $\phi_A(g') = g' \cdot A = (gh) \cdot A = g(h \cdot A) = g \cdot A = \phi_A(g)$.
$\phi_A(g')$ ne dépend pas de l'élément $g \in \dot{g}$
On peut donc bien définir $\bar{\phi}_A(\dot{g}) = \phi_A(g)$. On a $\bar{\phi}_A \circ \pi = \phi_A$ d'où la commutativité du diagramme.

De plus, $\bar{\phi}_A(G/_{\mathrm{Stab}_G(A)}) = \phi_A(G)$ donc $\bar{\phi}_A$ est surjective.
$\bar{\phi}_A(\dot{g}) = \bar{\phi}_A(\dot{g}') \Longrightarrow \phi_A(g) = \phi_A(g') \Longrightarrow g = g'\,\mathrm{Stab}_G(A) \Longrightarrow \dot{g} = \dot{g}'$ donc $\bar{\phi}_A$ est injective.

□

Corollaire 1 :

Si $\mathbb{K}$ est un corps fini, alors $|\mathrm{Orb}(A)| = \left|{}^{GL_m(\mathbb{K}) \times GL_n(\mathbb{K})}/_{\mathrm{Stab}_G(A)}\right|$

retour p14

$\mathrm{Orb}(A) \not\simeq {}^{GL_m(\mathbb{K}) \times GL_n(\mathbb{K})}/_{\mathrm{Stab}_G(A)}$
On a une bijection, mais pas un isomorphisme car ce ne sont pas forcément des groupes (le stabilisateur n'est en général pas distingué).

Les éléments d'une même orbite ayant des propriétés similaires, on se ramènera souvent à un élément "normal" ou commode de $\mathrm{Orb}(A)$ comme par exemple (avec $r = \mathrm{rg}\,A$) : $I_{r,0} := \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$

Proposition 1 :
Soit A une matrice de rang r. Alors $\mathrm{Stab}_{G}(A) = g\ \mathrm{Stab}_{G}(I_{r,0})\, g^{-1} \simeq \mathrm{Stab}_{G}(I_{r,0})$

Démonstration :
$\exists g \in GL_n(\mathbb{K})$ telle que $A = gI_{r,0}$ donc $\mathrm{Stab}_{G}(A) = \mathrm{Stab}_{G}(gI_{r,0})$
Soit $h \in \mathrm{Stab}_{G}(A)$ alors
$$\begin{aligned} & h \cdot (gI_{r,0}) = gI_{r,0} \\ \iff & hg \cdot I_{r,0} = gI_{r,0} \\ \iff & g^{-1}hg \cdot I_{r,0} = I_{r,0} \\ \iff & g^{-1}hg \in \mathrm{Stab}_{G}(I_{r,0}) \\ \iff & h \in g\,\mathrm{Stab}_{G}(I_{r,0})g^{-1} \end{aligned}$$

D'où $\mathrm{Stab}_{G}(A) = g\ \mathrm{Stab}_{G}(I_{r,0})\, g^{-1}$ et il est clair que $g\ \mathrm{Stab}_{G}(I_{r,0})\, g^{-1} \simeq \mathrm{Stab}_{G}(I_{r,0})$.

□

L'étude de $\mathrm{Stab}_{G}(A)$ est donc ramenée à l'étude de $\mathrm{Stab}_{G}(I_{r,0})$. Étudions donc $\mathrm{Stab}_{G}(I_{r,0})$:

Soient $P = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$ et $Q = \begin{bmatrix} A' & C' \\ B' & D' \end{bmatrix}$ dans $\mathrm{Stab}_{G}(I_{r,0})$.

$$\begin{aligned} PI_{r,0}Q^{-1} = I_{r,0} & \iff \begin{bmatrix} A & C \\ B & D \end{bmatrix} \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} A' & C' \\ B' & D' \end{bmatrix}^{-1} = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \\ & \iff \begin{bmatrix} A & C \\ B & D \end{bmatrix} \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} A' & C' \\ B' & D' \end{bmatrix} \\ & \iff \begin{bmatrix} A & 0 \\ B & 0 \end{bmatrix} = \begin{bmatrix} A' & C' \\ 0 & 0 \end{bmatrix} \\ & \iff A = A' \qquad B = 0 \qquad C' = 0 \\ & \iff P = \begin{bmatrix} A & C \\ 0 & D \end{bmatrix} \qquad Q = \begin{bmatrix} A & 0 \\ B' & D' \end{bmatrix} \end{aligned}$$


On n'inverse pas !

$P \in GL_m(\mathbb{K}) \iff A \in GL_r(\mathbb{K}), D \in GL_{n-r}(\mathbb{K})$ car $\det P = \det A \det D$
$C \in M_{r,n-r}(\mathbb{K})$. De même $B' \in M_{n-r,r}(\mathbb{K})$ et $D' \in GL_{n-r}(\mathbb{K})$.

Ainsi on verra que l'on peut écrire le groupe $\mathrm{Stab}_{G}(I_{r,0})$ sous forme de produits directs et semi-directs de groupes classiques :

$$\begin{aligned} \mathrm{Stab}_{G}(I_{r,0}) &= \begin{bmatrix} GL_r(\mathbb{K}) & M_{r,m-r}(\mathbb{K}) \\ 0 & GL_{m-r}(\mathbb{K}) \end{bmatrix} \times \begin{bmatrix} GL_r(\mathbb{K}) & 0 \\ M_{n-r,r}(\mathbb{K}) & GL_{n-r}(\mathbb{K}) \end{bmatrix} \\ &= GL_r(\mathbb{K}) \times GL_{m-r}(\mathbb{K}) \times GL_{n-r}(\mathbb{K}) \ltimes \big(M_{r,m-r}(\mathbb{K}) \oplus M_{n-r,r}(\mathbb{K})\big) \end{aligned}$$

retour p28

3 Propriétés topologiques

Les espaces de matrices sur $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ sont munis de la topologie de $\mathbb{R}$-espace vectoriel normé. Les opérations $+$ et $\times$ (produit matriciel) ne font intervenir que des polynômes en les variables et donc sont continues pour cette topologie.
Il est naturel d'étudier la topologie des orbites O_r des matrices de rang r. Elles ne sont en général ni ouvertes ni fermées, mais leur clôture est donnée par :

Proposition 2 :

$$\overline{O}_r = \bigsqcup_{0 \leq k \leq r} O_k$$

Démonstration :
Montrons que $\bigsqcup_{0 \leq k \leq r} O_k$ est un fermé. Soient $I \subset \{1, \dots, m\}, J \subset \{1, \dots, n\}$ tels que $|I| = |J| = r$.

Le mineur d'ordre r associé à (I, J) est l'image de $\Delta_{I,J}$: $\begin{array}{ccc} M_{m,n}(\mathbb{K}) & \longrightarrow & \mathbb{K} \\ A = (a_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} & \longmapsto & \det\left((a_{i,j})_{\substack{i \in I \\ j \in J}}\right) \end{array}$

Un théorème important d'algèbre linéaire dit que le rang de A est l'ordre du plus grand mineur non nul :
$\mathrm{rg}(A) = \max\{r : \exists \Delta_{I,J}(A) \neq 0, |I| = |J| = r\}$

Soit δ : $\begin{array}{ccc} M_{m,n}(\mathbb{K}) & \longrightarrow & \mathbb{K}^{\binom{n}{r+1}\binom{m}{r+1}} \\ A & \longmapsto & \left(\Delta_{I,J}(A)\right)_{\substack{I \subset \{1,\dots,m\} \\ J \subset \{1,\dots,n\} \\ |I|=|J|=r+1}} \end{array}$ (il y a $\binom{n}{r+1}\binom{m}{r+1}$ mineurs ou sous-matrices carrées de taille $r+1$)

$$\begin{aligned} \bigsqcup_{0 \leq k \leq r} O_k &= \{A \in M_{m,n}(\mathbb{K}) : \mathrm{rg}(A) \leq r\} \\ &= \{A \in M_{m,n}(\mathbb{K}) : \Delta_{I,J}(A) = 0 \quad \forall |I| = |J| \geq r+1\} \\ &= \{A \in M_{m,n}(\mathbb{K}) : \Delta_{I,J}(A) = 0 \quad \forall |I| = |J| = r+1\} \qquad \text{car les sous-matrices sont "emboîtées"} \\ &= \delta^{-1}(\{0\}) \qquad \text{où } 0 \text{ est le vecteur nul de } \mathbb{K}^{\binom{n}{r+1}\binom{m}{r+1}} \text{ et donc } \{0\} \text{ son sous-espace nul.} \end{aligned}$$

On a $\delta^{-1}(\{0\})$ fermé car les $\Delta_{I,J}$ sont continus (polynomiaux).

Montrons l'égalité :

- $O_r \subset \bigsqcup_{0 \leq k \leq r} O_k$ par construction. Comme ce dernier est fermé, $\overline{O}_r \subset \bigsqcup_{0 \leq k \leq r} O_k$.
- Réciproquement, soit $A \in \bigsqcup_{0 \leq k \leq r} O_k$. Alors $\exists 0 \leq k \leq r$ tel que $A = P I_{r,0} Q^{-1}$ avec $I_{r,0} = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix} \in M_{m,n}(\mathbb{K})$.

  Posons $A(\epsilon) := P \begin{bmatrix} I_k & 0 & 0 \\ 0 & \epsilon I_{r-k} & 0 \\ 0 & 0 & 0 \end{bmatrix} Q^{-1} \in O_r$. Ainsi $A(\epsilon) \xrightarrow[\epsilon \to 0]{} A \in \bigsqcup_{0 \leq k \leq r} O_k$.

  Donc $A \in \overline{O}_r$ et donc $\overline{O}_r = \bigsqcup_{0 \leq k \leq r} O_k$.

□

Remarques :
La fonction rg : $M_n(\mathbb{K}) \longrightarrow \mathbb{N}$ n'est pas continue car la fibre d'un fermé n'est pas fermée : $\mathrm{rg}^{-1}(\{r\}) = O_r$. Par contre la fibre $\mathrm{rg}^{-1}(\{0,\dots,r\}) = \bigsqcup_{0\leq k\leq r} O_k$ est fermée, ie. le rang est semi-continu inférieurement.

Corollaire 2 :
La seule orbite fermée est l'orbite minimale $O_0 = \{0\}$.
La seule orbite ouverte est l'orbite maximale $O_{\min(n,m)} = GL_{\min(n,m)}(\mathbb{K})$.

retour p34

La question naturelle qui se pose au vu du corollaire 1 est :
A-t-on un homéomorphisme $\mathrm{Orb}(A) \cong {}^{GL_m(\mathbb{K})\times GL_n(\mathbb{K})}\!/_{\mathrm{Stab}_G(A)}$ pour la topologie quotient (cf p21) ?
C'est ce que nous verrons au chapitre suivant.

Rappel :
Un homéomorphisme est une bijection bicontinue.

Eléments de géométrie, actions de groupes, Chap. 0, Rached Mneimné, **Cassini**

4 Annexe 1 : Connexité

Définition 3 :
Soit X un espace topologique. X est connexe $\iff$ les seuls fermés ouverts sont X et $\varnothing$.

Définition 4 :
Soit X un espace topologique.

X *est connexe par arcs* $\iff \forall x, y \in X, \quad \exists \gamma : [0,1] \longrightarrow X$ *continue telle que* $\begin{cases} \gamma(0) = x \\ \gamma(1) = y \end{cases}$

Proposition 3 :
Soient X, Y deux espaces topologiques et $f : X \longrightarrow Y$ continue. Si X est connexe alors $f(X)$ est connexe.

Remarque :
Cette proposition peut être généralisée. En effet, le caractère "lisse" des différentes connexités est conservé par des aplications de même caractère "lisse" :

- Soit f une application affine (ou linéaire). Si X est connexe par arcs polygonaux (i.e. par segments), alors $f(X)$ est connexe par arcs polygonaux.
- Soit f un $\mathcal{C}^k$-difféomorphisme. Si X est connexe par arcs, alors $f(X)$ aussi.

Proposition 4 :

i) X *connexe* $\iff X$ *ne peut pas être la réunion disjointe de deux fermés ouverts non-vides.*
$\iff \forall f : X \longrightarrow \{0,1\}$ *continue, f est constante.*

ii) *Si $X \subset Y \subset \overline{X}$, alors X connexe $\Longrightarrow Y$ connexe.*

Proposition 5 :

i) $\left.\begin{array}{l} X = X_1 \cup X_2 \cup \cdots \cup X_n \\ \forall 1 \leq i \leq n, \quad X_i \text{ connexe} \\ \forall 1 \leq i \leq n-1, \quad X_i \cap X_{i+1} \neq \varnothing \end{array}\right\} \Longrightarrow X$ *connexe*

ii) X, Y *connexes* $\Longrightarrow X \times Y$ *connexe.*

iii) X *connexe par arcs* $\Longrightarrow X$ *connexe.*

Remarque :
En général connexe $\not\Rightarrow$ connexe par arcs, cf l'espace "peigne" $\Big((\mathbb{Q} \cap [0,1[) \times [0,1]\Big) \cup ([0,1] \times \{0\})$.
Une exception notable : pour une variété différentielle (et donc en particulier pour tout groupe de Lie comme on verra p83) on a connexe $\iff$ connexe par arcs.

Chapitre II

Groupes topologiques, actions continues, exemples.

1 Normes sur $M_n(\mathbb{K})$

Dans tout le chapitre, $\mathbb{K}$ désignera le corps $\mathbb{R}$ ou $\mathbb{C}$.
Les normes de l'espace vectoriel $\mathbb{K}^n$ engendrent des normes, dites subordonnées, ou associées, sur $M_n(\mathbb{K})$: $|||A||| = \sup_{\|x\|=1} \|Ax\|$.

Norme vectorielle	Norme matricielle
$\|x\|_1 = \sum_{1\leq i\leq n} \|x_i\|$	$\|\|\|A\|\|\|_1 = \sup_{1\leq j\leq n} \sum_{1\leq i\leq n} \|a_{i,j}\|$
$\|x\|_2 = \sqrt{\sum_{1\leq i\leq n} \|x_i\|^2}$	$\|\|\|A\|\|\|_2 = \sqrt{\rho(A^*A)}$
$\|x\|_\infty = \max_{1\leq i\leq n} \|x_i\|$	$\|\|\|A\|\|\|_\infty = \sup_{1\leq i\leq n} \sum_{1\leq j\leq n} \|a_{i,j}\|$

avec le rayon spectral $\rho(A) = \max\{|\lambda| : \lambda \text{ valeur propre de } A\}$
On sait que toutes les normes sur l'espace vectoriel de dimension finie $M_n(\mathbb{K})$ sont équivalentes, mais les normes subordonnées ont l'avantage d'être multiplicatives, ie

$$|||AB||| \leq |||A|||\,|||B|||.$$

Dans la suite, toute partie de $M_{n,m}(\mathbb{K})$ sera munie de la topologie induite par celle de l'espace vectoriel normé $M_{n,m}(\mathbb{K})$.

2 Groupes topologiques, exemple fondamental

Définition 5 :

Un groupe topologique G est un groupe muni d'une topologie pour laquelle

$$\mu : \begin{array}{ccc} G\times G & \longrightarrow & G \\ (g,h) & \longmapsto & gh \end{array} \quad et \quad \iota : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1} \end{array} \quad \textit{sont continues}$$

Remarque :

ι étant involutive, i.e. $\iota^2 = \mathrm{Id}$, c'est un homéomorphisme.

Un outil simple et fondamental pour les groupes topologique est le "principe de translation" qui peut se résumer ainsi : la multiplication à gauche, resp. à droite, par x de G est un homéomorphisme de G dans G qui envoie l'élément neutre e sur x. Une propriété vraie dans un voisinage de e a donc des chances de le rester dans un voisinage de x pour tout x.

Proposition 6 :

Soit $n \geq 1$.

$GL_n(\mathbb{K})$ est un groupe topologique, ouvert et dense dans $M_n(\mathbb{K})$.

$GL_n(\mathbb{C})$ est connexe par arcs, mais $GL_n(\mathbb{R})$ n'est pas connexe.

retour p25

Démonstration :

μ est continue car composée de fonctions polynomiales. ι est continue comme composée de fractions rationnelles sur leur domaine de définition : $A^{-1} = \dfrac{{}^t\mathrm{com}\, A}{\det A}$.

$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : \det A \neq 0\} = \det^{-1}(\mathbb{K}^*)$ ouvert car det est continue.

$\overline{GL_n(\mathbb{K})} = \overline{O}_n = \bigsqcup_{0\leq k\leq n} O_k = M_n(\mathbb{K})$.

La deuxième égalité provenant de la proposition 2.

$\mathrm{Im}\det = \mathbb{R}^*$ non connexe, donc $GL_n(\mathbb{R})$ n'est pas connexe.

Montrons que $GL_n(\mathbb{C})$ est connexe par arcs :

Soient $A, B \in GL_n(\mathbb{C})$ et montrons qu'il existe un arc de $GL_n(\mathbb{K})$ qui les relie.

Soit $P : \mathbb{C} \longrightarrow \mathbb{R}$, $z \longmapsto \det(zA + (1-z)B)$

P est un polynôme non nul car $P(1) = \det A \neq 0$.

P possède un nombre fini de racines donc $\mathcal{C} := \{z : P(z) \neq 0\}$ est connexe par arcs (c'est le plan complexe privé d'un nombre fini de points).

Soit $\varphi : \begin{array}{ccc} \mathcal{C} & \longrightarrow & GL_n(\mathbb{C}) \\ z & \longmapsto & zA + (1-z)B \end{array}$

$A, B \in \varphi(\mathcal{C})$ connexe par arcs car image de $\mathcal{C}$ par une application continue, d'où $GL_n(\mathbb{C})$ connexe par arcs.

□

Tous les groupes classiques sont des sous-groupes de $GL_n(\mathbb{K})$, d'où son statut d'exemple fondamental, au même titre que $\mathcal{S}_n$ pour les groupes finis :

$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) : \det A = 1\}$

$O(n,\mathbb{K}) = \{A \in GL_n(\mathbb{K}) \,:\, {}^tA = A^{-1}\}$ $\qquad$ $U(n,\mathbb{C}) = \{A \in GL_n(\mathbb{C}) \,:\, A^* := {}^t\bar{A} = A^{-1}\}$

$SO(n,\mathbb{K}) = O(n,\mathbb{K}) \cap SL_n(\mathbb{K})$ $\qquad$ $SU(n,\mathbb{C}) = U(n,\mathbb{C}) \cap SL_n(\mathbb{C})$ $\qquad$ $\ldots$

3 Quelques applications des groupes topologiques.

Proposition 7 :
Soient $A, B \in M_n(\mathbb{K})$. Alors AB et BA ont même polynôme caractéristique χ (et donc même spectre).

Démonstration :
Si A est inversible, alors $AB = A(BA)A^{-1}$ d'où $\chi_{AB} = \chi_{BA}$ (car χ est un invariant partiel de similitude, voir p46).

Sinon, par densité il existe une suite $(A_n)_{n\in\mathbb{N}} \subset GL_n(\mathbb{K})$ telle que $A_n \xrightarrow[n\to\infty]{} A$ et donc

$$\chi_{AB}(X) = \lim_{n\to\infty} \chi_{A_nB}(X) = \lim_{n\to\infty} \chi_{BA_n}(X) = \chi_{BA}(X)$$

□

Le centre d'un groupe est un objet important. On le note $Z(G)$. C'est le noyau du morphisme

$$\begin{array}{rccccc} \phi : & G & \longrightarrow & \mathrm{Aut}\, G & & \\ & g & \longmapsto & \varphi_g : & G & \longrightarrow & G \\ & & & & h & \longmapsto & ghg^{-1} \end{array}$$

$Z(G) := \mathrm{Ker}\,\phi = \{g \in G \,:\, \varphi_g = \mathrm{Id}\} = \{g \in G \,:\, ghg^{-1} = h\}$

Proposition 8 :
Le centre de $GL_n(\mathbb{K})$ est réduit aux homothéties non nulles : $Z(GL_n(\mathbb{K})) \simeq \mathbb{K}^*$.

Démonstration :
Supposons que $\mathbb{K} = \mathbb{R}$ (le cas $\mathbb{K} = \mathbb{C}$ est plus simple et laissé en exercice).
Soit $A \in Z(GL_n(\mathbb{R}))$. Par densité et grâce à la continuité de la multiplication, A commute avec $M_n(\mathbb{R})$ et donc avec $M_n(\mathbb{C}) = M_n(\mathbb{R}) + iM_n(\mathbb{R})$. En particulier A commute alors avec $GL_n(\mathbb{C})$.
A est trigonalisable sur $\mathbb{C}$ donc il existe $P \in GL_n(\mathbb{C})$ et T triangulaire supérieure, telles que $T = PAP^{-1}$.
Comme A commute avec $GL_n(\mathbb{C})$, on a $T = A$ autrement dit A est triangulaire supérieure. De la même manière on montre que A est aussi triangulaire inférieure, donc diagonale (non nulle !).
Si on note $E_{i,j}$ les matrices élémentaires ($E_{i,j} = \delta_i \otimes \delta^j$ la matrice nulle sauf en la i-ème ligne et j-ème colonne) alors $A = \sum_{1\le k\le n} d_k E_{k,k} = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}$ et comme A commute aussi avec les matrices de transvection $T_{i,j}(a) = I_n + aE_{i,j}$,

$$T_{i,j}(1)A = AT_{i,j}(1) \iff \begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_i & \cdots & d_j & \\ & & & \ddots & \vdots & \\ & & & & d_j & \\ & & & & & \ddots \\ & & & & & & d_n \end{bmatrix} = \begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_i & \cdots & d_i & \\ & & & \ddots & \vdots & \\ & & & & d_j & \\ & & & & & \ddots \\ & & & & & & d_n \end{bmatrix} \qquad \forall 1 \le i,j \le n$$

$$\iff d_i = d_j \qquad \forall 1 \le i,j \le n$$

Donc $Z(GL_n(\mathbb{K})) = \{dI_n \,:\, d \in \mathbb{K}^*\} \simeq \mathbb{K}^*$.

□

Proposition 9 :

i) L'ensemble O_p des matrices des rang p est connexe.

ii) L'ensemble $\mathcal{P}_p$ des projecteurs de rang p est connexe.

iii) Les composantes connexes de l'ensemble des projecteurs $\mathcal{P}$ sont les $\mathcal{P}_p$.

Démonstration :

i) $O_p = \phi(GL_n(\mathbb{C})^2)$ connexe avec $\phi : \begin{array}{ccc} GL_n(\mathbb{C})^2 & \longrightarrow & M_n(\mathbb{C}) \\ (P,Q) & \longmapsto & PI_pQ^{-1} \end{array}$ continue. Rappel : $I_p = \left[\begin{smallmatrix} I_p & 0 \\ 0 & 0 \end{smallmatrix}\right]$

ii) $\psi : \begin{array}{ccc} GL_n(\mathbb{C}) & \longrightarrow & M_n(\mathbb{C}) \\ P & \longmapsto & PI_pP^{-1} \end{array}$ continue

Un projecteur est solution de $X^2 = X$. Donc comme $(PI_pP^{-1})^2 = PI_pP^{-1}$, on a $\psi(GL_n(\mathbb{C})) \subset \mathcal{P}_p$

De même, tout projecteur de rang p s'écrit PI_pP^{-1}, donc $\mathcal{P}_p \subset \psi(GL_n(\mathbb{C}))$.

Finalement, $P_p = \psi(GL_n(\mathbb{C}))$ connexe.

iii) Soient $p \neq q$. Montrons que $A \in \mathcal{P}_p$ et $B \in \mathcal{P}_q$ ne sont pas dans la même composante connexe. L'application trace restreinte aux projecteurs $\mathrm{Tr}\,|_{\mathcal{P}}$ est continue à valeurs dans $\{0, 1, \ldots, n\}$ donc $\mathrm{Tr}(A) \neq \mathrm{Tr}(B)$.

Or si P est un projecteur alors $\mathrm{Tr}(P) = \mathrm{rg}(P)$ (la réciproque n'est pas vraie) d'où $\mathrm{rg}(A) \neq \mathrm{rg}(B)$.

□

4 Groupe opérant continûment sur un ensemble.

Après cette section, on estime le lecteur suffisamment motivé sur la nécessité des groupes topologiques et des actions continues et nous en profitons pour introduire un minimum de formalisme.

Définition 6 :

Soient G un groupe et X un ensemble tous deux munis d'une topologie séparée.

Une action ou opération de G sur X, notée $G \circlearrowleft X$ est une application $\phi : \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x \end{array}$ *qui vérifie*

1) $g \cdot (g' \cdot x) = (gg') \cdot x$

2) $e \cdot x = x$.

De façon équivalente, $G \circlearrowleft X$ *si* $\psi : \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_X \\ g & \longmapsto & \psi_g(x) = g \cdot x \end{array}$ *est un morphisme de groupes.*

Une action peut donc être donnée soit par l'application ϕ, soit par le morphisme ψ. Il ne faut surtout pas les confondre : la seconde est un morphisme de groupes dont le noyau est souvent appelé noyau de l'action, la première est une simple application continue (entre autres ne jamais dire qu'un stabilisateur est un noyau, il n'est en général pas distingué !).

retour p10

Définition 7 :

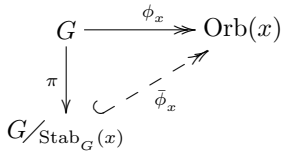
Une action est dite transitive si elle ne possède qu'une seule orbite : $\forall x \in X, \quad \mathrm{Orb}(x) = X$.

Autrement dit, $\forall x, y \in X, \exists g \in G \ : \ y = g \cdot x$.

Définition 8 :
Une action est dite libre si tous les stabilisateurs sont réduits au neutre : $\forall x \in X, \quad \mathrm{Stab}_{G}(x) = \{e\}$.
Une action est dite fidèle si tous l'intersection de tous les stabilisateurs est réduite au neutre, ou de façon équivalente si le noyau du morphisme ψ *est trivial. Le morphisme* ψ *injecte alors* G *dans* $\mathfrak{S}_{X}$.

Rappel :
On peut alors définir à x fixé $\phi_{x} : \begin{array}{ccc} G & \longrightarrow & \mathrm{Orb}(X) \\ g & \longmapsto & g \cdot x \end{array}$ et on a vu (théorème 3) qu'il existe alors une bijection

$\bar{\phi}_{x} : {}^{G}\!/_{\mathrm{Stab}_{G}(x)} \hookrightarrow\!\!\!\rightarrow \mathrm{Orb}(x)$ telle que $\bar{\phi}_{x} \circ \pi = \phi_{x}$



Ajoutons maintenant de la topologie à ces belles définitions :

Définition 9 :
Dans le cas où G *et* X *sont munis d'une topologie, on dit que l'action* $G \circlearrowleft X$ *est continue si l'application* $\phi : G \times X \longrightarrow X$ *est continue, où* $G \times X$ *est muni de la topologie produit.*

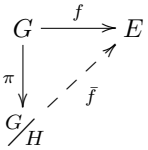
Les questions qui se posent alors sont : a-t-on une topologie sur ${}^{G}\!/_{\mathrm{Stab}_{G}(x)}$, et $\bar{\phi}_{x}$ est-il un homéomorphisme ?

Remarques :
- ϕ_{x} est continue car composée de fonctions continues. $\phi_{x} : G \longrightarrow G \times \{x\} \xrightarrow{\phi} X$.
- $\mathrm{Stab}_{G}(x) = \phi_{x}^{-1}(\{x\})$ est un sous groupe fermé de G.

Définition 10 :
Soit H *un sous groupe du groupe topologique* G. *On définit la topologie quotient sur* ${}^{G}\!/_{H}$ *par l'ensemble de ses ouverts* $\{\bar{S} \subset {}^{G}\!/_{H} : \pi^{-1}(\bar{S})$ *est ouvert dans* $G\}$. *Les ouverts de la forme* $\pi^{-1}(\bar{S})$ *sont appelés ouverts saturés.*

retour p14

Remarques :
Par construction de la topologie quotient, π est une application ouverte. Mais la propriété fondamentale de la topologie quotient (et ce pourquoi elle est définie ainsi) est la suivante : Si f est une application continue du groupe G vers un ensemble E et si f est constante sur les classes (à droite ou à gauche) modulo H, alors l'application $\bar{f}$ faisant commuter le diagramme ci-dessous est continue.



Ce triangle est souvent appelé "triangle magique", et parfois même tard le soir, "triangle magnifique".

Proposition 10 :
Soit G *un groupe topologique.*
G *séparé* $\iff \forall x \in G, \quad \{x\}$ *est fermé* $\quad \iff \{e\}$ *est fermé dans* G.

Démonstration :
La dernière équivalence est claire par principe de translation.
$\boxed{\Longrightarrow}$ Si G est séparé alors nécessairement les singletons sont fermés.
$\boxed{\Longleftarrow}$ Soit $x \neq e$ et supposons $\{x\}$ fermé. $G \setminus \{x\}$ est un ouvert contenant l'élément neutre e. Comme $\mu^{-1}(G \setminus \{x\})$

est ouvert, il existe $V \subset G \setminus \{x\}$ ouvert contenant e tel que $VV \subset G \setminus \{x\}$. Quitte à remplacer V par $V \cap V^{-1}$ (qui est bien un ouvert non vide), on peut supposer $V = V^{-1}$.
Alors les hypothèses impliquent que V et xV sont deux ouverts disjoints séparant e et x, donc G est séparé.

□

Proposition 11 :
Soit G un groupe topologique séparé et H un sous-groupe de G.

i) H *ouvert* $\Longrightarrow$ H *fermé.*

ii) H *fermé* $\Longleftrightarrow {}^{G}\!/_{H}$ *séparé.*

iii) ${}^{G}\!/_{H}$ *séparé* $\Longrightarrow \pi$ *envoie un compact sur un compact.*

Démonstration :

i) Supposons H ouvert. Son complémentaire $\complement_G H = \bigcup_{x \in G \setminus H} xH$ est réunion d'ouverts, d'où H est aussi fermé.

ii) $\boxed{\Longrightarrow}$ Soient $x, y \in G$. On veut séparer $\pi(x) \neq \pi(y)$ dans ${}^{G}\!/_{H}$. Par construction on a que $x^{-1}y \notin H$.
Considérons l'application continue $f : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, g') & \longmapsto & gx^{-1}yg' \end{array}$
$f(e,e) = x^{-1}y \notin H$ et H fermé donc puisque G est séparé, il existe U ouvert contenant $x^{-1}y$ et tel que $U \cap H = \varnothing$ (quitte à prendre $U = G/H$), ainsi que W ouvert tel que $WW \subset f^{-1}(U)$. On a alors $f(WW) \cap H = \varnothing$ donc $Wx^{-1}yW \cap H = \varnothing$, ce qui donne ainsi $yWH \cap xW^{-1}H = \varnothing$.
Donc $\pi(yW)$ et $\pi(xW^{-1})$ sont des ouverts de ${}^{G}\!/_{H}$ par définition, contenant $\pi(y)$ et $\pi(x)$ respectivement et de plus ils sont disjoints. Donc ${}^{G}\!/_{H}$ est séparé pour la topologie quotient.
$\boxed{\Longleftarrow}$ ${}^{G}\!/_{H}$ séparé $\Longleftrightarrow \{eH\}$ fermé, donc $\pi^{-1}(\{eH\}) = H$ est fermé puisque π est continue.

iii) Le fait que π envoie un compact sur un compact est un résultat général dans le cadre des topologies séparées.

□

Proposition 12 :
Soit G un groupe topologique séparé et H un sous-groupe de G. Les propositions suivantes sont équivalentes :

i) H *ouvert*

ii) $\{e\} \subset \mathring{H}$.

iii) ${}^{G}\!/_{H}$ *discret*

Démonstration :
i) $\Longrightarrow$ *ii)* Si H est ouvert alors $e \in H = \mathring{H} \Longrightarrow \{e\} \subset \mathring{H}$.
i) $\Longleftarrow$ *ii)* Si $\{e\} \subset \mathring{H}$ alors il existe un voisinage U de e dans H. D'où $H = \bigcup_{h \in H} hU$ ouvert car union d'ouverts.

i) $\Longrightarrow$ *iii)* Supposons H ouvert. Alors il est aussi fermé. De plus, π est ouverte,
donc $\pi(H) = \{eH\} \subset {}^{G}\!/_{H}$ est ouvert, et aussi fermé comme complémentaire de l'ouvert $\pi(G \setminus H)$. Conclusion, ${}^{G}\!/_{H}$ est discret, par principe de translation.
i) $\Longleftarrow$ *iii)* Si ${}^{G}\!/_{H}$ est discret, alors $H = \pi^{-1}(\{eH\})$ est ouvert.

□

Exemple :
Pour un exemple simple de cette situation, on pose $G = O(n)$ et $H = SO(n)$. Le sous-groupe H est bien ouvert dans G comme complémentaire du fermé $\{g \in G,\ det(g) = -1\}$. On a bien que ${}^{G}\!/_{H} \simeq \{1, -1\}$ est discret.

Le fait qu'un sous-groupe H est ouvert si et seulement il existe un voisinage de l'élément neutre inclus dans H est une application très simple du principe de translation. Mais ce fait s'avère extrèmement utile dans bien des situations, surtout joint au théorème de l'application ouverte dans les problèmes de surjectivité, voir chapitre VIII p83.

On peut maintenant donner un cas simple et fréquent dans lequel la réponse à notre question "$\bar{\phi}_x$ est-il un homéomorphisme ?" est positive :

Proposition 13 :
Si G est un groupe topologique compact qui agit continûment sur un ensemble X,
alors $\forall x \in X$, $\quad \bar{\phi}_x$ est un homéomorphisme.

Démonstration :
Soit $\bar{\phi}_x : {}^{G}\!/_{\mathrm{Stab}_G(x)} \longrightarrow \mathrm{Orb}(x)$ la bijection continue en question.
On rappelle qu'elle est continue car $\bar{\phi}_x^{-1}(S) = \pi(\phi_x^{-1}(S))$ ouvert pour tout ouvert $S \subset \mathrm{Orb}(x)$.
G étant compact, $\pi(G) = {}^{G}\!/_{\mathrm{Stab}_G(x)}$ est aussi compact. Tout fermé de ${}^{G}\!/_{\mathrm{Stab}_G(x)}$ étant ainsi compact, son image par l'application continue $\bar{\phi}_x$ est compact. Donc $\bar{\phi}_x$ est ouverte.
Bijective, continue et ouverte, c'est donc bien un homéomorphisme.

□

Définition 11 :
X localement compact $\Longleftrightarrow$ X est séparé et tout point possède un voisinage compact.

Définition 12 :
X dénombrable à l'infini $\Longleftrightarrow$ X est une réunion dénombrable de compacts.

Théorème 4 (d'homéomorphisme):
Soit G un groupe topologique localement compact et dénombrable à l'infini qui agit continûment et transitivement sur un espace topologique X localement compact.
Alors $\bar{\phi}_x$ est un homéomorphisme et donc ${}^{G}\!/_{\mathrm{Stab}_G(x)} \cong X$.

Remarque :
Tout d'abord, $M_n(\mathbb{K})$ est localement compact et dénombrable a l'infini. Ces hypothèses s'appliquent donc à $GL_n(\mathbb{K})$ et à tous ses sous-groupes ouverts ou fermés, pour $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.
En effet, $GL_n(\mathbb{K})$ est localement compact et dénombrable à l'infini car c'est un ouvert de l'espace vectoriel $M_n(\mathbb{K})$ (et donc les ouverts pour la topologie de $GL_n(\mathbb{K})$ sont aussi des ouverts pour celle de $M_n(\mathbb{K})$). De plus, un sous-groupe fermé de $GL_n(\mathbb{K})$ est encore localement compact et dénombrable à l'infini.

Démonstration :
$\bar{\phi}_x$ étant bijective et continue, il suffit de montrer que c'est une application ouverte, ce qui sera le cas si ϕ_x l'est.
On veut donc montrer que si U est un ouvert de G, alors $\phi_x(U) = U \cdot x$ est un ouvert de X.
Soit $g \in U$ et montrons que $g \cdot x$ est intérieur à $U \cdot x$ ou encore que x est intérieur à $g^{-1}(U \cdot x) = (g^{-1}U) \cdot x$ par principe de translation.
Comme $g^{-1}U$ est un voisinage de e, par hypothèse il existe un voisinage compact V tel que $e \in V \subset g^{-1}U$. Par continuité de la multiplication, il existe W voisinage compact de e tel que $W^2 \subset V \subset g^{-1}U$. Quitte à prendre

$W \cap W^{-1}$, on peut supposer que $W = W^{-1}$.
W étant un voisinage de e, tout hW est un voisinage de h et donc tout compact K peut être recouvert par des voisinages $kW, \quad k \in K$. Ainsi pour tout K compact, $K \subset \bigcup_{i=1}^{N} k_i W$. Il en résulte, comme G est dénombrable à l'infini, que $G = \bigcup_{i \in \mathbb{N}} g_i \cdot W$ est une union dénombrable de compacts.

Par transitivité de l'action, $X = G \cdot x = \left(\bigcup_{i \in \mathbb{N}} g_i \cdot W \right) \cdot x = \bigcup_{i \in \mathbb{N}} g_i \cdot W \cdot x$.

X étant localement compact, c'est un espace de Baire (voir en annexe, le théorème 6) et puisqu'il est d'intérieur non vide et réunion dénombrable de fermés, il existe un fermé d'intérieur non vide $g_{i_0} \cdot W \cdot x$ contenant le point $g_{i_0} \cdot w \cdot x$.
Par translation, x est donc intérieur à $w^{-1} \cdot g_{i_0}^{-1} \cdot (g_{i_0} \cdot W \cdot x) = w^{-1} \cdot W \cdot x \subset (W^2) \cdot x \subset (g^{-1}U) \cdot x$.

□

Définition 13 :
Si G est localement compact, dénombrable à l'infini et H un sous groupe fermé, on dira que G/H est un espace homogène.

5 Applications du théorème d'homéomorphisme

Elles sont de trois sortes :

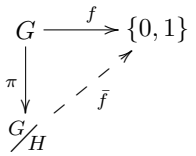
1) Comprendre des aspects topologiques du groupe G à partir de X et de $\mathrm{Stab}_G(x)$,
2) Comprendre des aspects topologiques de X à partir de G,
3) Definir une topologie sur X à partir de l'action d'un groupe topologique G.

Pour illustrer 1) montrons tout d'abord la proposition suivante :

Proposition 14 :
Soit G un groupe topologique et H un sous-groupe de G.
Si H et G/H sont connexes alors G est connexe.

retour p25

Démonstration :
Soit G un groupe topologique et H un sous groupe connexe tel que G/H soit connexe.
Pour montrer que G est connexe, on va montrer que si $f : G \longrightarrow \{0,1\}$ est continue, alors f est constante.
Tout d'abord, f est continue sur H, donc constante sur H puisque celui-ci est connexe. De même f est continue sur toutes les classes gH $(\forall g \in G)$ car chaque gH est connexe (principe de translation). f est donc constante sur toutes les classes à gauche et donc passe au quotient, ie. il existe $\bar{f}$ telle que :



La topologie quotient sur G/H assure que si f est continue et constante sur les classes alors $\bar{f}$ existe et est continue car $\bar{f}^{-1}(O) = \pi(f^{-1}(O))$ ouvert.

$\bar{f}$ est continue sur ${}^{G}\!/_{H}$ connexe donc $\bar{f}$ est constante.
Comme $\bar{f}({}^{G}\!/_{H}) = f(G)$, on conclut que f est constante sur G qui est donc connexe.

□

On a de même, voir [Mneimné-Testard, Chap. 2 Ex. 4]

Proposition 15 :
Soit G un groupe topologique et H un sous-groupe de G.
Si H et ${}^{G}\!/_{H}$ sont compacts alors G est compact.

On sait déjà que $GL_n(\mathbb{C})$ est connexe par arc d'après la proposition 6, donc connexe. Néanmoins, on va utiliser la proposition 15 pour démontrer d'une autre façon sa connexité, et surtout par une méthode plus générale.

Proposition 16 :
$GL_n(\mathbb{C})$ *est connexe.*

Démonstration :
Par récurrence sur n :

- Pour $n = 1 \quad GL_1(\mathbb{C}) = \mathbb{C}^*$ est connexe.
- $GL_n(\mathbb{C})$ agit sur $\mathbb{C}^n\backslash_{\{0\}}$ transitivement :
  En effet $\psi : \begin{array}{ccc} GL_n(\mathbb{C}) & \longrightarrow & \mathfrak{S}_{\mathbb{C}^n\backslash_{\{0\}}} \\ g & \longmapsto & \psi_g(v) = g \cdot v := g(v) \end{array}$ est clairement un morphisme car $g(g'(v)) = gg'(v)$
  Soient $v, w \in \mathbb{C}^n\backslash_{\{0\}}$. Chaque famille de vecteurs de $\mathbb{C}^n\backslash_{\{0\}}$ peut être complétée en une base d'après le théorème de la base incomplète. Ainsi, on peut construire à partir de v, w deux bases de $\mathbb{C}^n\backslash_{\{0\}}$ dont la matrice de passage g est dans $GL_n(\mathbb{C})$, réalisant le changement de base : $w = g(v)$. L'action est donc bien transitive.
  Le stabilisateur d'un élément, par exemple $\begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix}$, est $\begin{bmatrix} 1 & \mathbb{C}^{n-1} \\ 0 & GL_{n-1}(\mathbb{C}) \end{bmatrix} \simeq GL_{n-1}(\mathbb{C}) \ltimes \mathbb{C}^{n-1}$.

  L'action étant continue et transitive, les hypothèses localement compact et dénombrable à l'infini étant vérifiées on peut appliquer le théorème d'homéomorphisme pour conclure que ${}^{GL_n(\mathbb{C})}\!/_{GL_{n-1}(\mathbb{C})\ltimes\mathbb{C}^{n-1}} \cong \mathbb{C}^n\backslash_{\{0\}}$. Ce dernier étant connexe ainsi que $GL_{n-1}(\mathbb{C}) \ltimes \mathbb{C}^{n-1}$ par hypothèse de récurrence, on en déduit d'après la proposition 15 que $GL_n(\mathbb{C})$ est connexe.

□

Proposition 17 :
$GL_n^+(\mathbb{R}) := \{g \in GL_n(\mathbb{R}) \,:\, \det g > 0\}$ *est connexe.*

Démonstration :
Idem $GL_n^+(\mathbb{R})$ agit transitivement sur $\mathbb{R}^n\backslash_{\{0\}}$ pour $n \geq 2$. Laissé en exercice.

□

Proposition 18 :
SO_n *est compact et connexe.*

Démonstration :
Idem SO_n agit transitivement sur la sphère S^{n-1} de stabilisateur SO_{n-1}. Laissé en exercice.

□

Pour illustrer 2) c'est à dire l'étude des propriétés topologiques d'un ensemble grâce à l'action d'un groupe, on a déjà vu l'action $\begin{array}{ccccc} GL_m(\mathbb{K}) \times GL_n(\mathbb{K}) \times M_{m,n}(\mathbb{K}) & \longrightarrow & M_{m,n}(\mathbb{K}) \\ (P,Q,A) & \longmapsto & PAQ^{-1} \end{array}$ dont les orbites sont déterminées par le rang.
Si l'on restreint cette action à l'ensemble O_p des matrices complexes de rang p, on obtient alors une action transitive $GL_m(\mathbb{C}) \times GL_n(\mathbb{C}) \times O_p \longrightarrow O_p$.
Par le théorème d'homéomorphisme, on a ${}^{GL_m(\mathbb{C})\times GL_n(\mathbb{C})}\!/_{\text{Stab}} \cong O_p$ et comme $GL_m(\mathbb{C}) \times GL_n(\mathbb{C})$ est connexe par arcs et que le stabilisateur est un sous-groupe, cet espace homogène [2] muni de la topologie quotient est bien connexe par arcs (la projection canonique est continue).
On obtient donc la connexité par arcs de O_p grâce à cet homéomorphisme ainsi que celle de $\bar{O}_p$.

Pour illustrer 3) c'est à dire définir une topologie sur un ensemble par l'action d'un groupe, on considère la grassmanienne [3] $Gr_{m,n}(\mathbb{K}) = \{F \text{ s.e.v. de } \mathbb{K}^n \text{ tels que } \dim F = m\}$.

$GL_n(\mathbb{K})$ agit sur $Gr_{m,n}(\mathbb{K})$ transitivement (toujours par le théorème de la base incomplète, laissé en exercice), de stabilisateur un sous-groupe dit parabolique

$$P_{m,n-m}(\mathbb{K}) := \begin{bmatrix} GL_m(\mathbb{K}) & M_{m,n-m}(\mathbb{K}) \\ 0 & GL_{n-m}(\mathbb{K}) \end{bmatrix} \simeq GL_m(\mathbb{K}) \times GL_{n-m}(\mathbb{K}) \rtimes M_{m,n-m}(\mathbb{K})$$

Ainsi, on peut définir une topologie sur l'ensemble $Gr_{m,n}(\mathbb{K})$ par transport de structure en utilisant la bijection $GL_n(\mathbb{K})/P_{m,n-m} \simeq Gr_{m,n}(\mathbb{K})$ et la topologie quotient de $GL_n(\mathbb{K})/P_{m,n-m}$.
Posons maintenant $\mathbb{K} = \mathbb{R}$ et montrons que cette topologie dote la grassmannienne d'une structure d'espace compact. Effectivement, $O(n)$ agit sur $Gr_{m,n}(\mathbb{R})$ de façon transitive par le théorème de la base orthonormée incomplète. Et cette action est continue, puisque c'est la restriction de l'action de $GL_n(\mathbb{R})$ qui est continue par construction même de la topologie de la grassmannienne. Donc, par le théorème d'isomorphisme, $Gr_{m,n}(\mathbb{R})$ est homéomorphe à un quotient du groupe compact $O(n)$ par un stabilisateur fermé. Il en résulte que $Gr_{m,n}(\mathbb{R})$ est compact.

Remarque :
$Gr_{1,n}(\mathbb{K}) = \mathbb{P}^{n-1}(\mathbb{K})$ l'espace projectif que nous étudierons plus en détail à la fin du cours.

6 Produits semi-directs topologiques

Définition 14 :
Soit K un groupe topologique qui agit continûment sur un groupe topologique H par automorphisme. On note

$$\begin{array}{rccc} \varphi : & K & \longrightarrow & \operatorname{Aut} H \\ & k & \longmapsto & \varphi_k \end{array}$$

On définit le produit semi-direct topologique $K \ltimes_\varphi H$:

1. *comme ensemble $K \ltimes_\varphi H = K \times H$*
2. *comme espace topologique muni de la topologie produit*
3. *comme groupe muni du produit $(k,h) \cdot (k',h') = (kk', \varphi_{k'^{-1}}(h)h')$*

Remarque :
Attention à ne pas confondre l'action $k \cdot h$ et le produit semi-direct que l'on pourrait noter $(k,h) \cdot_\ltimes (k',h')$ s'il y a risque de confusion.

[2] Rappel : Pas forcément un groupe puisque le stabilisateur n'est en général pas distingué.
[3] Ce n'est pas un groupe mais un ensemble. En fait c'est une variété différentielle.

Proposition 19 :
Ainsi défini, $K \ltimes_{\varphi} H$ est un groupe topologique.

Démonstration :

- le produit semi-direct est bien une loi interne
- il est bien associatif :

$$\begin{aligned}(k,h)\cdot[(k',h')\cdot(k'',h'')] &= (k,h)\cdot(k'k'',\varphi_{k''^{-1}}(h')h'')\\ &= (kk'k'',\varphi_{(k'k'')^{-1}}(h)\varphi_{k''^{-1}}(h')h'')\\ &= (kk'k'',\varphi_{k''^{-1}}(\varphi_{k'^{-1}}(h)h')h'') \quad \text{car } \varphi_k \text{ automorphisme et } \varphi \text{ morphisme}\\ &= (kk',\varphi_{k'^{-1}}(h)h')\cdot(k'',h'')\\ &= [(k,h)\cdot(k',h')]\cdot(k'',h'')\end{aligned}$$

- l'élément neutre est (e_K, e_H)
- $(k,h)^{-1} = (k^{-1}, \varphi_k(h^{-1}))$

On a bien une structure de groupe et la continuité de μ et ι est alors claire.

□

Voici ce qui nous permet de reconnaître des produits semi-directs dans la nature :

Proposition 20 :
Soit G un groupe topologique et H, K deux sous-groupes topologiques tels que :

1. $H \lhd G$
2. $H \cap K = \{e\}$
3. $HK = G$

Alors G est isomorphe à $K \ltimes_{\varphi} H$, où φ est l'action par conjugaison (automorphisme) de K sur H :

$$\begin{array}{rccl}\varphi : & K & \longrightarrow & \mathrm{Aut}(H)\\ & k & \longmapsto & \varphi_k : h \longmapsto khk^{-1}\end{array}$$

Si de plus G est localement compact, dénombrable à l'infini et H fermé, alors cet isomorphisme est aussi un homéomorphisme.

Démonstration :
Par construction la multiplication $\mu : K \times H \longrightarrow G$ est continue, surjective , par (3), et injective, par (2). Pour montrer que c'est un isomorphisme, il suffit de voir que $(kh)(k'h') = (kk')\underbrace{(k'^{-1}hk'h')}_{\in H \text{ par } 1} = (kk')(\varphi_{k'^{-1}}(h)h')$
Si les hypothèses de compacité locale et de dénombrabilité à l'infini sont vérifiées, alors on fait agir K sur G/H à gauche $k\cdot(gH) := kgH$. Par 3 l'action est transitive i.e. $\mathrm{Orb}(e) = G$, et par 2 on a $\mathrm{Stab}(eH) = \{e_K\}$ d'où $\bar{\phi}_{eH} : K \cong K/\{e_K\} \cong G/H$. Un homéomorphisme inverse pour μ est alors

$$\begin{array}{rcl} G & \longrightarrow & K \times H\\ g & \longmapsto & \left(\bar{\phi}_{eH}^{-1}(gH), \left[\bar{\phi}_{eH}^{-1}(gH)\right]^{-1} g\right)\end{array}$$

On a bien $\bar{\phi}_{eH}^{-1}(gH) \in K$ et on montre que $h := \left[\bar{\phi}_{eH}^{-1}(gH)\right]^{-1} g \in H$ en faisant agir h à gauche sur la classe de e dans G/H.
Par construction, $\bar{\phi}_{eH}^{-1}(gH) \in H$ est l'unique élément (notons le k) de K tel que $g = kh$.

□

Définition 15 :
$1 \hookrightarrow H \xhookrightarrow{i} G \xrightarrow{\pi} \!\!\!\rightarrow {}^{G}\!/_{H} \longrightarrow 1$ *est une suite exacte de groupes lorsque* H *est distingué et* $\mathrm{Im}(i) = \mathrm{Ker}(\pi)$.

Rappel :
i est injective $\iff$ i est inversible à gauche $\iff$ il existe r (une rétraction) telle que $r \circ i = \mathrm{id}$.
π est surjective $\iff$ π est inversible à droite $\iff$ il existe s (une section) telle que $\pi \circ s = \mathrm{id}$.

Remarque :
On peut voir le produit semi-direct comme la suite exacte $1 \longrightarrow H \underset{\overset{\leftarrow}{r}}{\overset{i}{\hookrightarrow}} G \underset{\overset{\leftarrow}{s}}{\overset{\pi}{\twoheadrightarrow}} {}^{G}\!/_{H} \longrightarrow 1$ où la section [4] s est un morphisme de groupes d'image $K \subset G$. On dira aussi dans ce cas que la suite exacte est scindée.
Le produit est direct lorsque l'image de la section est distinguée dans G.

Le produit semi-direct topologique correspond au cas où la section s est aussi continue.
Dans la démonstration précédente, $s = \bar{\phi}^{-1}_{eH}$ et est bien continue, ceci étant assuré par l'hypothèse de locale compacité sur G.

Exemple :
Le groupe d'isotropie $G = \{ \left[\begin{smallmatrix} 1 & x \\ 0 & g \end{smallmatrix}\right], x \in \mathbb{R}^{n-1}, g \in GL_{n-1}(\mathbb{R}) \}$ est un produit semi-direct $GL_{n-1}(\mathbb{R}) \ltimes_{\varphi} \mathbb{R}^{n-1}$.

Pour le voir, on remarque que $\left[\begin{smallmatrix} 1 & x \\ 0 & g \end{smallmatrix}\right] \left[\begin{smallmatrix} 1 & x' \\ 0 & g' \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & x'+xg' \\ 0 & gg' \end{smallmatrix}\right]$.

On a la suite exacte $I_n \hookrightarrow \left[\begin{smallmatrix} 1 & \mathbb{R}^{n-1} \\ 0 & I_{n-1} \end{smallmatrix}\right] \xhookrightarrow{\mathrm{id}} \left[\begin{smallmatrix} 1 & \mathbb{R}^{n-1} \\ 0 & GL_{n-1} \end{smallmatrix}\right] \xrightarrow{\phi} \!\!\!\rightarrow \left[\begin{smallmatrix} 1 & 0 \\ 0 & GL_{n-1} \end{smallmatrix}\right] \longrightarrow I_{n-1}$

ou autrement dit $1 \hookrightarrow K \xhookrightarrow{\mathrm{id}} G \xrightarrow{\phi} \!\!\!\rightarrow H \longrightarrow 1$ avec $K \simeq \mathbb{R}^{n-1}$ et $H \simeq GL_{n-1}(\mathbb{R})$.

$\phi : \left[\begin{smallmatrix} 1 & x \\ 0 & g \end{smallmatrix}\right] \longmapsto g \sim \left[\begin{smallmatrix} 1 & 0 \\ 0 & g \end{smallmatrix}\right]$ est un morphisme de groupes et son noyau K est donc distingué dans G.
On a ainsi une section continue, $G \simeq K \ltimes_{\varphi} H$.

Pour comprendre φ, il suffit de faire agir K sur H par conjugaison et voir que

$$\begin{bmatrix} 1 & 0 \\ 0 & g \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & g \end{bmatrix}^{-1} = \begin{bmatrix} 1 & x \\ 0 & g \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & g^{-1} \end{bmatrix} = \begin{bmatrix} 1 & xg^{-1} \\ 0 & 1 \end{bmatrix} \text{ et ainsi } \varphi_g(x) = xg^{-1}.$$

Exercice :
Faire de même avec le groupe d'isotropie $\mathrm{Stab}_G(I_{r,0})$ de la leçon précédente, page 12.

Introduction à la théorie des groupes classiques, Chap. 1, 2, Rached Mneimné, Frédéric Testard, **Hermann**.
Pour les produits semi-directs et les suites exactes :
Eléments de géométrie, actions de groupes, chap. 0, Rached Mneimné, **Cassini**.
Cours d'algèbre, Chap. I, Daniel Perrin, **Ellipses**.

[4] Il faut savoir qu'une application est surjective ssi elle est inversible à droite (attention aux dyslexiques). Une section est un inverse à droite qui respecte la structure sous-jacente. Dans le cas présent, on appelle donc section un inverse à droite qui soit un morphisme de groupes.

7 Annexe 2 : Théorème de la base incomplète

Théorème 5 :
Toute famille libre d'un $\mathbb{K}$-espace vectoriel peut être complétée en une base.

Proposition 21 :
Une formulation équivalente en dimension finie est :
$GL_n(\mathbb{K})$ *agit simplement et transitivement sur l'ensemble des bases vectorielles.*

Démonstration :
Soient $p < n$ et $(a_i)_{1\leq i\leq p}$ une famille de vecteurs d'un $\mathbb{K}$-espace vectoriel de dimension n.
$(a_i)_{1\leq i\leq p}$ est libre $\iff$ la matrice A formée par les vecteurs (en colonnes) de cette famille est de déterminant non nul, i.e. $A \in GL_p(\mathbb{K})$.
Puisque toute matrice inversible de taille p peut-être complétée en une matrice inversible de taille n (par exemple en ne rajoutant que des 1 sur la diagonale), il est clair que l'on aura obtenu une base si et seulement si on a une correspondance biunivoque entre les matrices inversibles et les bases vectorielles. C'est ce à quoi correspond l'action simplement transitive en question.

□

Ce théorème fondamental, dont un corollaire nous assure qu'il existe une base dans tout espace vectoriel (y compris de dimension infinie, via l'axiome du choix) est particulièrement souple et peut se décliner en de nombreuses variantes, dont en voici une liste (non-exhaustive) ainsi que leur formulation en termes d'action transitive :

Théorèmes :

- *Toute famille libre d'un espace vectoriel euclidien peut être complétée en une base orthonormale euclidienne (pour le produit scalaire euclidien)*
  $\iff O_n(\mathbb{K})$ *agit simplement et transitivement sur l'ensemble des bases orthonormales euclidiennes.*

- *Toute famille libre d'un espace vectoriel euclidien peut être complétée en une base orthonormale directe euclidienne*
  $\iff SO_n(\mathbb{K})$ *agit simplement et transitivement sur l'ensemble des bases orthonormales directes euclidiennes.*

- *Toute famille libre d'un espace vectoriel hermitien peut être complétée en une base orthonormale hermitienne (pour le produit scalaire hermitien)*
  $\iff U_n(\mathbb{C})$ *agit simplement et transitivement sur l'ensemble des bases orthonormales hermitiennes.*

- *Toute famille libre d'un espace vectoriel hermitien peut être complétée en une base orthonormale directe hermitienne*
  $\iff SU_n(\mathbb{C})$ *agit simplement et transitivement sur l'ensemble des bases orthonormales directes hermitiennes.*

- *Toute famille libre d'un espace vectoriel symplectique* [5] *peut être complétée en une base orthonormée symplectique*
  $\iff Sp_n(\mathbb{K})$ *agit simplement et transitivement sur l'ensemble des bases orthonormées symplectiques. cf p**??***

Lorsqu'un espace vectoriel est plus généralement muni d'une forme bilinéaire quelconque [6] (non-dégénérée quand même, faut pas pousser), on ne peut pas toujours appliquer le théorème de la base incomplète.
En revanche, un outil de remplacement qui intervient alors est le théorème de Witt qui prolonge les isométries et qui peut être vu comme un théorème de multi-transitivité sous des conditions métriques (cf p50).

[5] Muni d'une forme symplectique, i.e. une forme bilinéaire antisymétrique non-dégénérée.
[6] On rappelle qu'un espace euclidien est muni d'une forme bilinéaire **symétrique définie positive**, qu'un espace symplectique est muni d'une forme bilinéaire **anti-symétrique non dégénérée**, et qu'un espace hermitien est muni d'une forme **sesquilinéaire définie positive à symétrie hermitienne**.

8 Annexe 3 : Actions classiques et leurs invariants

Le tableau qui suit, complètement non exhaustif, présente des groupes classiques, et des actions classiques qui aboutissent à des invariants totaux. Ceci peut apporter un peu de recul sur les définitions introduites dans le programme de mathématiques. Le second tableau donne une liste d'actions transitives liées au théorème de la base incomplète.

Groupe G	Ensemble X	Action $G \times X \longrightarrow X$	Espace quotient $X/_G$	Invariant
$\mathbb{K}^*$	Vecteurs non nuls : $\mathbb{K}^{n+1}\backslash_{\{0\}}$	$\lambda \cdot v = \lambda v$	$\mathbb{P}^n(\mathbb{K})$	Droites de $\mathbb{K}^{n+1}$
$SO(2)$	Couples de droites du plan	Action diagonale	$\mathbb{R}/_{\pi\mathbb{R}}$	Angles de droites
$SO(2)$	Couples de vecteurs de norme 1	$g \cdot (v, v') = (gv, gv')$	$\mathbb{R}/_{2\pi\mathbb{R}}$	Angles orientés de vecteurs
$O(2)$	Couples de droites du plan	$g \cdot (v, v') = (gv, gv')$	$\mathbb{R}/_{2\pi\mathbb{R}}$ mod $x = -x$	Angles non orientés de vecteurs
$GL_n(\mathbb{K})$	Sous-espaces vectoriels de $\mathbb{K}^n$	$g \cdot F = g(F)$	$\{0, \dots, n\}$	Dimension
$GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$	$M_{m,n}(\mathbb{K})$	$(P, Q) \cdot A = PAQ^{-1}$	$\{0, \dots, \min(m, n)\}$	Rang cf p10
$GL_n(\mathbb{K})$	Matrices diagonalisables : $\mathcal{D}_n(\mathbb{K})$	$P \cdot A = PAP^{-1}$	$\mathbb{K}^n/_{\mathfrak{S}_n}$	Valeurs propres cf p33
$GL_n(\mathbb{K})$	Matrices nilpotentes : $\mathcal{N}_n(\mathbb{K})$	$P \cdot A = PAP^{-1}$	partitions de n	Tableaux de Young cf p35
$GL_n(\mathbb{R})$	Matrices symétriques : $\mathcal{S}_n(\mathbb{R})$	$P \cdot A = PA\,{}^tP$	$\{(p, q, r) \in \mathbb{N}^3 \ : \ p + q + r = n\}$	Signature et rang cf p55
$GL_n(\mathbb{R})$	Matrices symétriques inversibles : $\mathcal{S}_n(\mathbb{R}) \cap GL_n(\mathbb{R})$	$P \cdot A = PA\,{}^tP$	$\{(p, q) \in \mathbb{N}^2 \ : \ p + q = n\}$	Signature
$PGL_2(\mathbb{C})$	Quadruplets de points de $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ trois premiers distincts	Action diagonale $A \cdot z = \frac{az+c}{bz+d}$	$\mathbb{P}^1(\mathbb{C})$	Birraport cf p100 $\frac{z_4-z_2}{z_4-z_1} : \frac{z_3-z_2}{z_3-z_1}$
$GL_n(\mathbb{Z})$	Sous-réseaux de $\mathbb{Z}$	$g \cdot \mathcal{R} = g(\mathcal{R})$	$0 \leq r \leq n$ $d_1 \vert d_2 \vert \dots \vert d_r \in \mathbb{N}$	Rang et invariants de la base adaptée
$GL_n(\mathbb{C})$	$M_n(\mathbb{C})$	$P \cdot A = PAP^{-1}$	$P_1 \vert P_2 \vert \dots \vert P_n$ Polynômes unitaires	Invariants de similitude cf p33
$GA_2(\mathbb{R})$	Coniques du plan	$g \cdot \mathcal{C} = g(\mathcal{C})$	Ellipses, hyperboles, paraboles...	Classification des coniques
Is^+	Ellipses	$g \cdot \mathcal{E} = g(\mathcal{E})$	$\{(a, b) \in \mathbb{N}^2 \ : \ a \leq b\}$	Petit axe / Grand axe cf p117
$\mathbb{R}^* \times Is^+$	Ellipses	$g \cdot \mathcal{E} = g(\mathcal{E})$	$]0, 1]$	Excentricité

Actions transitives :	**Actions simplement transitives** :
$\mathfrak{S}_n$ sur $\{1, \dots, n\}$ $\quad$ Stab$(k) = \mathfrak{S}_{\{1,\dots,n\}\backslash_{\{k\}}}$	$GL_n(\mathbb{K})$ sur les bases vectorielles de $\mathbb{K}^n$ cf p29
$GL_n(\mathbb{K})$ sur $\mathbb{K}^n\backslash_{\{0\}}$ $\quad$ Stab$(e_1) = GL_{n-1}(\mathbb{K}) \ltimes \mathbb{K}^{n-1}$	$O(n)$ sur les bases orthonormales euclidiennes cf p29
$O(q)$ sur les k-sous-espaces vectoriels isotropes	$SO(n)$ sur les bases orthonormales directes euclidiennes cf p29
$SO(n)$ sur S^{n-1} $\quad$ Stab$(e_1) = SO(n-1)$	$SU(n)$ sur les bases orthonormales directes hermitiennes cf p29
$SU(n)$ sur S^{2n-2} $\quad$ Stab$(e_1) = SU(n-1)$ cf p81	$Sp_n(\mathbb{K})$ sur les bases orthonormées symplectiques cf p29
	$GA_n(\mathbb{K})$ sur les repères affines, i.e. les bases de $\mathbb{A}^n$ cf p94

9 Annexe 4 : Compacité locale

Voici tout le matériel nécessaire pour aborder la compacité locale.

Définition 16 :
Un espace est dit localement compact s'il est séparé et si tout point de cet espace possède un voisinage ouvert à clôture compacte.

On trouve aussi dans la littérature une autre définition :

Définition 17 :
Un espace est dit localement compact s'il est séparé et si tout point de cet espace possède une base de voisinages ouverts à clôture compacte.

Le fait que ces deux définitions coïncident s'appuie fortement sur la séparabilité.

Proposition 22 :
Les définitions 16 et 17 sont équivalentes.

Démonstration :
Il suffit de montrer que la première implique la seconde.
Soit donc x dans X, localement compact selon la première définition. Soit V un voisinage ouvert de x. On veut trouver un voisinage compact de x contenu dans V. Soit U un voisinage ouvert de x à fermeture compacte, quitte à prendre l'intersection avec V, on peut supposer que $U \subset V$. Supposons construit un voisinage ouvert W de x inclus dans U tel que $\overline{W} \subset U$. Alors, $\overline{W}$ est compact et inclus dans V, ce qui confirmerait la proposition. Montrons donc l'existence d'un tel ouvert W. Soit δU la frontière de U, qui est compacte. Pour tout x_i de δU, il existe un ouvert U_i de x_i et un ouvert W_i de x qui les séparent. Le compact δU est recouvert de tous les U_i et donc par un nombre fini de ceux-ci. Posons W l'intersection finie des W_i correspondant, alors W est un voisinage ouvert de x et par construction $\overline{W}$ n'intersecte pas δU. Il en résulte $\overline{W} \subset U$.

□

$\mathbb{R}$, $\mathbb{C}$ et plus généralement tout espace de dimension finie sur ces corps sont localement compacts pour la topologie métrique. Cela vient du fait qu'un compact est un fermé borné.
Si X est localement compact, tout ouvert O de X l'est également. Cela vient du fait que tout ouvert de O est un ouvert de X ; on se raméne alors à la definition de la compacité par les recouvrements ouverts.
Si X est localement compact, alors tout fermé de X l'est également. Cela vient du fait que l'intersection d'un compact avec un fermé est encore compact, puisque c'est un fermé dans un compact. Avec ces deux propriétés, on peut en faire une troisième :

Proposition 23 :
Si X est localement compact et si $X_n \subset X_{n-1} \subset \ldots \subset X_0 = X$ est une suite d'espaces topologiques tels que X_i est soit fermé soit ouvert dans X_{i-1}, alors X_n est localement compact.

La preuve suivante est instructive, à defaut d'être efficace (voir une preuve express à la fin) :

Proposition 24 :
$\mathbb{Q}$ *n'est pas localement compact.*

Démonstration :
Supposons $\mathbb{Q}$ localement compact. Alors tout point de $\mathbb{Q}$ aurait un voisinage ouvert à clôture compacte. Choisissons un ouvert U de 0 à clôture compacte. Tout ouvert de U est également à clôture compacte, donc on peut prendre

pour U un intervalle ouvert $]-t,t[\cap\mathbb{Q}$, où t est un irrationnel (cela forme effectivmeent une base d'ouverts de 0 dans $\mathbb{Q}$). L'ensemble $]-t,t[\cap\mathbb{Q} = [-t,t]\cap\mathbb{Q}$ est à la fois ouvert et fermé dans $\mathbb{Q}$ car t est irrationnel. Donc, U est compact. Maintenant, on prend une suite x_n de rationnels de U tendant vers t. C'est une suite dans un compact qui ne possède pas de sous-suite convergente dans le-dit compact, puisque toutes ces sous-suites tendent vers t. Ce qui contredit la compacité de U.

□

Voici maintenant de quoi briller en société.

Un espace topologique est appelé espace de Baire s'il vérifie que toute intersection dénombrable d'ouverts denses est encore dense. Le fait qu'on ait besoin dans le cours d'espaces topologiques localement compacts vient entre autres du théorème.

Théorème 6 :
Tout espace localement compact est un espace de Baire.

retour p24

Démonstration :
Soit donc (U_j) une suite d'ouverts partout denses. Pour prouver que l'intersection est partout dense, il suffit de montrer que, si V est un ouvert non vide quelconque, il existe un point commun à V et à tous les U_j. Nous allons construire par récurrence une suite d'ensembles fermes B_j vérifiant $B_1 \subset U_1 \cap V$ et $B_{j+1} \subset U_{j+1} \cap \overset{\circ}{B}_j$. Il nous suffira alors de montrer que l'intersection des B_j est non vide pour avoir le résultat. Nous allons exiger que les B_j soient des compacts d'intérieur non vide. L'ouvert $U_1 \cap V$ étant non vide, il est voisinage de l'un quelconque de ses points x, et comme l'espace est localement compact, il existe B_1 un voisinage de x compact contenu dans $U_1 \cap V$. On construit de meme B_{j+1} à partir de $\overset{\circ}{B}_j \cap U_{j+1}$. Or, une suite décroissante de compacts non vides à une intersection non vide (c'est une conséquence de la propriété de Borel-Lebesgue), l'intersection des B_j est non vide.

□

Remarque :
On a une preuve express que $\mathbb{Q}$ est non localement compact car $\mathbb{Q}$ n'est pas de Baire. Il suffit de prendre une suite r_n de tous les nombres rationnels et les ouverts denses $X_n := \mathbb{Q}\backslash\{r_n\}$ ont une intersection vide.

Notons que l'ensemble des irrationnels n'est pas localement compact alors que c'est un espace de Baire. Notons pour finir que la locale compacité est essentielle pour définir la compactification d'Alexandroff, c'est à dire la possibilité de prolonger l'espace X en un espace $\overline{X}$ qui est compact.

Chapitre III

Réduction des endomorphismes

Nous allons appliquer systématiquement la méthode du premier chapitre : définir, si nécessaire en motivant son importance, une action continue de groupe topologique sur un espace topologique, puis trouver des invariants totaux pour cette action et enfin regarder les clôtures d'orbites ou comment ces invariants totaux évoluent après passage à la limite.
On étudie ici l'action de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$ par conjugaison. Ce problème, qui se ramène à l'étude des matrices semblables (et donc aux fameux invariants de similitude), est beaucoup plus difficile, que celui des matrices équivalentes. Tout d'abord, il va dépendre du corps choisi (mais pas dramatiquement) et notre étude va se limiter au cas $\mathbb{K} = \mathbb{C}$. Mais surtout, la classification est radicalement différente si on s'intéresse aux matrices diagonalisables, ou si elles sont nilpotentes. On étudiera les deux, et le cas général se fait facilement à l'aide de la décomposition de Dunford. L'invariant total des matrices diagonalisables est le spectre avec multiplicité, et celui des matrices nilpotentes est la suite des dimensions des noyaux emboités. Pour l'étude topologique, il sera pratique de stocker l'information des noyaux emboités sous forme de tableaux de Young.

1 Action $GL_n(\mathbb{C}) \circlearrowleft \mathcal{D}_n(\mathbb{C})$ par conjugaison

On note $\mathcal{D}_n(\mathbb{C})$ les matrices diagonalisables sur $\mathbb{C}$. On rappelle que $O_{_A} = \{PAP^{-1} \,:\, P \in GL_n(\mathbb{C})\}$ est l'orbite de A sous l'action de $GL_n(\mathbb{C})$ par conjugaison (matrices semblables à A). On considère le spectre d'une matrice comme la donnée de n complexes (non nécessairement distincts) à permutation près ; un spectre est donc un élément de $\mathbb{C}^n\!/_{\mathfrak{S}_n}$.

Théorème 7 :

$$\begin{array}{rccll} \varphi : & \mathcal{D}_n(\mathbb{C})/_{GL_n(\mathbb{C})} & \longrightarrow & \mathbb{C}^n/_{\mathfrak{S}_n} & \textit{est bijective} \\ & O_{_A} & \longmapsto & \mathrm{Spec}(A) & \end{array}$$

Démonstration :
φ est bien définie car deux matrices diagonalisables semblables ont même spectre. Donc le spectre ne dépend pas du choix de l'élément A de l'orbite $O_{_A}$.
φ est clairement surjective puisque pour tout spectre (à permutation près), il existe une matrice diagonale dont les éléments diagonaux sont les éléments du spectre (valeurs propres).
Supposons que $\mathrm{Spec}(A) = \mathrm{Spec}(B)$. Comme A et B sont diagonalisables, elles sont semblables à la matrice diagonale des valeurs propres, donc appartiennent à la même orbite, $O_{_A} = O_{_B}$ et ainsi φ est injective.

□

Corollaire 3 :
Le polynôme caractéristique ou le spectre sont des invariants totaux de similitude pour les matrices diagonalisables.

Remarque :
En revanche, le polynôme minimal est un invariant mais pas un invariant total. Il est facile d'en trouver un exemple : les matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

ont même polynôme minimal mais ne sont pas semblables.

L'étude est donc plus simple que ce que l'on imaginait. Maintenant, l'étude topologique, c'est à dire la décomposition des clôtures d'orbites en orbites. Et là, les choses sont encore plus simples, puisque nous allons montrer que les orbites sont fermées. Et on obtient même une réciproque, c'est à dire, une caractérisation topologique de la diagonalisation !

Proposition 25 :
A est diagonalisable $\iff$ O_A est fermé dans $M_n(\mathbb{C})$

Démonstration :

$\boxed{\Longrightarrow}$ Supposons $A \in M_n(\mathbb{C})$ diagonalisable. Soit $(B_k)_{k\in\mathbb{N}} \subset O_A$ telles que $B_k \xrightarrow[k\to\infty]{} B$. Montrons que $B \in O_A$.

$B_k \in O_A \Longrightarrow \prod_{i=1}^{n}(B_k - \lambda_i I_n) = 0$ avec $(\lambda_i)_{1\le i\le n} \subset \mathrm{Spec}(A)$ distinctes (et de multiplicité 1 car A diagonalisable).

A la limite ($k\to\infty$), $\prod_{i=1}^{n}(B - \lambda_i I_n) = 0$. Donc B annulé par un polynôme scindé à racines simples est diagonalisable.

On pose $r_{i,k} := \dim \mathrm{Ker}(B_k - \lambda_i I_n)$ et $r_i := \dim \mathrm{Ker}(B - \lambda_i I_n)$ les multiplicités géométriques. On a

1. $\sum_{i=1}^{n} r_{i,k} = n$ car comme B_n est diagonalisable, par le lemme des noyaux $E = \oplus \mathrm{Ker}(B_k - \lambda_i I_n)$
2. $\sum_{i=1}^{n} r_i = n$ car B est diagonalisable (et toujours le lemme des noyaux)
3. $r_i \ge r_{i,k}$ par semi-continuité du rang, voir remarque p13

Donc $\forall k \in \mathbb{N}$, $r_i = r_{i,k}$ et finalement $\mathrm{Spec}(B_k) = \mathrm{Spec}(B)$ et $B \in O_A$.

$\boxed{\Longleftarrow}$ Par contraposée, supposons A non diagonalisable, alors la décomposition de Dunford donne $A = D + N$, avec N non nulle par hypothèse. Quitte à prendre un conjugué de A, on peut supposer que D est diagonale et N est une matrice de Jordan nilpotente. A l'aide des dimension des noyaux emboités, on obtient que pour tout λ non nul, $D + \lambda N$ est semblable à A. Mais, en faisant tendre λ vers 0, on obtient D qui n'est pas semblable à A puisque D est par nature diagonalisable. L'orbite O_A n'est donc pas fermée.

□

Remarque :
On peut montrer en exercice que $\mathcal{D}_n(\mathbb{C})$ est dense dans $M_n(\mathbb{C})$ et son intérieur est constitué des matrices de valeurs propres différentes.

2 Action $GL_n(\mathbb{C}) \circlearrowleft \mathcal{N}_n(\mathbb{C})$ par conjugaison

$\mathcal{N}_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) : A \text{ est nilpotente i.e. } \exists m \, : \, A^m = 0\}$
n'est pas un sous-espace vectoriel de $M_n(\mathbb{C})$ mais un cône (stable par homothétie) :
$\forall A \in \mathcal{N}_n(\mathbb{C}), \forall \lambda \in \mathbb{C}, \quad \lambda A \in \mathcal{N}_n(\mathbb{C})$

Soit $A \in \mathcal{N}_n(\mathbb{C})$. On va noter $K_i = \mathrm{Ker}(A^i)$ ses sous-espaces caractéristiques. On a :

$$\{0\} = K_0 \subsetneq K_1 \subset K_2 \subset \cdots \subset K_n = \mathbb{C}^n$$

Nous allons voir que la suite des $\dim K_i$ s'essouffle.

Lemme :
$\forall 1 \leq i \leq n-1, \qquad \dim K_i - \dim K_{i-1} \geq \dim K_{i+1} - \dim K_i$

Démonstration :
On considère les morphismes : $\begin{array}{ccccc} K_{i+1} & \xrightarrow{\nu} & K_i & \xrightarrow{\pi_i} & {}^{K_i}\!/_{K_{i-1}} \\ X & \longmapsto & AX & \longmapsto & \overline{AX} \end{array}$

$\mathrm{Ker}(\pi_i \circ \nu) = (\pi_i \circ \nu)^{-1}(\{\bar{0}\}) = \nu^{-1}\big(\pi_i^{-1}(\{\bar{0}\})\big) = \nu^{-1}(K_{i-1}) = K_i \quad$ donc ${}^{K_{i+1}}\!/_{K_i} \hookrightarrow {}^{K_i}\!/_{K_{i-1}}$

De cette injection on déduit que $\dim\left({}^{K_{i+1}}\!/_{K_i}\right) \leq \dim\left({}^{K_i}\!/_{K_{i-1}}\right)$ d'où le résultat.

□

Définition 18 :
Un tableau de Young de taille n est une partition de n :
$(d_i)_{1 \leq i \leq m} \subset \mathbb{N}^*$ *telle que* $d_m \leq \cdots \leq d_1$, $\displaystyle\sum_{i=1}^{m} d_i = n$ *représentée par n cases juxtaposées*

d_m *cases* $\rightarrow$ □
⋮
d_2 *cases* $\rightarrow$ □□□ … □
d_1 *cases* $\rightarrow$ □□□ ……. □

Définition 19 :
Le tableau de Young $T := T(A)$ associé à la matrice nilpotente A est celui donné par la partition
$d_i(T) = \dim K_i - \dim K_{i-1}$. *On notera aussi* $k_i(T) := \dim K_i = \displaystyle\sum_{j=1}^{i} d_j(T)$.

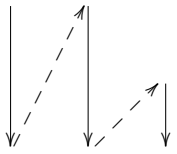
Il est raisonnable de se demander pourquoi cette façon d'assembler des boîtes en tableaux serait si pratique. Une première raison en est qu'on peut lire dans le tableau une information horizontale (les noyaux emboités) et une verticale que nous allons présenter.

Etude préliminaire :
Soit $A \in \mathcal{N}_n(\mathbb{C})$ une matrice nilpotente d'ordre m. On a la suite de noyaux emboîtés $\{0\} \subsetneq K_1 \subset \cdots \subset K_m = \mathbb{C}^n$.
On part d'un sous-espace G_m supplémentaire de K_{n-1} dans $K_m = \mathbb{C}^n$, donc tel que $K_{n-1} \oplus G_m = K_m$
et on note $\mu_m := \dim G_m = \dim K_m - \dim K_{m-1}$.

Soit $(v_m^1, \dots, v_m^{\mu_m})$ une base de G_m. Ensuite, on construit un supplémentaire G_r de K_{r-1} dans K_r de la façon suivante : on montre (exercice !) que $(Av_m^1, \dots, Av_m^{\mu_m})$ est une famille libre qui engendre un espace intersectant K_{m-1} trivialement, famille que l'on peut compléter en une base $(Av_m^1, \dots, Av_m^{\mu_m}, v_{m-1}^{\mu_m+1} \dots, v_{m-1}^{\mu_{m-1}})$ d'un supplémentaire G_{m-1} de K_{m-1} dans K_m.
Par itération, on peut remplir le tableau de Young de A ligne par ligne, successivement en multipliant par A puis en complétant.

Nouveau jeu de l'été : le sudoku "variante de l'algébriste". Compléter le tableau de Young suivant :

v_m^1	v_m^2	$\dots$	$v_m^{\mu_m}$							
Av_m^1	Av_m^2	$\dots$	$Av_m^{\mu_m}$	$v_{m-1}^{\mu_m+1}$	$\dots$	$v_{m-1}^{\mu_{m-1}}$				
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$			
$A^{n-r}v_m^1$	$A^{n-r}v_m^2$	$\dots$	$A^{n-r}v_m^{\mu_m}$		$\dots$			$v_r^{\mu_r}$		
$\vdots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$A^{m-1}v_m^1$		$\dots$			$\dots$					$v_1^{\mu_1}$

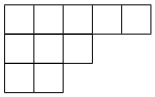
On obtient alors en relisant le tableau colonne par colonne et de haut en bas 

une nouvelle base $(v_m^1, Av_m^1, \dots, A^{m-1}v_m^1, v_m^2, \dots, A^{m-1}v_m^2, \dots, v_1^{\mu_1})$ de $\mathbb{C}^n$ dans laquelle A s'écrit $\begin{bmatrix} J_{d_1^*} & & 0 \\ & \ddots & \\ 0 & & J_{d_k^*} \end{bmatrix}$.

C'est la réduite de Jordan (ou forme de Jordan) semblable à A.

Où $(d_j^*)_{1 \le j \le k}$ est la partition duale (obtenue en lecture verticale) et $J_p = \begin{bmatrix} 0 & & & 0 \\ 1 & 0 & & \\ & \ddots & 0 & \\ 0 & & 1 & 0 \end{bmatrix} \in M_p(\mathbb{R})$ est la matrice de Jordan de taille p.

Exemple :
Soit une matrice $A \in M_{10}(\mathbb{C})$ nilpotente d'ordre 3 telle que $\dim K_1 = 2$ et $\dim K_2 = 5$.
$\dim K_3 - \dim K_2 = 5$, $\dim K_2 - \dim K_1 = 3$, $\dim K_1 - \dim K_0 = 2$

La partition $5 \ge 3 \ge 2$ de tableau  a pour partition duale $3 \ge 3 \ge 2 \ge 1 \ge 1$.

Donc dans la nouvelle base, A s'écrit $\begin{bmatrix} J_3 & & & & \\ & J_3 & & & \\ & & J_2 & & \\ & & & J_1 & \\ & & & & J_1 \end{bmatrix} = \begin{bmatrix} 0&0&0 & & & & \\ 1&0&0 & & & & \\ 0&1&0 & & & & \\ & & & 0&0&0 & \\ & & & 1&0&0 & \\ & & & 0&1&0 & \\ & & & & & & 0\,0 \\ & & & & & & 1\,0 \\ & & & & & & & 0 \\ & & & & & & & & 0 \end{bmatrix}$

Théorème 8 :
Soient A, B deux matrices nilpotentes. Alors leur classe de similitude est caractérisée par leur tableau de Young :
$O_A = O_B \iff T(A) = T(B)$

Démonstration :

$\boxed{\Longrightarrow}$ Supposons $O_A = O_B$ c'est à dire A et B similaires. Alors $\exists P \in GL_n(\mathbb{C})$: $B = PAP^{-1}$, d'où $\dim \operatorname{Ker} B^i = \dim \operatorname{Ker}(PA^iP^{-1}) = \dim \operatorname{Ker} A^i \Longrightarrow T(A) = T(B)$.

$\boxed{\Longleftarrow}$ Supposons $T(A) = T(B)$. Alors A et B ont la même partition $(d^A) = (d^B)$ donc la même partition duale $(d^{A*}) = (d^{B*})$ et ainsi la même réduite de Jordan. Donc A et B sont semblables, i.e. $O_A = O_B$.

□

Soit $p(n)$ le nombre de partitions possibles du nombre n. Par exemple $p(4) = 5$ correspondant aux partitions de 4 ;

$$4, \quad 3 \geq 1, \quad 2 \geq 2, \quad 2 \geq 1 \geq 1, \quad 1 \geq 1 \geq 1 \geq 1$$

Ce nombre $p(n)$ compte les tableaux de Young à n blocs, et donc les classes de matrices nilpotentes pour la conjugaison. Pour la calculer, nous allons utiliser l'anneau des séries formelles en l'indeterminée X. Effectivement, il est pratique de considérer la *série génératrice*

$$s(X) = \sum_{i=0}^{\infty} p(n) X^n.$$

On a alors facilement :

Corollaire 4 :
Le nombre de classes de conjugaisons pour l'action de $GL_n(\mathbb{C})$ sur le cône nilpotent $\mathcal{N}_n(\mathbb{C})$ est le nombre $p(n)$ égal au coefficient en X^n du produit infini

$$s(X) = \prod_{k=1}^{\infty} \frac{1}{1 - X^k}.$$

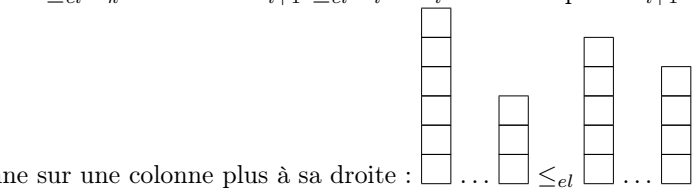
On se convaincra facilement de la preuve en cherchant le terme en X^4 dans l'expression de droite que l'on calcule sous la forme

$$\prod_{1}^{\infty} \frac{1}{1 - X^k} = (1 + X + X^2 + \ldots)((1 + X^2 + (X^2)^2 + \ldots)(1 + X^3 + (X^3)^2 + \ldots)(1 + X^4 + (X^4)^2 + \ldots) \ldots$$

Le terme est donc $X^4 + XX^3 + (X^2)^2 + (X)^2X^2 + (X)^4 = 5X^4$, on voit bien comment ce produit infini "compte" les partitions de n pour tout n.

3 Clôture d'orbites nilpotentes

Définition 20 :
On peut ordonner l'ensemble des tableaux de Young de taille n (voir en annexe p45 l'ordre des partitions de 6*) :*
$T(A) \leq T'(A) \iff k_i(T) \leq k_i(T') \quad \forall i.$

Remarque :
On montre facilement que c'est l'ordre engendré par $\leq_{el}$:
$T \leq T' \iff T = T_1 \leq_{el} T_2 \leq_{el} \cdots \leq_{el} T_k = T'$ avec $T_{i+1} \leq_{el} T_i$ si T_i est identique à T_{i+1} après qu'un bloc soit "tombé" du sommet d'une colonne sur une colonne plus à sa droite : 

Il est possible d'affiner cet ordre élémentaire en prenant la colonne immédiatement à sa droite, mais cela demande un peu plus de travail et sera inutile pour la suite.

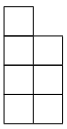
Théorème 9 :
Soit A une matrice nilpotente de taille n. Alors $\overline{O}_A = \bigsqcup_{T(B) \leq T(A)} O_B$

Démonstration :
Par double inclusion,

$\boxed{\subset}$ Si $A_m \xrightarrow[m\to\infty]{} A$ alors $k_i(T(A)) = \dim \operatorname{Ker} A^i \geq \dim \operatorname{Ker} A_m^i = k_i(T(A_m))$ car à la limite le noyau ne peut pas "rétrécir" par semi-continuité inférieure du rang.

$\boxed{\supset}$ Montrons que si $T(B) \leq_{el} T(A)$ alors $O_B \subset \overline{O}_A$.

Comme chaque colonne correspond à un bloc de Jordan, il suffit de le montrer pour deux colonnes, d'après la remarque qui précède.

Soient $p \geq q$, une matrice B de type  (hauteurs p, q avec $p+q=n$) et A de type  (hauteurs $p+1, q-1$).

Soit $A_m = \begin{bmatrix} J_p & 0 \\ 0 & J_q \end{bmatrix} + \frac{1}{m} E_{n,p}$. Par exemple pour $n = 4+3$, $A_m = \begin{bmatrix} 0&0&0&0 & & & \\ 1&0&0&0 & & & \\ 0&1&0&0 & & & \\ 0&0&1&0 & & & \\ & & & & 0&0&0 \\ & & & & 1&0&0 \\ & & & \frac{1}{m} & 0&1&0 \end{bmatrix}$. On vérifie facilement que :

1. $\operatorname{rg} A_m = n-2$
2. $A_m^{p+1} = 0$
3. $A_m^p \neq 0$

Par le théorème 8, on a $A \sim A_m \implies O_A = O_{A_m}$. Comme $\lim_{m\to\infty} A_m = \begin{bmatrix} J_p & 0 \\ 0 & J_q \end{bmatrix} = B' \sim B$, on a bien $B' \in \overline{O}_{A'} = \overline{O}_A$. Comme $\overline{O}_A$ est stable par l'action de $GL_n(\mathbb{C})$, par continuité il vient $O_B \subset \overline{O}_A$.
Conclusion : si $T(B) \leq T(A)$, alors $T(B) = T(B_0) \leq_{el} T(B_1) \leq_{el} \cdots \leq_{el} T(B_r) = T(A)$.
On a $O_B = O_{B_0} \subset \overline{O}_{B_1} \subset \overline{\overline{O}}_{B_2} \subset \cdots \subset \overline{\vdots}_{B_r} = \overline{O}_A$

□

On en déduit :

Corollaire 5 :
L'orbite minimale nulle est la seule orbite fermée. Elle est caractérisée par le tableau $\underbrace{\square\square\square\square\square}_{n}$

L'orbite maximale est la seule orbite ouverte. Elle est caractérisée par le tableau $\left.\begin{array}{c}\square\\\square\\\square\\\square\\\square\end{array}\right\}n$

4 Action $GL_n(\mathbb{C}) \circlearrowleft M_n(\mathbb{C})$ par conjugaison

Revenons au cas général, c'est à dire l'action de $GL_n(\mathbb{C})$ sur $M_n(\mathbb{C})$ par conjugaison. Comme cette action respecte le polynôme caractéristique, on peut se ramener à l'action de $GL_n(\mathbb{C})$ sur $M_n(\chi) = \{B \in M_n(\mathbb{C}) : \chi_B = \chi\}$ l'ensemble des matrices de polynôme caractéristique χ, où $\chi = \prod(X - \lambda_i)^{n_i}$ est un polynôme de degré n donné. Posons $N(A)_i = (A - \lambda_i I_n)|_{\mathrm{Ker}(A-\lambda_i I_n)^{n_i}}$ qui est nilpotente sur un espace de dimension n_i.

Théorème 10 :
Soient $A, B \in \chi_n(\mathbb{C})$. *Alors* $A \sim B \iff \forall i, \quad T(N(A)_i) = T(N(B)_i)$

Démonstration :
Laissé en exercice.

□

Question :
Combien y a-t-il d'orbites pour l'action de $GL_n(\mathbb{C})$ sur $M_n(\chi)$?
Montrer qu'une orbite O_A est fermée si et seulement si A est diagonalisable.

5 Pour en finir avec les invariants de similitude

Il reste encore deux petites choses à regarder. La première est de comprendre comment résoudre le problème analogue sur le corps de réels. C'est finalement très simple, puisqu'un résultat classique dit que :

Proposition 26 :
Pour des matrices réelles, $GL_n(\mathbb{C})$*-semblable* $\iff$ $GL_n(\mathbb{R})$*-semblable.*

Démonstration :
Voir TD.

□

Une orbite $GL_n(\mathbb{R}) \cdot A$ d'une matrice réelle A est donc exactement l'intersection de $GL_n(\mathbb{C}) \cdot A$ avec $M_n(\mathbb{R})$. Ce sera loin d'être le cas dans le chapitre suivant sur l'action de congruence où l'intersection de $GL_n(\mathbb{C}) \cdot A$ avec $M_n(\mathbb{R})$ sera une union disjointe d'orbites pour l'action de $GL_n(\mathbb{R})$.

La seconde est de faire le lien entre les invariants de similitude que nous venons de voir, avec ce que l'on appelle couramment "facteurs invariants" (de similitudes) ou forme de Smith.

Pour l'instant, les invariants de similitude totaux d'une matrice quelconque sont **l'ensemble des tableaux de Young pour chaque valeur propre**.
Mais on peut aussi obtenir des invariants (totaux) de similitude par des opérations sur les lignes et colonnes de la matrice caractéristique et qui nous donnent la forme de Smith de cette dernière (voir exemple plus loin).
Ces deux types d'objets, matrices de Jordan et polynômes de la forme de Smith portent la même information, invariante totalement par similitude.

On va voir que ces deux invariants peuvent s'obtenir aisément l'un à partir de l'autre et inversement. Par exemple, le polynôme minimal se trouve être le premier des invariants de Smith.
On peut aussi le construire grâce aux informations données par la première colonne de chaque tableau de Young :
Pour le premier facteur invariant, il n'est pas difficile de constater que

$$F_1(A) = \pi_{_A} = \prod_{\lambda_i \in \mathrm{Spec}(A)} (X - \lambda_i)^{d_1^*(\lambda_i)},$$

avec $d_1^*(\lambda_i)$ le nombre de cases de la **première colonne** du tableau de Young correspondant à la valeur propre λ_i.
Ce résultat se généralise en :

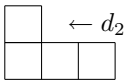
$$F_k(A) = \prod_{\lambda_i \in \mathrm{Spec}(A)} (X - \lambda_i)^{d_j^*(\lambda_i)},$$

avec $d_j^*(\lambda_i)$ le nombre de cases de la j**-ème colonne** du tableau de Young correspondant à la valeur propre λ_i.
Nous illustrons cela sur deux exemples :

Exemples : Soit $A = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}$. $\quad \chi_{_A}(\lambda) = \begin{vmatrix} 2-\lambda & 0 & & & \\ 0 & 2-\lambda & & & 1 \\ & & 2-\lambda & 0 & 0 \\ & & 3 & 2-\lambda & 0 \\ & & 0 & 0 & 4-\lambda \end{vmatrix} = -(\lambda-2)^4(\lambda-4)$

Ainsi $\mathrm{Spec}(A) = \{2, 4\}$.

- On regarde $K_1 = Ker(A - 2 \cdot I_{_5}) =< (1,0,0,0,0), (0,1,0,0,0), (0,0,0,1,0) >$ $\quad \dim K_1 = 3$.
  Puis $K_2 = Ker[(A - 2 \cdot I_{_5})^2] =< (1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0) >$ $\quad \dim K_2 = 4$.
  Pas besoin d'aller plus loin puisque la suite $d_i = \dim K_i - \dim K_{i-1}$ s'essouffle (donc $\dim K_3 = 4$).

  On a la partition de 4 suivante : $d_3 = 0 < d_2 = 1 \leq d_1 = 3$ correspondant au tableau  ($\leftarrow d_2$, $\leftarrow d_1$)
  En lisant le tableau verticalement, la partition duale est $2 \geq 1 \geq 1$. Son premier élément, correspondant au nombre de cases de la première colonne, nous donne la multiplicité de la valeur propre 2 dans le polynôme minimal, à savoir 2 ici (ou encore la taille du bloc de Jordan associé à la partie nilpotente associée à la valeur propre 2).
  Le deuxième nous donne la multiplicité dans un second invariant et le troisième de même (ou la taille des autres blocs de Jordan).
  Nous avons donc parmi les invariants (incomplets !), $(\lambda - 2)^2$ une partie de notre polynôme minimal, et les polynômes $\lambda - 2$ et $\lambda - 2$ (ou les blocs de Jordan de taille correspondante).

- On regarde enfin $K_1 = Ker(A - 4 \cdot I_{_5}) =< (0,0,0,0,1) >$ $\quad \dim K_1 = 1$ on a une partition triviale correspondant au tableau 
  Ainsi la valeur propre 4 est de multiplicité 1 dans le polynôme minimal (ce qui n'est pas une surprise vu qu'il divise $\chi_{_A}$). Il faudra donc ajouter le facteur $(\lambda - 4)$ à notre polynôme minimal.

On a donc $F_1(A) = \pi_{_A} = (X-2)^2(X-4)$ pour premier facteur invariant, les autres invariants étant $F_2(A) = X-2$ et $F_3(A) = X-2$.

Ce qui nous mène aux formes de Jordan J_2, J_1, J_1 ajoutées à l'identité fois la valeur propre 2 et J_1 ajoutée à l'identité fois la valeur propre 4, tout cela à permutation des blocs près.

$$A \sim \begin{bmatrix} J_1 + 2\cdot I_1 & & & \\ & J_1 + 2\cdot I_1 & & \\ & & J_2 + 2\cdot I_2 & \\ & & & J_1 + 4\cdot I_1 \end{bmatrix} = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 2 & 0 \\ & & 1 & 2 \\ & & & & 4 \end{bmatrix}$$

Autre exemple, autre méthode : Soit $A = \begin{bmatrix} 3 & 2 & -5 \\ 2 & 6 & -10 \\ 1 & 2 & -3 \end{bmatrix}$.

Sa matrice caractéristique est donc $C_{_A} = \begin{bmatrix} 3-X & 2 & -5 \\ 2 & 6-X & -10 \\ 1 & 2 & -3-X \end{bmatrix}$

$$L_1 \longleftrightarrow L_3 \Longrightarrow \begin{bmatrix} 1 & 2 & -3-X \\ 2 & 6-X & -10 \\ X-3 & -2 & 5 \end{bmatrix}$$

Attention ! l'échange d'un nombre pair (ici 2) de lignes (ou de colonnes) change le signe du déterminant.

$$L_2 \longleftarrow L_2 - 2L_1 \text{ et } L_3 \longleftarrow L_3 + (3-X)L_1 \quad \Longrightarrow \begin{bmatrix} 1 & 2 & -3-X \\ 0 & 2-X & 2X-4 \\ 0 & 4-2X & X^2-4 \end{bmatrix}$$

$$C_2 \longleftarrow C_2 - 2C_1 \text{ et } C_3 \longleftarrow C_3 + (3-X)C_1 \quad \Longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2-X & 2X-4 \\ 0 & 4-2X & X^2-4 \end{bmatrix}$$

$$L_3 \longleftarrow L_3 - 2L_2 \quad \Longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2-X & 2X-4 \\ 0 & 0 & (X-2)^2 \end{bmatrix}$$

$$C_3 \longleftarrow C_3 + 2L_2 \quad \Longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2-X & 0 \\ 0 & 0 & (X-2)^2 \end{bmatrix} = S_{C_A}$$

Le facteurs invariants sont alors $F_1(A) = (X-2)^2, \quad F_2(A) = X-2$. Le spectre est réduit à la seule valeur propre 2.

L'invariant en termes de tableau de Young est donné par  pour la valeur propre 2.
La décomposition de blocs de Jordan est immédiate :

$$A \sim 2\cdot I_3 + \begin{bmatrix} J_1 & \\ & J_2 \end{bmatrix} = \begin{bmatrix} J_1 + 2\cdot I_1 & \\ & J_2 + 2\cdot I_2 \end{bmatrix} = \begin{bmatrix} 2 & & \\ & 2 & 0 \\ & 1 & 2 \end{bmatrix}$$

6 Invariants de similitude et groupes abéliens finis

L'extraordinaire unité des mathématiques fait que ce phénomène d'invariants se retrouve dans une autre classification, en un peu plus digeste. Et c'est d'ailleurs pour cela qu'il est bon de le signaler. Il s'agit de la classification des groupes abéliens finis.
Le lien entre réduction d'endomorphisme et groupe abélien peut être vu ainsi : un endomorphisme f d'un espace vectoriel E sur $\mathbb{K}$ induit une structure de $\mathbb{K}[X]$-module sur E par $P.u = P(f)(u)$, $P \in \mathbb{K}[X]$, $u \in E$, et la décomposition en blocs de Jordan peut se voir en terme de décomposition en $\mathbb{K}[X]$-modules indécomposables. Maintenant, un groupe abélien G (noté additivement) est un $\mathbb{Z}$-module par $n.g = ng$, $n \in \mathbb{Z}$, $g \in G$. Il n'y a donc rien d'etonnant à ce que le problème de décomposition d'un groupe abélien fini ressemble au problème de réduction des endomorphismes, surtout lorsqu'on sait que $\mathbb{Z}$ et $\mathbb{K}[X]$ partagent la propriété remarquable d'être des anneaux principaux.
On rappelle ce théorème fondamental que l'on peut retrouver dans tou bon livre d'algèbre et théorie des nombres.

Théorème 11 (de Kronecker):
Soit G un groupe abélien fini. Alors il existe une unique suite finie d'entiers non nuls $(n_i)_{1\leq i\leq r}$ telle que $\forall 1 \leq i \leq r-1, \quad n_{i+1}|n_i$ *et*

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/_{n_i}\mathbb{Z}$$

Nous illustrons sur deux exemples parallèles, l'un sur une réduction d'endomorphisme, l'autre sur un groupe abélien fini, et nous affinerons la similitude entre les deux situations. Les facteurs invariants de Smith du premier correspondent au nombres n_i du théorème dans le second. De même il y a correspondance entre, respectivement, polynôme minimal, polynôme caractéristique, valeurs propres avec élément annulateur minimal, cardinal du groupe, et diviseurs premiers du cardinal.

Décomposition d'un groupe abélien fini :

Supposons que $G \simeq \mathbb{Z}/_{180}\mathbb{Z} \oplus \mathbb{Z}/_{48}\mathbb{Z} \oplus \mathbb{Z}/_{10}\mathbb{Z} \simeq \mathbb{Z}/_{5\times 3^2\times 2^2}\mathbb{Z} \oplus \mathbb{Z}/_{3\times 2^4}\mathbb{Z} \oplus \mathbb{Z}/_{5\times 2}\mathbb{Z}$ en soit une décomposition (parmi d'autres).

Alors, en utilisant la décomposition du lemme chinois et en regroupant, on obtient

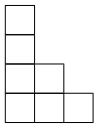
$$G \simeq \mathbb{Z}/_{5\times 3^2\times 2^4}\mathbb{Z} \oplus \mathbb{Z}/_{5\times 3\times 2^2}\mathbb{Z} \oplus \mathbb{Z}/_{2}\mathbb{Z}$$

décomposition unique pour la propriété de divisibilité de ses indices :

$$2 \text{ divise } 5\times 3\times 2^2 \text{ qui lui-même divise } 5\times 3^2\times 2^4.$$

Ce sont donc les "facteurs invariants" du groupe.

Aussi, cette divisibilité permet de voir que l'idéal annulateur de G est $5\times 3^2\times 2^4\mathbb{Z} = 720\mathbb{Z}$.
L'ordre du groupe G est donné par le produit des facteurs invariants $720\times 60\times 2 = 86400$. Faisons un lien avec les tableaux de Young pour chaque diviseur premier de l'ordre de G.

- pour le facteur premier 2 on a la partition de son exposant dans $|G|$ $7 = 4+2+1$ d'où le tableau de Young 
- pour le facteur premier 3 on a la partition $3 = 2+1$ d'où le tableau 

• pour le facteur premier 5 on a la partition $2 = 1 + 1$ d'où le tableau $\square\square$

Réduction d'un endomorphisme en dimension finie :

Soit a un endomorphisme d'un $\mathbb{K}$-espace vectoriel E de dimension 12, de matrice $A = \begin{bmatrix} 4 & 1 & & & & & & & & & & \\ -1 & 6 & & & & & & & & & & \\ & & 2 & 1 & 0 & & & & & & & \\ & & -1 & 4 & 1 & & & & & & & \\ & & 0 & 0 & 3 & & & & & & & \\ & & & & & 1 & 1 & & & & & 0 \\ & & & & & -1 & 3 & 1 & & & & \\ & & & & & & & 2 & 1 & & & \\ & & & & & & & & 2 & 1 & & \\ & & & & & & & & & 2 & 1 & \\ & & & & & -1 & & & & & 2 & 1 \\ & & & & & -1 & 1 & & & & & 2 \end{bmatrix}$

Par des opérations sur les lignes et les colones de $C_{_A} = I_{12}X - A$, on obtient la forme de Smith [7]

$$S_{_A} = \begin{bmatrix} 1 & & & & & & & & & & & \\ & \ddots & & & & & & & & & & \\ & & 1 & & & & & & & & & \\ & & & X-2 & & & & & & & & \\ & & & & (X-5)(X-3)(X-2)^2 & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & (X-5)(X-3)^2(X-2)^4 \end{bmatrix}$$

qui nous donne son polynôme minimal $\pi_{_A}(X) = (X-5)(X-3)^2(X-2)^4$ ainsi que deux autres invariants.
Remarque : leur produit donne le polynôme caractéristique $\chi_{_A}(X) = (X-5)^2(X-3)^3(X-2)^7$.

Alors réduire cet endomorphisme revient à l'étude d'une structure de $\mathbb{K}[X]$-module sur E, celle associé à l'endomorphisme a c'est à dire dont tout élément annulera l'endomorphisme a ainsi que tous les endomorphismes similaires.

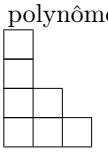
En fait on a une action $\begin{array}{ccc} \mathbb{K}[X] \times E & \longrightarrow & E \\ (P, x) & \longmapsto & P(a)(x) \end{array}$

Si on note $f_1 = X - 2, \quad f_2 = (X-5)(X-3)(X-2)^2, \quad f_3 = (X-5)(X-3)^2(X-2)^4$, on a une décomposition (unique) du $\mathbb{K}[X]$-module E :

$$E \simeq \mathbb{K}[X]/(f_1) \oplus \mathbb{K}[X]/(f_2) \oplus \mathbb{K}[X]/(f_3)$$

donnée par les idéaux annulateurs dans $\mathbb{K}[X]$ que sont $(f_1), (f_2), (f_3)$.
Ces idéaux annulateurs étant caractérisés par leurs éléments minimaux, à savoir $f_1 = X - 2$,
$f_2 = (X-5)(X-3)(X-2)^2, \quad f_3 = (X-5)(X-3)^2(X-2)^4$ et leurs (uniques) décompositions en polynômes irréductibles respectives, on a les partitions suivantes pour chaque polynôme irréductible divisant l'élément minimal :

• pour le facteur irréductible $X - 2$ on a la partition de son exposant dans le polynôme caractéristique de A

$7 = 4 + 2 + 1$ d'où le tableau de Young 

• pour le facteur irréductible $X - 3$ on a la partition $3 = 2 + 1$ d'où le tableau 

• pour le facteur irréductible $X - 5$ on a la partition $2 = 1 + 1$ d'où le tableau $\square\square$

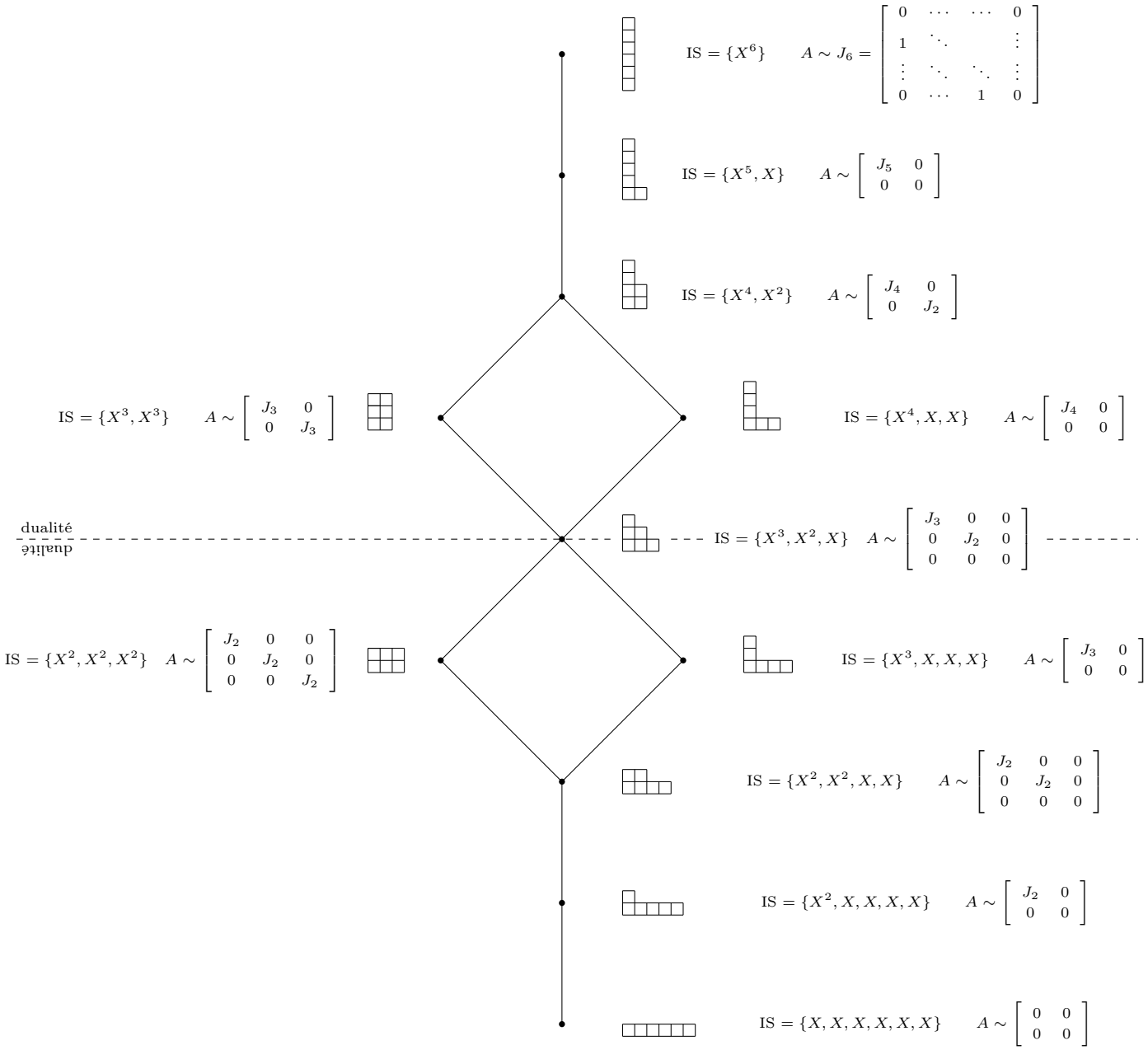
[7] On rappelle que la forme de Smith est un invariant total de similitude (il réunit les mêmes informations que l'ensemble des tableaux de Young).

Eléments de géométrie, actions de groupes, Note 0-C, Rached Mneimné, **Cassini**.
Pour les invariants de similitudes :
Algèbre linéaire, Rémi Goblot, Chap. 7, **Ellipses**

7 Annexe 5 : Ordre des onze partitions de 6 et tableaux de Young

Soit $A \in M_6(\mathbb{C})$ nilpotente.
Son polynôme caractéristique est $\chi_A(X) = X^6$.

Notation : IS $= \{X^5, X\}$ est un ensemble d'invariants totaux de similitude, dont le premier est le polynôme minimal.
Remarque : On voit bien ici que les exposants des invariants sont aussi les indices des blocs de Jordan.



retour p38

8 Annexe 6 : Lemme des noyaux et décomposition de Dunford

On rappelle quelques résultats essentiels pour les théorèmes de réduction. On pourra trouver les preuves dans le Goblot, Algèbre linéaire, Chapitre 7.

Lemme (des noyaux):

Soit A un endomorphisme de $E = \mathbb{K}^n$ et $P = \prod_{i=1}^{r} (X - \lambda_i)^{n_i}$ un polynôme (λ_i distincts).

Si $P(A) = 0$ alors $E = \operatorname{Ker}\big(P(A)\big) = \bigoplus_{i=1}^{r} \operatorname{Ker}(A - \lambda_i I_n)^{n_i}$ et $\operatorname{Ker}(A - \lambda_i I_n)^{n_i}$ est stable par A

Remarque :
On peut remplacer dans le lemme les polynômes $X - \lambda_i$, λ_i distincts, par des polynômes g_i premiers entre eux. Ceci peut être utile si on travaille sur un corps non algébriquement clos.

Remarque :
Si P est le polynôme caractéristique χ_A alors $n_i = \dim \operatorname{Ker}(A - \lambda_i I_n)^{n_i}$.

Théorème 12 (décomposition de Dunford):
Soit A un endomorphisme d'un espace vectoriel de dimension finie. Si son polynôme minimal π_A est scindé, alors il existe D diagonalisable et N nilpotente telles que :

1. $A = D + N$
2. $DN = ND$
3. *D et N sont des polynômes en A*
4. $\chi_D = \chi_A$

Remarque :
1) et 3) garantissent l'unicité de la décomposition, et 3) implique 2).

Exemples :
$A = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ n'est PAS une décomposition de Dunford car A est diagonalisable (et de plus ces deux matrices ne commutent pas)... on a $A = A + 0$.
$B = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$
$C = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ diagonalisable dans $\mathbb{C}$.

Si deux matrices A et B sont semblables ($B = PAP^{-1}$), alors elles ont le même rang, le même déterminant, la même trace, le même polynôme caractéristique, le même polynôme minimal, mais ceux-ci ne sont que des invariants partiels de l'action par conjugaison, et ne suffisent pas à eux seul à caractériser la classe de similitude d'une matrice quelconque.

retour p19

Chapitre IV

Groupes conservant une forme bilinéaire

Nous allons maintenant présenter les groupes classiques fixant une forme bilinéaire donnée. Encore une fois, le déroulement du chapitre passe par les actions de groupe et invariants d'action. Tout d'abord, la classification les formes bilinéaires va passer par les orbites de $GL_n(\mathbb{K})$ pour l'action de congruence. On dégagera des invariants partiels (rang, discriminant), puis des invariants totaux, permettant de caractériser les orbites. Mais un invariant, qu'il soit partiel ou total, dépend dramatiquement du corps choisi (on se limitera aux corps $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$, mais pour aller plus loin, il est conseillé de feuilleter le petit "Cours d'arithmétique" de Serre).
Une fois la classification faite, à l'aide de ces invariants totaux, les groupes classiques étudiés arriveront naturellement comme stabilisateurs d'éléments choisis dans une orbite (on rappelle que le stabilisateur ne dépend pas, à isomorphisme près de l'élément choisi dans une orbite). On trouvera en Annexe 7, p55, la plupart des définitions, notations, et résultats classiques utilisés dans ce chapitre.

Pour des raisons qui paraitront évidentes par la suite, on travaille sur un corps $\mathbb{K}$ de caractéristique différente de 2. Le bon objet d'étude tout au long de cette section est, à mon goût personnel, la forme quadratique, c'est à dire un polynôme homogène de degré 2, appelons q cette forme. Il existe une pléthore de formes bilinéaires b telles que $b(x,x) = q(x)$ pour tout x. Mais il en existe une unique qui soit symétrique, il s'agit de

$$b(x,y) = \frac{q(x+y) - q(x) - q(y)}{2}.$$

Le fait de substituer l'étude d'une forme bilinéaire à cette d'une forme quadratique est astucieuse, en fait, selon la stratégie des Horaces et des Curiaces, on préfère attaquer deux fois le degré 1 plutôt qu'une fois le degré deux. Enfin, le choix d'une forme bilinéaire **symétrique** provient de l'unicité ci-dessus.

On note A la matrice de la forme bilinéaire symétrique associée à q.
Les invariants rang, discriminant, ont été définis en Annexe. Dans le cas réel, on peut définir un nouvel invariant $p(A) = p(b) := \max\{\dim F,\, F \subset E = \mathbb{K}^n,\, q(x) > 0\ \forall x \in F\}$ qui ne dépend que de b et non de A donc qui ne dépend pas de la base.

Théorème 13 :

- *Si* $\mathbb{K} = \mathbb{C}$, $\quad O_A = O_{A'} \iff \operatorname{rg} A = \operatorname{rg} A'$
- *Si* $\mathbb{K} = \mathbb{R}$, $\quad O_A = O_{A'} \iff \operatorname{rg} A = \operatorname{rg} A'$ *et* $p(A) = p(A')$
- *Si* $\mathbb{K} = \mathbb{F}_q$, $\quad O_A = O_{A'} \iff \operatorname{rg} A = \operatorname{rg} A'$ *et* $\delta(A) = \delta(A') \mod (\operatorname{Ker} \phi_b)$

Démonstration :

$\boxed{\mathbb{K} = \mathbb{C}}$ $\Longrightarrow$ est clair, montrons $\Longleftarrow$.

Supposons $\operatorname{rg} A = r \neq 0$ (sinon l'assertion est triviale). Alors il existe ϵ : $q(\epsilon) \neq 0$ (sinon b serait nulle).

Soit $\lambda \in \mathbb{C}^*$ tel que $\lambda^2 = q(\epsilon)$ et $\epsilon_1 := \frac{\epsilon}{\lambda}$. Alors $q(\epsilon_1) = 1$. b étant non-dégénérée sur $\mathbb{C}\epsilon_1$, on a $E = \mathbb{C}\epsilon_1 \oplus (\mathbb{C}\epsilon_1)^\perp$.

Donc $A \equiv \begin{bmatrix} 1 & 0 \\ 0 & A' \end{bmatrix}$ avec $\operatorname{rg} A' = r - 1$ et par itération $A \equiv \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}$ où forcément $k = r$ par invariance du rang.

$\boxed{\mathbb{K} = \mathbb{R}}$ $\Longrightarrow$ est clair, montrons $\Longleftarrow$.

Soit A telle que $\operatorname{rg} A := r$, $p(A) := p$ et $q := n - p - r$.

Analogue au cas complexe sauf que si $q(\epsilon) > 0$ en posant $\epsilon_1 := \frac{\epsilon}{\lambda}$ et avec $q(\epsilon) = \lambda^2$ on a $q(\epsilon_1) = 1$

si $q(\epsilon) < 0$ on posant $\epsilon_1 := \frac{\epsilon}{\lambda}$ et avec $-q(\epsilon) = \lambda^2$ on a $q(\epsilon_1) = -1$

Alors par itération on obtient que $A \equiv \begin{bmatrix} I_{p'} & & \\ & -I_{q'} & \\ & & 0 \end{bmatrix}$ où $p' = p$, $q' = q$ et $p + q = r$ par invariance de $p(A)$.

$\boxed{\mathbb{K} = \mathbb{F}_q}$ $\Longrightarrow$ est clair, montrons $\Longleftarrow$.

Quitte à prendre un supplémentaire de $\operatorname{Ker} \phi_b$, on peut supposer b non-dégénérée. Soit ξ un non-carré de $\mathbb{F}_q^*$.

Alors, en utilisant la même méthode que précédemment, c'est à dire procédé d'orthogonalisation par récurrence décroissante sur la dimension, on obtient

$$A \equiv \begin{bmatrix} \epsilon_1 & & \\ & \ddots & \\ & & \epsilon_n \end{bmatrix},$$

avec $\epsilon_i = 1$ ou ξ. On peut encore faire mieux. Pour cela, faire d'abord l'exercice très classique :

Exercice :

Montrer que $ax^2 + by^2 = 1$ avec $a, b \neq 0$ a au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q \backslash_{\{(0,0)\}}$.

Indication : Montrer qu'il existe $\frac{q+1}{2}$ éléments de la forme ax^2 et autant de la forme $1 - by^2$. Ainsi puisque $\frac{q+1}{2} + \frac{q+1}{2} > q$, il existe un élément de la forme $ax^2 = 1 - by^2$.

Donc d'après l'exercice, dans un espace de dimension $n \geq 2$, toute forme quadratique possède un vecteur v tel que $q(v) = 1$. On déduit alors aisément que

$$A \equiv \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \epsilon_n \end{bmatrix}.$$

□

Remarque :

Toute matrice est congruente à une matrice diagonale.

Le cas $\mathbb{K} = \mathbb{R}$ correspond au théorème d'inertie de Sylvester.

Il est alors naturel de s'intéresser au groupe d'isotropie de chaque orbite :

- $\boxed{\mathbb{K} = \mathbb{C}}$ $\operatorname{Orb}(I_n) = \{P\,{}^tP \in M_n(\mathbb{C}) \,:\, P \in GL_n(\mathbb{C})\}$

  $\operatorname{Orb}(I_{r,0}) = \{PI_{r,0}\,{}^tP \in M_n(\mathbb{C}) \,:\, P \in GL_n(\mathbb{C})\}$ avec $I_{r,0} = \left[\begin{smallmatrix} I_r & 0 \\ 0 & 0 \end{smallmatrix}\right]$

  Groupe d'isotropie de I_n : $\operatorname{Stab}(I_n) = O(n, \mathbb{C}) = \{P \in GL_n(\mathbb{C}) \,:\, P\,{}^tP = I_n\} = \{P \in GL_n(\mathbb{C}) \,:\, {}^tPP = I_n\}$

Groupe d'isotropie de $I_{r,0}$: $\mathrm{Stab}(I_{r,0}) = O(n,r,\mathbb{C}) = \{P \in GL_n(\mathbb{C}) \,:\, PI_{r,0}\,{}^tP = I_{r,0}\}$

Exercice :
Montrer que $O(n,r,\mathbb{C}) \simeq (O(r,\mathbb{C}) \times GL_{n-r}(\mathbb{C})) \ltimes_\varphi M_{r,n}(\mathbb{C})$ avec $\varphi : (A,D)\cdot C \longmapsto ACD^{-1}$.

Le groupe classique important est donc $O(n,\mathbb{C})$.

- $\boxed{\mathbb{K} = \mathbb{R}}$ $\mathrm{Orb}(I_n) = \{P\,{}^tP \in M_n(\mathbb{R}) \,:\, P \in GL_n(\mathbb{R})\} = \mathcal{S}_n^{++}(\mathbb{R})$ l'ensemble des produits scalaires.
  $\mathrm{Orb}(I_{p,q}) = \{PI_{p,q}\,{}^tP \in M_n(\mathbb{R}) \,:\, P \in GL_n(\mathbb{R})\}$ avec $I_{p,q} = \begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix}$

  Groupe d'isotropie de I_n : $\mathrm{Stab}(I_n) = O(n,\mathbb{R}) = \{P \in GL_n(\mathbb{R}) \,:\, P\,{}^tP = I_n\}$

  Groupe d'isotropie de $I_{p,q}$: $\mathrm{Stab}(I_{p,q}) = O(p,q,\mathbb{R}) = \{P \in GL_n(\mathbb{R}) \,:\, PI_{p,q}\,{}^tP = I_{p,q}\}$

  Exercice :
  Montrer que $\overline{\mathrm{Orb}(I_{p,q})} = \bigsqcup_{\substack{0\le h\le p \\ 0\le h'\le q}} \mathrm{Orb}(I_{p-h,q-h'})$

- $\boxed{\mathbb{K} = \mathbb{F}_q}$ $\mathrm{Orb}(I_n) = \{P\,{}^tP \in M_n(\mathbb{F}_q) \,:\, P \in GL_n(\mathbb{F}_q)\}$
  $\mathrm{Orb}(I_\xi) = \{PI_\xi\,{}^tP \in M_n(\mathbb{F}_q) \,:\, P \in GL_n(\mathbb{F}_q)\}$ avec $I_\xi = \begin{bmatrix} I_{n-1} & 0 \\ 0 & \xi \end{bmatrix}$ et ξ un non-carré.

  Groupe d'isotropie de I_n : $\mathrm{Stab}(I_n) = O(n,\mathbb{F}_q) = \{P \in GL_n(\mathbb{F}_q) \,:\, P\,{}^tP = I_n\}$

  Groupe d'isotropie de I_ξ : $\mathrm{Stab}(I_\xi) = O(n,\xi,\mathbb{F}_q) = \{P \in GL_n(\mathbb{F}_q) \,:\, PI_\xi\,{}^tP = I_\xi\}$

Définition 21 :
Soit $P \in M_n(\mathbb{C})$ une matrice complexe. Sa matrice adjointe est la transconjuguée $P^* := {}^t\overline{P}$.

Le cas hermitien est analogue et laissé en exercice, on introduit l'action par congruence hermitienne :

$$\begin{array}{ccc} GL_n(\mathbb{C}) \times M_n(\mathbb{C}) & \longrightarrow & M_n(\mathbb{C}) \\ (P,A) & \longmapsto & PAP^* \end{array}$$

Et la signature ainsi que le rang classifient les orbites.

$\mathrm{Orb}(I_n) = \{PP^* \in M_n(\mathbb{C}) \,:\, P \in GL_n(\mathbb{C})\} = H_n^{++}(\mathbb{C})$ l'ensemble des produits scalaires hermitiens [8].
$\mathrm{Orb}(I_{p,q}) = \{PI_{p,q}P^* \in M_n(\mathbb{C}) \,:\, P \in GL_n(\mathbb{C})\}$

Groupe d'isotropie de I_n : $\mathrm{Stab}(I_n) = U(n,\mathbb{C}) = \{P \in GL_n(\mathbb{C}) \,:\, PP^* = I_n\}$

Groupe d'isotropie de $I_{p,q}$: $\mathrm{Stab}(I_{p,q}) = U(p,q,\mathbb{C}) = \{P \in GL_n(\mathbb{C}) \,:\, PI_{p,q}P^* = I_{p,q}\}$

[8] Remarque : Ce sont les matrices hermitiennes définies positives. On verra que cet ensemble est homéomorphe à l'espace vectoriel des matrices hermitiennes (de dimension n^2) via l'exponentielle de matrices, p62

1 Action des groupes orthogonaux

Soit q une forme quadratique sur $\mathbb{K}$ et b sa forme bilinéaire symétrique associée de matrice A.
On associe à q son groupe d'isotropie $O(q) := O(b) := \mathrm{Stab}(A) = \{P \in GL_n(\mathbb{K}) \ : \ PA\,{}^tP = A\}$
$= \{P \in GL_n(\mathbb{K}) \ : \ b(Px, Py) = b(x, y) \quad \forall x, y \in \mathbb{K}^n\}$
$= \{P \in GL_n(\mathbb{K}) \ : \ (Px)A\,{}^t(Py) = {}^txAy \quad \forall x, y \in \mathbb{K}^n\}$
Ainsi P est par construction une isométrie.

Remarque :
Si deux formes quadratiques q et q' sont dans la même orbite pour l'action de congruence de $GL_n(\mathbb{K})$, alors $O(q)$ et $O(q')$ sont isomorphes.

D'après la remarque qui précède, on peut introduire les groupes classiques dits orthogonaux : tout d'abord sur $\mathbb{C}$ (où l'invariant total est le rang), il y a le groupe $O(n, \mathbb{C})$ qui est le stabilisateur de l'identité. Les autres orbites correspondent aux rangs inférieurs, et comme d'habitude, on obtient les stabilisateurs comme produits semi-directs de groupes classiques.
Ensuite, pour $\mathbb{K} = \mathbb{R}$, il y a les groupes $O(p, q)$ qui stabilisent une forme de signature (p, q). Il y a parmi eux le célèbre groupe orthogonal $O(n, \mathbb{R}) = O(n, 0)$ et qu'entre nous on appelle affectueusement $O(n)$ car il est le stabilisateur de notre bonne vieille forme euclidienne.
On peut faire la remarque bête que si $PI_n^tP = I_n$, alors $P(-I_n)^tP = -I_n$. On en déduit facilement que $O(p, q) = O(q, p)$. Ce qui entache la réciproque : on peut très bien avoir des stabilisateurs isomorphes (et même carrément égaux) sans que les matrices soient dans la même orbite.
Plus généralement, on notera $O(n, \mathbb{K})$ le stabilisateur de l'identité dans $GL_n(\mathbb{K})$.

Il résulte de la définition que $O(q)$ agit sur les nappes (appelées quadriques) $N_k = \{x \in \mathbb{K}^n \ : \ q(x) = k\}$ où $k \in \mathbb{K}$.
En effet, on voit que $\forall P \in O(b), \quad q(Px) = b(Px, Px) = b(x, x) = q(x) = k$, pour tout $x \in N_k$. D'où $Px \in N_k$.
Les nappes constituent un objet d'étude important en soi. On peut les voir comme la généralisation à plusieurs variables de l'équation du second degré.

Question :
Cette action est-elle transitive ?

Regardons sur un exemple : Soit E l'espace vectoriel euclidien de dimension n, et N_1 la sphère de rayon 1. On sait, d'après le théorème de la base orthonormée incomplète, que l'action est transitive. La transitivité sur N_k en découle.

On peut aussi se poser la question de transitivité suivante : l'action de $O(q)$ est elle transitive sur une grassmannienne ? Dit autrement, pour tout $F, F' \subset E$ de même dimension, existe-t-il $P \in O(q) \ : \ P(F) = F'$. Il est clair que la reponse est non en général : prendre pour F une droite engendrée par un vecteur isotrope et pour F' une droite engendrée par un vecteur non isotrope.
Les théorèmes de base incomplète, si utiles jusqu'à présent, sont dans le cadre d'un espace muni d'une forme quadratique, remplacés par le puissant théorème de Witt, et dont une preuve peut être lue dans le Perrin.

Théorème 14 (de Witt):
Soit un espace vectoriel E muni d'une forme bilinéaire non-dégénérée b sur $\mathbb{K}$ de caractéristique différente de 2, et $F, F' \subset E$ deux sous-espaces.
Alors toute isométrie $\sigma : F \longrightarrow F'$ peut-être prolongée en une isométrie $\tilde{\sigma} : E \longrightarrow E$.

retour p121

Le corollaire suivant est immédiat :

Corollaire 6 :
Le groupe $O(q)$ est transitif sur la nappe $N_k := \{v,\ q(v) = k\}$

Un peu plus général, le théorème de Witt peut être vu comme un théorème de multi-transitivité (transitivité sur des m-uplets) sous des conditions métriques :

Corollaire 7 :
Soit b une forme bilinéaire symétrique sur $\mathbb{K}$, $(x_i)_{1\leq i\leq m}$ et $(y_j)_{1\leq j\leq m}$ dans $\mathbb{K}^n$ telles que $\forall i,j \quad b(x_i,x_j) = b(y_i,y_j)$. Alors il existe une isométrie $P \in O(b)$ telle que $\forall i,j \quad Px_i = y_i$.

Voici un exemple important à avoir en tête :

Exemple :
$O(2)$ et même $SO(2)$ agit sur les couples de vecteurs du cercle $\mathcal{S}^1$ (cas $m = 2$). La condition $b(x_1,x_2) = b(y_1,y_2)$ correspondant à l'égalité des angles : $\cos(x_1,x_2) = \cos(y_1,y_2)$. Le lecteur pourra en déduire que le quotient $(S^1 \times S^1)/SO(2)$ correspond aux angles orientés et le quotient $(S^1 \times S^1)/O(2)$ aux angles non orientés.

2 Formes bilinéaires antisymétriques

Soit un corps $\mathbb{K}$ (toujours de caractéristique différente de 2).
Une forme bilinéaire b est dite antisymétrique si $\forall x,y \in \mathbb{K}^n, \quad b(x,y) = -b(y,x)$.
On note $\mathcal{A}_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : {}^tA = -A\}$ l'espace vectoriel des matrices antisymétriques.

Proposition 27 :
$GL_n(\mathbb{K}) \circlearrowleft \mathcal{A}_n(\mathbb{K})$ continûment par congruence et les orbites sont classifiées par le rang (qui est pair).

Démonstration :
Quitte à prendre un supplémentaire au noyau de la forme, on peut la supposer non-dégénérée (i.e. A de rang n maximal).
Son rang est forcément pair car $0 \neq \det A = \det {}^tA = \det(-A) = (-1)^n \det A$ donc n est pair. On pose $n = 2p$.

Comme b est non nulle, $\exists(\epsilon,\epsilon')$ tel que $b(\epsilon,\epsilon') \neq 0$. Alors (ϵ,ϵ') forme une famille libre, sinon on aurait $\epsilon' = k\epsilon$ et donc $b(\epsilon,\epsilon') = kb(\epsilon,\epsilon) = 0$.
On pose donc $\epsilon_1 = \dfrac{\epsilon}{b(\epsilon,\epsilon')}$ et $F =< \epsilon,\epsilon' >$ et on a $F = \mathbb{K}\epsilon \oplus \mathbb{K}\epsilon'$.
$\mathrm{mat}(b|_{F\times F}) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ dans la base (ϵ_1,ϵ') de F. Elle est donc non-dégénérée et $E = F \oplus F^\perp$. Ainsi $A \equiv \begin{bmatrix} 0 & 1 & \\ -1 & 0 & \\ & & A' \end{bmatrix}$ avec $\det A' \neq 0$ toujours car b non-dégénérée, et par récurrence sur n, il vient que $A \equiv \begin{bmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ & & & & \ddots \end{bmatrix}$ dans une base $(\epsilon_1,\epsilon'_1,\ldots,\epsilon_p,\epsilon'_p)$. Donc en permutant lignes et colonnes, on obtient finalement $A \equiv \begin{bmatrix} 0 & I_p \\ -I_p & 0 \end{bmatrix} = J_n$ dans la base $(\epsilon_1,\epsilon_2,\ldots,\epsilon_p,\epsilon'_1,\ldots,\epsilon_p)$.
Conclusion : deux matrices de même rang r sont congruentes à $\begin{bmatrix} J_r & 0 \\ 0 & 0 \end{bmatrix}$.

□

Revenons à l'action $GL_n(\mathbb{K}) \circlearrowleft \mathcal{A}_n(\mathbb{K})$ par congruence. On a $\mathrm{Orb}(J_n) = \{PJ_n\,{}^tP \in \mathcal{A}_n(\mathbb{K}) : P \in GL_n(\mathbb{K})\}$

Et on introduit le groupe d'isotropie de J_n : $\mathrm{Stab}(J_n) = S_p(n, \mathbb{K}) = \{P \in GL_n(\mathbb{K}) \, : \, PJ_n \, {}^tP = J_n\}$.

3 Applications à la loi de réciprocité quadratique.

Voici une application des invariants de congruence à un très beau résultat de théorie des nombres qui a vu passer des mathématiciens illustres comme Fermat, Legendre, Euler, puis enfin Gauss.
Faisons tout d'abord quelques rappels sur le symbole de Legendre. Afin de résoudre des équations du second degré sur un corps $\mathbb{K}$ donné, on est amené à se demander si un certain élément (en l'occurence le discriminant) est un carré ou pas. C'est vrai en général pour tout problème concernant les formes quadratiques, mais cela dépend bien sûr du choix du corps.
Si $\mathbb{K} = \mathbb{C}$, tout élément est un carré et c'est terminé. Si $\mathbb{K} = \mathbb{R}$, alors un élément est un carré si et seulement si il est positif.
Supposons maintenant, $\mathbb{K} = \mathbb{F}_p$, p premier. Alors une réponse bien connue est la suivante :
Proposition 28 :
Soit p un nombre premier impair, et $a \in \mathbb{F}_p^*$. Alors $a^{\frac{p-1}{2}} = \pm 1$. De plus, a est un carré si et seulement si $a^{\frac{p-1}{2}} = 1$.

Démonstration. La première assertion est claire, posons $b = a^{\frac{p-1}{2}}$. Alors $b^2 = a^{p-1} = 1$ par le théorème de Lagrange. Or sur un corps $X^2 - 1 = 0$ a pour unique racine 1 et -1.
Montrons la seconde assertion. Soit $\mathcal{S}$ l'ensemble des solutions de l'équation $X^{\frac{p-1}{2}} = 1$ dans $\mathbb{F}_p^*$. L'ensemble $\mathcal{C}$ des carrés de $\mathbb{F}_p^*$ est un sous-groupe, c'est l'image du morphisme $\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$. Donc, $\#\mathcal{C} = \#im\phi = \#F_p^* / \operatorname{Ker}\phi = \#F_p^*/\{1, -1\} = \frac{p-1}{2}$.
De plus, si a est un carré, par exemple $a = c^2$, alors $a^{\frac{p-1}{2}} = c^{p-1} = 1$. On a donc $\mathcal{C} \subset \mathcal{S}$. Pour avoir l'égalité, il suffit de remarquer que $\#\mathcal{C} = \frac{p-1}{2} \geq \#\mathcal{S}$, car sur un corps, le nombre de racines d'un polynôme est inférieur au degré du polynôme. Conclusion $\mathcal{C} = \mathcal{S}$ et la proposition est montrée. □

On définit donc le symbole de Legendre

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$$

qui permet de savoir si a est ou non un carré dans $\mathbb{F}_p^*$. Le problème est que le calcul $a^{\frac{p-1}{2}}$ peut être très fastidieux. Il faut donc trouver un moyen raisonnable pour déterminer le symbole de Legendre d'un nombre. Commençons par une remarque :

Remarque :
Le symbole de Legendre $a \mapsto \left(\frac{a}{p}\right)$ fournit un morphisme de groupes entre $\mathbb{F}_p^*$ et $\{1, -1\}$ et en fait, le seul morphisme non trivial entre ces deux groupes (on le montre facilement en utilisant le fait que le groupe $\mathbb{F}_p^*$ est cyclique).

Soit n un entier. On veut savoit si n est ou non un carré modulo p. On veut donc calculer $\left(\frac{\bar{n}}{p}\right)$, où $\bar{n}$ est la classe de n modulo p. D'après la remarque précédente :

$$\left(\frac{\bar{n}}{p}\right) = (\pm)^{\frac{p-1}{2}} \prod \left(\frac{\bar{q_i}}{p}\right)^{\alpha_i},$$

où $n = \pm \prod q_i^{\alpha_i}$ est la décomposition en premiers de n.
On se ramène donc au problème de savoir si q est un carré modulo p avec q premier.
La solution de ce problème est la loi de réciprocité quadratique, conjecturée par Euler et résolue par un Gauss de 19

ans[9]. Voici un énoncé ainsi une preuve que je trouve ravissante avec des groupes, des invariants et de la géométrie des corps finis :

Théorème 15 :
Soient p et q deux nombres premiers impairs, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Démonstration. L'idée est de calculer de deux manières le cardinal modulo p de la variété algébrique

$$X := \{(x_1, \dots, x_p), \sum_i x_i^2 = 1\} \subset \mathbb{F}_q^p.$$

Une manière va consister à utiliser l'action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur X. L'autre, par l'action du groupe $O_p(\mathbb{F}_q)$ sur la forme quadratique et l'invariant total discriminant qui nous permet de nous ramener à un cas plus simple.
Commençons par un résultat qui découle directement de la proposition précédente :

$$\text{Assertion : Le cardinal de } \{x,\, ax^2 = 1\} \text{ dans } \mathbb{F}^p \text{ est égal à } 1 + \left(\frac{a}{p}\right).$$

Approche 1.

$$\#X = \left(\frac{p}{q}\right) + 1 \mod p.$$

Pour cela, on fait agir $\mathbb{Z}/p\mathbb{Z}$ par permutation cyclique sur X.

$$i.(x_1, \dots, x_p) = (x_{1+i}, \dots, x_{p+i}),$$

où les indices sont vus modulo p.
Un point sur une orbite a pour stabilisateur $\mathbb{Z}/p\mathbb{Z}$ ou $\{1\}$. Donc, il y a soit les orbites de la forme $(x, x, \dots, x)$, soit des orbites de cardinal p. Or, une orbite de la forme $(x, x, \dots, x)$ est dans X si et seulement si $px^2 = 1$. D'après l'assertion précédente, on a le résultat annoncé.
Approche 2.

$$\#X = (q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})q^{\frac{p-1}{2}}.$$

Soit A la matrice $p \times p$ à coefficients dans $\mathbb{F}_q$:

$$A := \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & 1 & \\ & & & & & 1 & 0 & \\ & & & & & & & a \end{pmatrix},$$

où on a posé $a = (-1)^{\frac{p-1}{2}}$. Le discriminant de B vaut 1, elle est donc congruente à la matrice identité.

[9]Non satisfait de sa première preuve qu'il trouvait un peu bourrin, il en a trouvé une dizaine d'autres au cours de sa carrière.

Cela implique que via un changement de variables linéaire,

$$X = \{(y_1, z_1, \ldots, y_{\frac{p-1}{2}}, z_{\frac{p-1}{2}}, x_p),\ 2(y_1 z_1 + \ldots y_{\frac{p-1}{2}} z_{\frac{p-1}{2}} + a x_p^2 = 1\}.$$

Comptons X en faisant deux cas.
Premier cas : $(y_1, \ldots, y_{\frac{p-1}{2}}) = (0, \ldots, 0)$.
Dans ce cas, d'après l'assertion précédente, on a $q^{\frac{p-1}{2}}(1 + a^{\frac{q-1}{2}})$ possibilités.
Second cas : $(y_1, \ldots, y_{\frac{p-1}{2}}) \neq (0, \ldots, 0)$.
Dans ce cas, chaque fois que l'on fixe $(y_1, \ldots, y_{\frac{p-1}{2}})$ et x_p, il reste à choisir les points d'un hyperplan en dimension $\frac{p-1}{2}$. Donc, le cardinal pour ce cas est $(q^{\frac{p-1}{2}} - 1)qq^{\frac{p-1}{2}-1}$. Au total, on obtient bien le résultat annoncé.
Faisons maintenant le bilan de ces deux approches

$$(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})q^{\frac{p-1}{2}} = \binom{p}{q} + 1 \mod p.$$

D'où, d'après la proposition précédente :

$$(\binom{q}{p} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})\binom{q}{p} = \binom{p}{q} + 1 \mod p.$$

Ce qui donne après simplification le résultat annoncé. □

4 Annexe 7 : Généralités sur les formes bilinéaires

Soit $\mathbb{K}$ un corps de caractéristique différente de 2. On considère l'action par congruence

$$\begin{array}{ccc} GL_n(\mathbb{K}) \times M_n(\mathbb{K}) & \longrightarrow & M_n(\mathbb{K}) \\ (P, A) & \longmapsto & PA\,{}^tP \end{array}$$

Voici ce qui va rendre les choses un peu plus difficile : contrairement à l'action par conjugaison, si $O_{\mathbb{C}}$ est une orbite pour $\mathbb{K} = \mathbb{C}$, $\quad O_{\mathbb{C}} \cap M_n(\mathbb{R})$ n'est pas une orbite sous l'action de $GL_n(\mathbb{R})$ mais une réunion de celles-ci.
Autrement dit, pour des matrices réelles, $GL_n(\mathbb{C})$-congruent $\not\Rightarrow GL_n(\mathbb{R})$-congruent.
Par exemple, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Nous avons tout de même des **Invariants :**

- Le rang (ou la dimension du noyau) : $\mathrm{rg}(PA\,{}^tP) = \mathrm{rg}(A)$
- Le discriminant : $\begin{array}{rccl} \delta : & M_n(\mathbb{K}) & \longrightarrow & \{0\} \sqcup \mathbb{K}^*/\mathbb{K}^{*2} \\ & A & \longmapsto & \det A \mod \mathbb{K}^{*2} \end{array}$

Remarque :
$\mathbb{C}^*/\mathbb{C}^{*2} = \{1\}$ $\qquad$ $\mathbb{R}^*/\mathbb{R}^{*2} = \{-1, 1\}$ $\qquad$ $\mathbb{F}_q^*/\mathbb{F}_q^{*2} = \{1, \xi\}$

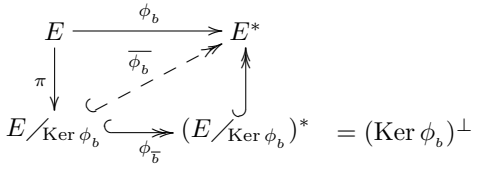
L'action peut se restreindre à l'ensemble des matrices symétriques $\quad \mathcal{S}_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : {}^tA = A\}$ (espace vectoriel de dimension $\frac{n(n+1)}{2}$)
ou antisymétriques $\quad \mathcal{A}_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) : {}^tA = -A\}$ (espace vectoriel de dimension $\frac{n(n-1)}{2}$).

On supposera dans tout le cours que $\mathbb{K}$ est de caractéristique différente de 2.
Dans $\mathbb{K}^n$ on peut identifier matrices et formes bilinéaires via la base canonique. On ne s'intéressera qu'aux formes bilinéaires symétriques et antisymétriques puisque les deux espaces de ces formes sont en somme directe.
On rappelle pour cela : $b(x, y) = \frac{b(x,y)+b(y,x)}{2} + \frac{b(x,y)-b(y,x)}{2}$.

A la forme bilinéaire b, on associe le morphisme $\phi_b : E \longrightarrow E^*$ vérifiant $< \phi_b(x), y >= b(x, y)$.

Le morphisme ϕ_b détermine b et sera essentiel dans la suite. Comme nous ne traiterons que des formes symétriques ou antisymétriques (ce que l'on supposera par la suite), il est inutile de faire l'équivalent à droite de cette procédure.
Si ϕ_b n'est pas injective, on dira que la forme b est dégénérée. On préfère travailler sur des formes non dégénérées, les raisons étant contenues dans la proposition qui suit.
Afin de pouvoir passer d'une forme dégénérée à son "analogue" en non dégénéré, on peut penser au passage au quotient. Effectivement, on voit que b passe au quotient en définissant sur $E/\operatorname{Ker}\phi_b$, la forme $\bar{b}$ par $\bar{b}(\bar{x}, \bar{y}) = b(x, y)$, qui est bien définie.

Le passage de b à $\bar{b}$ peut se résumer en ce diagramme commutatif :



Pour ceux que ce diagramme effraieraient, mettons des matrices pour mieux comprendre ce que l'on fait (mais ça demande de faire un choix de base et du coup c'est moins canonique, tant pis pour vous !) $\bar{b}$ de matrice $\overline{A}$ est la

forme non-dégénérée associée à b : $A = \mathrm{mat}(b) = \begin{bmatrix} 0 & 0 \\ 0 & \overline{A} \end{bmatrix}$ après choix d'un supplémentaire de $\mathrm{Ker}\,\phi_b$ dans E.

Définition 22 :
$\mathrm{Ker}\,\phi_b = \{x \in E \,:\, b(x,y) = 0,\ \forall y \in E\}$ *est le noyau (à gauche) de la forme* b.

Remarque : $\delta(A) \neq 0 \iff \det A \neq 0 \iff b$ non-dégénérée $\iff \mathrm{Ker}\,\phi_b$ est trivial $\iff \phi_b$ est injective (donc un isomorphisme).

Proposition 29 :
Soient b *une forme bilinéaire et* F *un sous-espace vectoriel de* $E = \mathbb{K}^n$.
On définit $F^\perp = \{x \in E \,:\, b(x,y) = 0,\ \forall y \in F\}$.

i) $\dim E \leq \dim F + \dim F^\perp$,

ii) $\dim E = \dim F + \dim F^\perp$ *si* b *est non-dégénérée,*

iii) $E = F \oplus F^\perp$ *si* $b|_{F\times F}$ *est non-dégénérée (i.e.* $F \cap F^\perp = \{0\}$*, on dit aussi que* F *est régulier),*

iv) $F \cap F^\perp = \mathrm{Ker}\,\phi_{b|_{F\times F}} \neq 0$ *si* $b|_{F\times F}$ *est dégénérée, on dit aussi que* F *est isotrope),*

v) $F \subset F^\perp$ *si* $b|_{F\times F}$ *est nulle (on dit aussi que* F *est totalement isotrope).*

Démonstration :
Il suffit de voir que si $r_F : E^* \to F^*$ est le morphisme de restriction (qui est surjectif), alors $F^\perp = \mathrm{Ker}(r_F \circ \phi_b) = \phi_b^{-1}(\mathrm{Ker}(r_F))$. En utilisant la formule du rang deux fois (sur r_F et sur la restriction de ϕ_b à $F^\perp$), on obtient $i)$ et $ii)$. Pour prouver $iii)$, on peut montrer que si x est dans $F \cap F^\perp$, alors x est dans le noyau de la forme $b|_{F\times F}$ et est donc nul par hypothèse. On conclut en utilisant $i)$ comme argument de dimension.
Pour $iv)$ il est clair que $\{0\} \neq \mathrm{Ker}\,\phi_{b|_{F\times F}} \subset F \cap F^\perp$, d'où la double inclusion. Le $v)$ est immédiat.

□

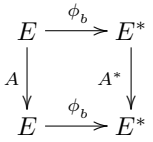
Remarque :
$\mathrm{Ker}(r_F)$ est l'orthogonal "canonique" de F qui habite en fait dans F^*. L'orthogonal de F pour la forme bilinéaire b n'est rien autre que cet orthogonal canonique transporté par ϕ_b^{-1}.

Le dual E^* jouant le rôle d'un "miroir" pour l'espace vectoriel E, il est naturel que l'on cherche à déterminer l'image dans ce miroir d'un endomorphisme de E. On aboutit à la notion d'adjoint.

Proposition 30 :
Soit A *un endomorphisme de* E *et* b *une forme bilinéaire non-dégénérée. Alors il existe un unique endomorphisme* A^* *appelé endomorphisme adjoint pour* b*, vérifiant* $b(x,y) = b(A^*x, y)$.
Si F *est un sous-espace stable par* A*, alors* $F^\perp$ *est stable par* A^*.

Démonstration :
On se donne un vecteur x de E et on considère la forme linéaire $\phi \in E^*$ définie par $\phi(y) = b(x, Ay)$.
Comme ϕ_b est un isomorphisme, il existe un unique x' tel que $b(x', y) = \phi(y)$ pour tout y et c'est bien sûr $x' = \phi_b^{-1}(\phi)$.
On voit (entre autre grâce à l'unicité) que l'application $x \mapsto x'$ existe et est linéaire. On peut donc écrire $x' = A^*x$, où A^* est un endomorphisme et on a par construction $b(A^*x, y) = b(x', y) = \phi(y) = b(x, Ay)$.
Pour la dernière assertion, on remarque que si $x \in F^\perp$ et y dans F, alors $b(A^*x, y) = b(x, Ay) = 0$ car $Ay \in F$.
Il vient donc que $A^*x \in F^\perp$.

□

On peut résumer cette construction en un diagramme commutatif : 

Introduction à la théorie des groupes classiques, Chap. 4, 5, Rached Mneimné, Frédéric Testard, **Hermann**.
Cours d'algèbre, Chap. V, VI, VIII, Daniel Perrin, **Ellipses**.

Chapitre V

Décomposition polaire et applications

Ce n'est pas sous Sarko 1er que je vais devoir expliquer l'adage "Il faut diviser pour régner". Cette tactique étant féconde dans des milieux diverses allant de la politique à l'informatique, il est naturel qu'elle le soit en mathématiques. Les théorèmes de décomposition en sont l'illustration flagrante. Par exemple, la décomposition de Dunford permet de séparer les problèmes de réduction en 1) diagonalisable (où l'avantage est orbites fermées, polynômes caractéristiques comme invariants totaux...) et 2) nilpotents (avantages : nombre fini d'orbites, une seule valeur propre...).
Nous allons voir que, pour la plupart des groupes classiques sur $\mathbb{R}$ et $\mathbb{C}$, ceux-ci se divisent en deux parties aux avantages complémentaires. Une partie est compacte, l'autre ne l'est pas, mais en revanche, est homéomorphe à un espace topologique particulièrement sympathique : l'espace vectoriel. C'est donc la décomposition polaire qui va permettre de régner sur les groupes classiques, au moins de façon topologique. Comme application, nous montrerons que la décomposition polaire permet d'avoir une description des composantes connexes de $O(p,q)$, et donc finalement des quadriques réelles sur lesquelle $O(p,q)$ agit transitivement.

1 Théorème de décomposition polaire

Voici ce qui sera le théorème principal du chapitre.

Théorème 16 :
La multiplication définit un homéomorphisme :

i) $\mu : O(n,\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) \cong GL_n(\mathbb{R})$

ii) $\mu : U(n,\mathbb{C}) \times H_n^{++}(\mathbb{C}) \cong GL_n(\mathbb{C})$

Rappel :
$\mathcal{S}_n^{++}(\mathbb{R}) := \{S \in GL_n(\mathbb{R}) : {}^tS = S, \quad {}^txSx > 0 \quad \forall x \in \mathbb{R}^n\backslash_{\{0\}}\} = \{P\,{}^tP \in M_n(\mathbb{R}) : P \in GL_n(\mathbb{R})\}$
$H_n^{++}(\mathbb{C}) := \{H \in GL_n(\mathbb{C}) : H^* = H, \quad x^*Hx > 0 \quad \forall x \in \mathbb{C}^n\backslash_{\{0\}}\} = \{PP^* \in M_n(\mathbb{C}) : P \in GL_n(\mathbb{C})\}$
On sait que $\forall x \in \mathbb{C}, \quad x^*Hx =< x, x >_H \in \mathbb{R}$ car $<,>_H$ est un produit scalaire (hermitien).
De plus, pour $n = 1$, *ii)* donne $z = \rho e^{i\theta}$.

Démonstration :

i) μ est bien définie et clairement continue. Montrons sa surjectivité :
Soit $M \in GL_n(\mathbb{R})$. Alors ${}^tMM \in \mathcal{S}_n^{++}(\mathbb{R})$ car dans l'orbite de I_n pour l'action de congruence.
Donc ${}^tMM = P \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} P^{-1}$ avec $P \in O(n,\mathbb{R})$ car ${}^tMM$ est symétrique et $\lambda_i > 0$ car elle est définie

positive. On pose alors $S = P \begin{bmatrix} \sqrt{\lambda_1} & & \\ & \ddots & \\ & & \sqrt{\lambda_n} \end{bmatrix} P^{-1}$ qui est encore dans $\mathcal{S}_n^{++}(\mathbb{R})$.

On a $S^2 = {}^tMM$ et si on pose $O = MS^{-1}$, alors ${}^tOO = {}^t(MS^{-1})MS^{-1} = {}^tS^{-1}\,{}^tMMS^{-1} = S^{-1}S^2S^{-1} = I_n$
Ainsi $M = OS$ avec $O \in O(n,\mathbb{R})$ et $S \in \mathcal{S}_n^{++}(\mathbb{R})$ d'où μ surjective.
Montrons qu'elle est injective :
Supposons que $M = OS = O'S'$ avec $O \neq O'$ dans $O(n,\mathbb{R})$ et $S \neq S'$ dans $\mathcal{S}_n^{++}(\mathbb{R})$.
Alors $S^2 = {}^tMM = {}^t(O'S')O'S' = {}^tS'\,{}^tO'O'S'$ d'où $S^2 = S'^2$.
Soit Q un polynôme d'interpolation de Lagrange tel que $Q(\lambda_i) = \sqrt{\lambda_i}$, pour les λ_i distincts. Alors

$$S = P \begin{bmatrix} \sqrt{\lambda_1} & & \\ & \ddots & \\ & & \sqrt{\lambda_n} \end{bmatrix} P^{-1} = PQ\left(\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}\right) P^{-1} = Q\left(P \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} P^{-1}\right) = Q(S^2) = Q(S'^2)$$

S' commute avec S'^2 donc avec $Q(S'^2) = S$ d'où S' et S sont diagonalisables dans une base commune.
Ainsi, si l'on note $d(\mu_i) = \begin{bmatrix} \mu_1 & & \\ & \ddots & \\ & & \mu_n \end{bmatrix}$, on a $S' = P_0 d(\mu'_i) P_0^{-1}$ et $S = P_0 d(\mu_i) P_0^{-1}$.
Donc $S'^2 = S^2 \implies P_0 d(\mu_i'^2) P_0^{-1} = P_0 d(\mu_i^2) P_0^{-1}$
$\implies \mu_i'^2 = \mu_i^2 \quad \forall 1 \leq i \leq n$
$\implies \mu'_i = \mu_i \quad \forall 1 \leq i \leq n \quad$ car $S, S' \in \mathcal{S}_n^{++}(\mathbb{R}) \implies \mu_i, \mu'_i \in \mathbb{R}^{+*}$
$\implies S = S'$ et donc $O = O'$ d'où finalement μ injective.
Montrons sa bicontinuité :
Soit $(M_p)_{p\in\mathbb{N}} = (O_p S_p)_{p\in\mathbb{N}}$ une suite de $O(n,\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$ telle que $M_p \xrightarrow[p\to\infty]{} M \in GL_n(\mathbb{R})$,
avec $M = OS \in O(n,\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R})$.
Il suffit de montrer la continuité réciproque, c'est à dire que O_p et S_p convergent respectivement vers O et S.
Or $O(n,\mathbb{R})$ est compact (fermé borné pour $\|\!|\cdot|\!\|_2$). Soit $\bar{O}$ une valeur d'adhérence de $(O_p)_{p\in\mathbb{N}}$, i.e. telle que $O_{p_k} \xrightarrow[k\to\infty]{} \bar{O}$. On a $S_{p_k} \xrightarrow[k\to\infty]{} \bar{O}^{-1}M$ qui est symétrique et définie positive car

$$\bar{S} := \bar{O}^{-1}M \in GL_n(\mathbb{R}) \cap \overline{\mathcal{S}_n^{++}(\mathbb{R})} = GL_n(\mathbb{R}) \cap \mathcal{S}_n^{+}(\mathbb{R}) = \mathcal{S}_n^{++}(\mathbb{R}).$$

(Ah ! Les clotures d'orbites...) On a donc $M = \bar{O}\,\bar{S}$ et $\bar{O} = O,\ \bar{S} = S$ par unicité de la décomposition polaire (injectivité de μ).

ii) Similaire. Laissé en exercice.

□

Exercice :
Montrer que $\|\!|A|\!\|_2 = \sqrt{\rho({}^tAA)}$ avec $\rho(M) = \max_{1\leq i\leq n}\{|\lambda_i| :\ \lambda_i \in \mathrm{Spec}(M)\}$ en utilisant la décomposition polaire.

Remarque :
Les groupes classiques G réels ou complexes que nous étudions contiennent un sous-groupe compact K maximal et tel que G/K soit homéomorphe à un espace vectoriel.
Ce sous-groupe est unique à conjugaison près : c'est $O(n)$ dans $GL_n(\mathbb{R})$, $SO(n)$ dans $SL_n(\mathbb{R})$ par exemple, ou encore $U(n)$ dans $GL_n(\mathbb{C})$ et $SU(n)$ dans $SL_n(\mathbb{C})$. Attention, $O(n,\mathbb{C})$ aurait du mal à être compact ; par exemple, il agit transitivement sur la nappe $z_1^2 + z_2^2 = 1$ qui contient l'hyperbole $x_1^2 - y_2^2 = 1$.

2 L'exponentielle

L'exponentielle est un outil fondamental dans le cadre des groupes de Lie, cf Chapitre VIII p83. Son utilité principale étant qu'elle permet de retrouver le groupe à partir de son espace tangent en l'identité. Le premier exemple basique bien connu est la formule de Moivre $exp(it) = \cos t + i \sin t$ où l'on voit que le groupe du cercle peut être retrouvé à partir de son espace tangent en 1 (l'axe des imaginaires), et ce passage se fait via l'exponentielle.
Soit un corps $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. On définit

$$\begin{array}{rccc} \exp : & M_n(\mathbb{K}) & \longrightarrow & M_n(\mathbb{K}) \\ & A & \longmapsto & \exp(A) = \sum_{i=0}^{\infty} \frac{A^i}{i!} \end{array}$$

Voici un résumé des diverses formules et propriétés de l'exponentielles qui serviront dans la suite. Nous laissons les preuves au lecteur en donnant toutefois quelques indications.

Propositions :

- *La série* $\exp(A)$ *converge normalement sur tout compact. C'est une fonction continue.*
- $\exp(PAP^{-1}) = P \exp(A) P^{-1}$, $\exp({}^tA) = {}^t\exp(A)$.
- *Si* A *et* B *commutent alors* $\exp(A+B) = \exp(A)\exp(B)$.
  (Le terme de droite est un produit de séries $\sum_{i=1}^{\infty} a_i \sum_{j=1}^{\infty} b_j$ et le terme de gauche est, comme A et B commutent, la série produit $\sum_{k=1}^{\infty} \sum_{i=1}^{\infty} a_i b_{k-i}$ de ces deux séries. La convergence absolue assure que la série produit converge vers le produit des séries).
- $\exp(-A) = \exp(A)^{-1}$. En particulier $\exp(A)$ est inversible.
- Sur une matrice diagonale $d(a_i) = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$, on a $\exp d(a_i) = d(e^{a_i})$.
- Si N est nilpotente, alors $\exp(N - Id)$ est nilpotente.
- Le spectre de $\exp(A)$ est $\{e^{\lambda},\ \lambda \in \mathrm{Spec}(A)\}$
  (On peut utiliser par exemple la décomposition de Dunford).
- Soit $A \in M_n(\mathbb{K})$, alors $\{exp(tA),\ t \in \mathbb{R}\}$ est un sous-groupe de $GL_n(\mathbb{K})$.
- La fonction exp n'est pas injective (calculer $\exp \begin{bmatrix} 0 & 2\pi i \\ -2\pi i & 0 \end{bmatrix}$).
  La différentielle de exp en 0 est Id. En particulier, par le théorème d'inversion locale (voir théorème 18), exp réalise un difféomorphisme local sur un voisinage de 0.
  On peut définir son inverse sur la boule ouverte centrée en Id de rayon 1 :

$$\log(\mathrm{Id} + H) = \sum_{k \geq 1} (-1)^{k-1} \frac{H^k}{k}$$

Proposition 31 :

i) $\exp : \mathcal{S}_n(\mathbb{K}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{K})$ *est un homéomorphisme*

ii) $\exp : H_n(\mathbb{C}) \longrightarrow H_n^{++}(\mathbb{C})$ *est un homéomorphisme*

retour p50

Démonstration :

i) Soit $S \in \mathcal{S}_n(\mathbb{K})$. Alors $S = Pd(\lambda_i)P^{-1}$, avec $d(\lambda_i)$ matrice diagonale des $\lambda_i \in \mathbb{R}$.
$\exp(S) = Pd(e^{\lambda_i})P^{-1} \in \mathcal{S}_n^{++}(\mathbb{K})$ car $e^{\lambda_i} > 0 \quad \forall i$ et $P \in O(n, \mathbb{K})$, donc exp est bien définie et par restriction, elle est continue.
Montrons qu'elle est surjective : Soit $B \in \mathcal{S}_n^{++}(\mathbb{K})$. $B = Pd(\mu_i)P^{-1}$, avec $P \in O(n, \mathbb{K})$. Alors puisque $\mu_i > 0$, $\exists A = Pd(\ln \mu_i)P^{-1} \in \mathcal{S}_n(\mathbb{K})$ telle que $\exp A = B$ d'où la surjectivité.
Montrons qu'elle est injective : supposons que $\exp A = \exp A' \in \mathcal{S}_n^{++}(\mathbb{K})$, avec $A, A' \in \mathcal{S}_n(\mathbb{K})$.
Soit Q un polynôme interpolateur de Lagrange tel que $Q(e^{\lambda_i}) = \lambda_i$. Alors A' commute avec $Q(\exp A') = Q(\exp A) = A$. Par diagonalisation simultanée, on conclut, comme dans la preuve de la décomposition polaire, que $A = A'$ et donc exp est injective.
Montrons qu'elle est bicontinue : Soit $(B_p)_{p\in\mathbb{N}} = (\exp(A_p))_{p\in\mathbb{N}}$ telle que $B_p \xrightarrow[p\to\infty]{} B = \exp A \in \mathcal{S}_n^{++}(\mathbb{K})$.
Montrons que $A_p \xrightarrow[p\to\infty]{} A$.
$B_p \xrightarrow[p\to\infty]{} B$ donc B_p est bornée pour $\|\cdot\|_2$. De même, $B_p^{-1} \xrightarrow[p\to\infty]{} B^{-1}$ car $B \in \mathcal{S}_n^{++}(\mathbb{K})$, donc B_p^{-1} est bornée pour $\|\cdot\|_2$. Or si $M \in \mathcal{S}_n^{++}(\mathbb{K})$,

$$\begin{aligned} \|M\|_2 &= \sqrt{\rho({}^tMM)} \text{ (voir exercice page 60)} \\ &= \sqrt{\rho(M^2)} \\ &= \rho(M) \\ &= \max\{\mathrm{Spec}(M)\} \end{aligned}$$

Donc $(\mathrm{Spec}\, B_p)_{p\in\mathbb{N}}$ appartient à un compact K de $[0, +\infty[$ et en appliquant le même raisonnement à B_p^{-1}, on peut se ramener à un compact de $]0, +\infty[$. Donc les valeurs propres de A_p logarithmes des valeurs propres de B_p sont dans un compact de $\mathbb{R}$, car $\ln(K)$ est inclus dans un compact.
Donc A_p est bornée pour $\|\cdot\|_2$.
Toutes ses valeurs d'adhérence valent A car $\exp A_{p_k} = B_{p_k} \Longrightarrow \exp \overline{A} = B = \exp A \Longrightarrow \overline{A} = A$ par unicité.
Donc $A_p \xrightarrow[p\to\infty]{} A$.

ii) Similaire. Laissé en exercice

□

A l'aide de l'exponentielle, on arrive donc aux conséquences topologiques annoncées du théorème de décomposition polaire.

Corollaire 8 :
On a les homéomorphismes :

$$GL_n(\mathbb{R}) \cong O(n, \mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}} \qquad et \qquad GL_n(\mathbb{C}) \cong U(n, \mathbb{C}) \times \mathbb{R}^{n^2}$$

3 Applications à l'étude[10] de $O(p,q)$

Nous avons choisi de présenter une application de la décomposition polaire à l'étude du groupe $O(p,q)$. Il va en résulter une description de sa composante connexe en l'identité. Contrairement au cas de $O(n,\mathbb{R})$, il ne s'agira pas de $SL_n(\mathbb{R}) \cap O(p,q)$, mais d'un sous-groupe d'indice deux de ce dernier, appelé groupe orthochrone, nom qui lui va comme un gant, mais qui irait aussi à un groupe de Heavy Metal si besoin était.

Proposition 32 :
Soient $p, q \neq 0$.
$O(p,q) \cong O(p) \times O(q) \times \mathbb{R}^{pq}$

Démonstration :
Soit $M \in O(p,q) \subset GL_n(\mathbb{R})$, avec $n = p+q$.
$\exists O \in O(n,\mathbb{R})$ et $\exists S \in \mathcal{S}_n^{++}(\mathbb{R})$ telles que $M = OS$. (décomposition polaire)
On veut montrer que S et O sont dans $O(p,q)$. Pour cela, il suffit de montrer que S l'est.

Soit $T = {}^tMM$. On a comme à l'accoutumée $S^2 = T$.
Montrons dans un premier temps que $O(p,q)$ est stable par transposition.

$$\begin{aligned} M \in O(p,q) &\implies MI_{p,q}\,{}^tM = I_{p,q} \\ &\implies {}^tM^{-1} I_{p,q} M^{-1} = I_{p,q} \\ &\implies {}^tM^{-1} \in O(p,q) \\ &\implies {}^tM \in O(p,q) \end{aligned}$$

On en déduit que $T = {}^tMM \in O(p,q)$
On a donc $S^2 \in O(p,q)$. Pour conclure sur S, il va falloir prendre la "racine carrée" de T, donc, via l'exponentielle, diviser par deux. $T = S^2 \in \mathcal{S}_n^{++}(\mathbb{R}) \implies T = \exp U$ avec $U \in \mathcal{S}_n(\mathbb{R})$

$$\begin{aligned} T \in O(p,q) &\iff TI_{p,q}\,{}^tT = I_{p,q} \\ &\iff {}^tT = I_{p,q} T^{-1} I_{p,q}^{-1} \\ &\iff {}^t\exp U = I_{p,q} \exp^{-1} U\, I_{p,q}^{-1} \\ &\iff \exp{}^tU = I_{p,q} \exp(-U)\, I_{p,q}^{-1} \\ &\iff \exp{}^tU = \exp(-I_{p,q} U I_{p,q}^{-1}) \\ &\iff {}^tU = U = -I_{p,q} U I_{p,q}^{-1} \qquad \text{car } \exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R}) \text{ bijective} \\ &\iff UI_{p,q} + I_{p,q}U = 0 \qquad \text{condition linéaire} \end{aligned}$$

$$\implies \frac{U}{2} I_{p,q} + I_{p,q} \frac{U}{2} = 0$$

$$\begin{aligned} &\iff \frac{{}^tU}{2} = -I_{p,q} \frac{U}{2} I_{p,q}^{-1} \\ &\iff \exp\left(\frac{{}^tU}{2}\right) = \exp\left(-I_{p,q} \tfrac{U}{2} I_{p,q}^{-1}\right) \\ &\iff {}^t\exp\left(\tfrac{U}{2}\right) = I_{p,q} \exp^{-1}\left(\tfrac{U}{2}\right) I_{p,q}^{-1} \end{aligned}$$

Or $\exp\left(\frac{U}{2}\right) \in \mathcal{S}_n(\mathbb{R})$ et $\exp^2\left(\frac{U}{2}\right) = \exp U = T$
Donc $\exp\left(\frac{U}{2}\right) = S$ et $SI_{p,q}\,{}^tS = I_{p,q}$ ie. $S \in O(p,q)$. Et voila !

[10] On notera $O(p,q)$ le groupe $O(p,q,\mathbb{R})$ puisqu'il est clair que celui-ci n'est défini que sur $\mathbb{R}$. On notera aussi dans ce contexte $O(p)$ le groupe $O(p,\mathbb{R})$. Contrairement à $O(p,q)$, on peut toutefois définir $O(p)$ sur $\mathbb{C}$.

D'où $O \in O(p,q)$ et $O(p,q) \cong \big(O(p,q) \cap O(n)\big) \times \big(O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R})\big)$
La continuité venant de ce que la décomposition polaire est un homéomorphisme.
Reste à comprendre le groupe $O(p,q) \cap O(n)$ ainsi que $O(p,q) \cap S_n^{++}$. Pour le premier :
Soit $O = \begin{bmatrix} A & C \\ B & D \end{bmatrix} \in O(p,q) \cap O(n)$

$$O \in O(p,q) \iff \begin{cases} {}^tAA - {}^tBB = I_p \\ {}^tAC - {}^tBD = 0 \\ {}^tCA - {}^tDB = 0 \\ {}^tCC - {}^tDD = -I_q \end{cases} \quad \text{car} \quad \begin{bmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{bmatrix} \begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix} \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{bmatrix} \begin{bmatrix} A & C \\ -B & -D \end{bmatrix}$$

$$= \begin{bmatrix} {}^tAA - {}^tBB & {}^tAC - {}^tBD \\ {}^tCA - {}^tDB & {}^tCC - {}^tDD \end{bmatrix} = \begin{bmatrix} I_p & 0 \\ 0 & -I_q \end{bmatrix}$$

$$O \in O(n) \iff \begin{cases} {}^tAA + {}^tBB = I_p \\ {}^tAC + {}^tBD = 0 \\ {}^tCA + {}^tDB = 0 \\ {}^tCC + {}^tDD = I_q \end{cases} \quad \text{car} \quad \begin{bmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{bmatrix} \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} {}^tAA + {}^tBB & {}^tAC + {}^tBD \\ {}^tCA + {}^tDB & {}^tCC + {}^tDD \end{bmatrix} = \begin{bmatrix} I_p & 0 \\ 0 & I_q \end{bmatrix}$$

D'où ${}^tBB = 0$. Ainsi $Spec({}^tBB) = \{0\}$ donc $\|B\|_2^2 = \rho({}^tBB) = 0 \Longrightarrow B = 0$. De même $C = 0$, donc $A \in O(p)$ et $D \in O(q)$

Donc $O(p,q) \cap O(n) \cong \left\{ \begin{bmatrix} A & 0 \\ 0 & D \end{bmatrix} \,:\, A \in O(p), D \in O(q) \right\} \cong O(p) \times O(q)$

Pour le second, on réutilise l'exponentielle :
$\exp : \mathcal{S}_n(\mathbb{R}) \longrightarrow \mathcal{S}_n^{++}(\mathbb{R})$ est un homéomorphisme,
ainsi que $\exp : L = \{U \in GL_n(\mathbb{R}) : UI_{p,q} + I_{p,q}U = 0\} \longrightarrow O(p,q)$ comme on a vu plus haut, d'où

$$\mathcal{S}_n(\mathbb{R}) \cap L \cong O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R})$$

$\mathcal{S}_n(\mathbb{R})$ étant un $\mathbb{R}-$espace vectoriel (de dimension $\frac{n(n+1)}{2}$), et son intersection avec L étant de dimension pq (exercice), on a que $O(p,q) \cap \mathcal{S}_n^{++}(\mathbb{R}) \cong \mathbb{R}^{pq}$, d'où finalement :

$$O(p,q) \cong O(p) \times O(q) \times \mathbb{R}^{pq}$$

□

Remarque :
Cette preuve est importante, car elle utilise une méthode applicable à beaucoup de groupes.

Remarque :
On déduit de la proposition que $O(p,q)$ est compact si et seulement si $p = 0$ ou $q = 0$.

Proposition 33 :

i) $O(p,q)$ *a quatre composantes connexes,*

ii) *La composante connexe de l'identité est* $SO_0(p,q) = \left\{ \left[\begin{smallmatrix} A & C \\ B & D \end{smallmatrix} \right] \in SO(p,q) \,:\, A \in GL_p^+(\mathbb{R}) \right\}$.

iii) $O(p,q)/SO_0(p,q) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Remarque :
On rappelle que la composante connexe de l'identité dans $O(n,\mathbb{K})$ est $SO(n,\mathbb{K})$, qui est d'indice 2 dans $O(n,\mathbb{K})$, $\mathbb{K}$ désignant le corps complexe ou réel.

Démonstration :

i) il est clair par l'homéomorphisme précédent, que $O(p,q)$ a quatre composantes connexes, puisque $O(n)$ en a deux.

ii) $O(p,q) \xrightarrow{\det} \{\pm 1\}$ et puisque $\mathrm{Ker}(\det) = SO(p,q)$, on a la suite exacte

$$1 \hookrightarrow SO(p,q) \hookrightarrow O(p,q) \xrightarrow{\det} \{\pm 1\} \twoheadrightarrow 1$$

Et donc ${}^{O(p,q)}\!/_{SO(p,q)} \simeq \{\pm 1\}$. Ainsi $O(p,q) = SO(p,q) \sqcup g\, SO(p,q)$ avec $g \in O(p,q) \backslash_{SO(p,q)}$.

Par exemple $g = \begin{bmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$, d'où $SO(p,q)$ a deux composantes connexes. Soit $M = \begin{bmatrix} A & C \\ B & D \end{bmatrix} \in SO(p,q)$.

On a vu que ${}^tAA = I_n + {}^tCC$, donc ${}^tAA \in \mathcal{S}_n^{++}(\mathbb{R})$ car $< Ax, Ax > = < x, x > + < Cx, Cx > > 0$, pour $x \neq 0$.

Puisque $\det A \neq 0$, on peut définir $f : \begin{array}{ccc} SO(p,q) & \longrightarrow & \{\pm 1\} \\ \begin{bmatrix} A & C \\ B & D \end{bmatrix} & \longmapsto & \dfrac{\det A}{|\det A|} \end{array}$ morphisme continu (fraction de polynômes).

Ainsi puisque $f(I_n) = 1$, et f constante sur sa composante connexe, on a $f|_{SO_0(p,q)} = 1$

Finalement, $SO(p,q) = SO_0(p,q) \sqcup h\, SO_0(p,q)$ avec h de la forme $\begin{bmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ & & & & -1 \end{bmatrix}$ et $f|_{hSO_0(p,q)} = -1$.

On a bien $SO_0(p,q) = \mathrm{Ker}(f) = \left\{ \left[\begin{smallmatrix} A & C \\ B & D \end{smallmatrix} \right] \in SO(p,q) \,:\, A \in GL_p^+(\mathbb{R}) \right\}$

iii) Laissé en exercice. ${}^{O(p,q)}\!/_{SO_0(p,q)} = \{SO_0(p,q),\, g\, SO_0(p,q),\, h\, SO_0(p,q),\, gh\, SO_0(p,q)\}$

□

Remarque :
On a vu que $O(p,q)$ agissait de façon transitive sur les nappes d'équation

$$\sum_{i=1}^{p} x_i^2 - \sum_{i=1}^{q} y_i^2, \quad x_i, y_i \in \mathbb{R}.$$

On montre facilement qu'il en est de même de $SO(p,q)$. (en dimension $n \leq 2$). En conclusion, une telle nappe a au plus deux composantes connexes. En dimension 3, on voit qu'il existe des hyperboloïdes à une nappe et des hyperboloïdes à deux nappes. Par le théorème de Sylvester, on voit que les composantes connexes possibles pour une quadrique sont au nombre de 1 ou 2. Lorsqu'il y a deux composantes connexes, le groupe $SO_0(p,q)$ agit transitivement sur chacune des composante connexe, mais pas sur tout la nappe, par connexité.

Remarque :
Le groupe $SO_0(p,q)$ est appelé groupe orthochrone, pour forcer le respect, mais aussi en lien avec la forme de Lorentz $x^2 + y^2 + z^2 - t^2$, où le groupe orthochrone agit sur les nappes en préservant l'orientation du temps, ce qui est préférable.

Pour vérifier si vous avez bien compris les méthodes de ce chapitre, vous pouvez faire l'exercice suivant :

Exercice :
Montrer que $O(n,\mathbb{C}) \cong O(n,\mathbb{R}) \times \mathbb{R}^{\frac{n(n-1)}{2}}$ (décomposition polaire hermitienne).

Introduction à la théorie des groupes classiques, chap. 1, 3, 4, 5, Rached Mneimné, Frédéric Testard, **Hermann**.

Chapitre VI

Combinatoire algébrique

« Rhââ lovely »

Frenzy, Alfred Hitchcock, 1972.

Les corps finis sont un passage obligé dans grand nombre de problèmes arithmétiques, mais nous n'aborderons malheureusement pas ce point de vue. Dans ce chapitre, nous apportons un nouvel éclairage sur les groupes classiques et la géométrie en les considérant sur les corps finis. On retrouve l'équivalent des groupes déjà étudiés sur $\mathbb{R}$ et $\mathbb{C}$ (groupe linéaire, groupe spécial linéaire, groupe orthogonal), mais cette fois-ci l'approche combinatoire se substitue à l'approche topologique. Les groupes agiront sur des objets géométriques, mais la surjectivité ou parfois l'injectivité, pourra être montrée à l'aide du dénombrement.
Le dénombrement des objets du cours possède un premier avantage, il permet de mieux comprendre, voire de tester sa compréhension, selon le principe que "compter, c'est comprendre". Par exemple, il n'y a rien de mieux pour sentir que l'on a dominé la notion de repère projectif, que de compter le nombre de repères projectifs sur les corps finis, et ainsi, réaliser l'aide qu'apporte une action du groupe adéquat dans ce dénombrement. Le second point positif, c'est que cette approche des objets géométriques est particulièment jubilante : compter, c'est jouer avec les nombres, c'est la magie de l'enfance des mathématiques, et ici, jointe à une géométrie des corps finis, hautement hallucinogène.

Nous profiterons de cet enthousiasme général pour faire passer des premières notions de géométrie projective, qui seront reprises dans les prochains chapitres. Nous rencontrerons l'espace projectif, les repères projectifs et le groupe projectif. Enfin, nous remarquerons des isomorphismes dits exceptionnels entre groupes de nature différente, pour n'en citer qu'un, le groupe projectif $PSL_2(\mathbb{F}_5)$, défini comme étant le quotient du groupe $SL_2(\mathbb{F}_5)$ par ses homothéties est isomorphe au groupe alterné $\mathcal{A}_5$. Encore une fois, le dénombrement sera essentiel dans l'étude de ces isomorphismes. Les isomorphismes exceptionnels sur $\mathbb{R}$ et $\mathbb{C}$, plus difficiles, seront étudiés dans un chapitre ultérieur, à l'aide non seulement de la topologie, mais d'une structure de variété différentielle sur les groupes (dits de Lie).

1 Dénombrement sur les corps finis

Nous allons dénombrer quelques objets courants de la géométrie sur un corps fini $\mathbb{F}_q$.
On rappelle que $\mathbb{P}^{n-1}(\mathbb{F}_q)$ représente l'ensemble des droites de l'espace $\mathbb{F}_q^n$. Le groupe $PGL_n(\mathbb{F}_q)$ est le quotient de $GL_n(\mathbb{F}_q)$ par ses homothéties $\mathbb{F}_q^*$. Sa fonction étant d'agir de façon fidèle sur l'espace projectif $\mathbb{P}^{n-1}(\mathbb{F}_q)$. Un repère projectif de $\mathbb{P}^{n-1}(\mathbb{F}_q)$ est un $(n+1)$-uplet de droites de $\mathbb{F}_q^n$ telles qu'aucune sous-famille à n éléments ne soit dans un même hyperplan de $\mathbb{F}_q^n$. Pour se familiariser avec la notion de repère projectif, il est recommandé de regarder le cas de la dimension 2, voir page 95.

Proposition 34 :
On a les cardinalités suivantes :

i) *Espace vectoriel* $\quad |\mathbb{F}_q^n| = q^n$.

ii) *Espace projectif* $\quad |\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^n$

iii) *Groupe général linéaire* $\quad |GL_n(\mathbb{F}_q)| = (q^n-1)(q^{n-1}-1)\cdots(q-1)q^{\frac{n(n-1)}{2}}$. *C'est aussi le nombre de bases de* $\mathbb{F}_q^n$.

iv) *Groupe projectif linéaire* $\quad |PGL_n(\mathbb{F}_q)| = (q^n-1)(q^{n-1}-1)\cdots(q^2-1)q^{\frac{n(n-1)}{2}}$, *c'est aussi le nombre de repères de* $\mathbb{P}^{n-1}$.

v) *Groupe spécial linéaire* $\quad |SL_n(\mathbb{F}_q)| = (q^n-1)(q^{n-1}-1)\cdots(q^2-1)q^{\frac{n(n-1)}{2}}$

vi) *Grassmanienne* $\quad |Gr_{m,n}(\mathbb{F}_q)| = \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-m+1}-1)}{(q^m-1)(q^{m-1}-1)\cdots(q-1)}$ *qui tend vers* $\binom{n}{m}$ *quand* $q \to 1$.

vii) *Variété de drapeau* $\quad \mathcal{F}_n(\mathbb{K}) = \{(F_0,\ldots,F_n),\ \dim F_i = i,\ \{0\} = F_0 \subset \cdots \subset F_n = \mathbb{K}^n\}$
$|\mathcal{F}_n(\mathbb{F}_q)| = \displaystyle\prod_{k=1}^{n-1}(1 + q + \cdots + q^k)$

Démonstration :

i) Clair.

ii) On fait agir le groupe multiplicatif $\mathbb{K}^*$ sur $\mathbb{K}^{n+1}\backslash_{\{0\}}$ par homothétie i.e. $(\lambda, v) \longmapsto \lambda v$.
Soit $v \in \mathbb{K}^{n+1}\backslash_{\{0\}}$. Alors $\mathrm{Stab}(v) = \{1\}$ (l'action est libre), d'où pour $\mathbb{K} = \mathbb{F}_q$:
$|\mathbb{P}^1(\mathbb{F}_q)| = \left|\mathbb{F}_q^{n+1}\backslash_{\{0\}} \middle/ \mathbb{F}_q^*\right| = \dfrac{|\mathbb{F}_q^{n+1}\backslash_{\{0\}}|}{|\mathbb{F}_q^*|} = \dfrac{q^{n+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^n$
Dit autrement : les orbites sont les droites de $\mathbb{F}_q^{n+1}$. Avec $q^{n+1}-1$ vecteurs directeurs possibles (on enlève le vecteur nul) et sachant qu'une même droite peut être engendrée par $q-1$ vecteurs directeurs différents, elles sont donc bien au nombre de $\dfrac{q^{n+1}-1}{q-1}$.

iii) On fait agir $GL_n(\mathbb{K})$ sur $\mathbb{K}^n\backslash_{\{0\}}$.
L'action est transitive et de stabilisateur $\mathrm{Stab}(e_1) = \begin{bmatrix} 1 & * \\ 0 & GL_{n-1}(\mathbb{K}) \end{bmatrix} = GL_{n-1}(\mathbb{K}) \ltimes \mathbb{K}^{n-1}$.

Pour $\mathbb{K} = \mathbb{F}_q$, on a $\left| {}^{GL_n(\mathbb{F}_q)}\middle/_{GL_{n-1}(\mathbb{F}_q)\ltimes\mathbb{F}_q^{n-1}} \right| = |\mathbb{F}_q^n\backslash_{\{0\}}| \Longrightarrow |GL_n(\mathbb{F}_q)| = |GL_{n-1}(\mathbb{F}_q)| \cdot q^{n-1}(q^n-1)$.
Par itération, $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

Une autre méthode consiste à compter le nombre de bases de $\mathbb{F}_q^n$.
En effet, on a une bijection $\phi :\ \begin{array}{ccc} GL_n(\mathbb{K}) & \longrightarrow & \mathbb{B} = \{\text{ bases de } \mathbb{K}^n\} \\ g & \longmapsto & g\,\mathcal{B}_0 \end{array}$
ou encore, $GL_n(\mathbb{K})$ agit sur $\mathbb{B}$ de façon simplement (ϕ injective) transitive (ϕ surjective).

Pour $\mathbb{K} = \mathbb{F}_q$, une base étant une partie libre à n éléments de $\mathbb{F}_q^n$, son premier vecteur est non nul : il y en a donc $q^n - 1$.
Le second vecteur doit être non-colinéaire au premier, il y en a $q^n - q$. On continue jusqu'au n-ième vecteur, non-colinéaire aux $n-1$ premiers vecteurs et donc au choix parmi $q^n - q^{n-1}$ vecteurs.
On obtient bien $|\mathbb{B}| = |GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

iv) Le gagne-pain de $PGL_n(\mathbb{K})$, c'est d'agir sur les droites. On a la suite exacte :

$$1 \longrightarrow \mathbb{K}^* \hookrightarrow GL_n(\mathbb{K}) \twoheadrightarrow PGL_n(\mathbb{K}) \longrightarrow 1$$

D'où $PGL_n(\mathbb{K}) \simeq {}^{GL_n(\mathbb{K})}\!/_{\mathbb{K}^*}$ et pour $\mathbb{K} = \mathbb{F}_q$,

$$|PGL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{|\mathbb{F}_q^*|} = (q^n-1)(q^{n-1}-1)\cdots(q^2-1)q^{\frac{n(n-1)}{2}}$$

On peut encore compter le nombre de bases projectives de $\mathbb{P}^{n-1}$:

$$|PGL_n(\mathbb{F}_q)| = (\underbrace{1+q+\cdots+q^{n-1}}_{\in \mathbb{P}^{n-1}})(\underbrace{q+\cdots+q^{n-1}}_{\in \mathbb{P}^{n-1}\setminus\{1\}})\cdots \underbrace{q^{n-1}}_{\in \mathbb{P}^{n-1}\setminus\mathbb{P}^{n-2}}\ (q-1)^{n-1}$$

v) De même, on a la suite exacte $1 \longrightarrow SL_n(\mathbb{K}) \hookrightarrow GL_n(\mathbb{K}) \xrightarrow{\det} \mathbb{K}^* \longrightarrow 1$
D'où $\mathrm{Im}(\det) = \mathbb{K}^* \simeq {}^{GL_n(\mathbb{K})}\!/_{\mathrm{Ker}(\det)} = {}^{GL_n(\mathbb{K})}\!/_{SL_n(\mathbb{K})}$ et pour $\mathbb{K} = \mathbb{F}_q$, $\quad |SL_n(\mathbb{F}_q)| = \dfrac{|GL_n(\mathbb{F}_q)|}{|\mathbb{F}_q^*|}$

Remarque :
Un groupe quotient n'est pas toujours un sous-groupe. En revanche, un espace vectoriel quotient est toujours un sous-espace vectoriel. Voir le chapitre sur les produits semi-directs p26.

vi) $GL_n(\mathbb{K})$ agit transitivement sur la grassmanienne $Gr_{m,n}(\mathbb{K})$. Démonstration détaillée p**??**.

$$\begin{aligned}\mathrm{Stab}(F) &= \{g \in GL_n(\mathbb{K}) \,:\, g(f_i) = \lambda(f_i),\ \lambda \in \mathbb{K}\} = \begin{bmatrix} GL_m(\mathbb{K}) & M_{m,n-m}(\mathbb{K}) \\ 0 & GL_{n-m}(\mathbb{K}) \end{bmatrix} \\ &= (GL_m(\mathbb{K}) \times GL_{n-m}(\mathbb{K})) \ltimes M_{m,n-m}(\mathbb{K})\end{aligned}$$

Ainsi pour $\mathbb{K} = \mathbb{F}_q$, $\quad |Gr_{m,n}(\mathbb{F}_q)| = \dfrac{|GL_n(\mathbb{F}_q)|}{|GL_m(\mathbb{F}_q)| \cdot |GL_{n-m}(\mathbb{F}_q)| \cdot |M_{m,n-m}(\mathbb{F}_q)|}$

Remarque :
On montre mieux : l'expression de $|Gr_{m,n}(\mathbb{F}_q)|$ est un polynôme $P_{m,n}(q)$ tel que $P_{m,n}(1) = \binom{n}{m}$. Ce polynôme représente "l'équivalent polynomial" des nombres binomiaux.

vii) Par le théorème de la base incomplète (encore lui !), $GL_n(\mathbb{K})$ agit transitivement sur les variétés de drapeaux $\mathcal{F}_n(\mathbb{K})$ par translation, et de stabilisateur le groupe des matrices triangulaires supérieures d'éléments diagonaux dans $\mathbb{K}^*$ et donc isomorphe à $(\mathbb{K}^*)^n \ltimes \mathbb{K}^{\frac{n(n-1)}{2}}$ de cardinal (pour $\mathbb{K} = \mathbb{F}_q$) égal à $(q-1)^n q^{\frac{n(n-1)}{2}}$. Donc

$$|\mathcal{F}_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{(q-1)^n q^{\frac{n(n-1)}{2}}}$$

□

Proposition 35 :
Soit q un nombre premier. Les q-Sylow de $GL_n(\mathbb{F}_q)$ sont isomorphes au groupe TSU_n des matrices triangulaires supérieures avec des 1 sur la diagonale. L'ensemble de ces q-Sylow est en bijection naturelle avec les drapeaux complets de $\mathbb{F}_q^n$.

Démonstration :
Posons $G = GL_n(\mathbb{F}_q)$. L'ordre de G est $q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\dots(q-1)$. On en déduit que les q-Sylow de G sont d'ordre $q^{\frac{n(n-1)}{2}}$.
TSU_n est clairement un sous-groupe de $GL_n(\mathbb{F}_q)$ d'ordre $q^{\frac{n(n-1)}{2}}$. C'est donc bien un q-Sylow de G.
On sait qu'un groupe fini G agit transitivement par conjugaison sur l'ensemble $\mathcal{S}$ de ses q-Sylow. L'ensemble $\mathcal{S}$ est donc en bijection avec G/N, où N est le normalisateur d'un Sylow.
Appelons donc N le normalisateur de TSU_n et montrons qu'il s'agit du sous-groupe TS_n des matrices triangulaires supérieures de G.
On a clairement $TS_n \subset N$, puisque si $b \in TS_n$, $u \in TSU_n$, alors bub^{-1} est triangulaire supérieure avec pour seule valeur propre 1.
Réciproquement, soit $m \in N$, montrons que $m \in TS_n$. Tout d'abord, soit $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{F}_q^n$, montrons alors que e_1 est vecteur propre pour m. Pour cela, on sait que la droite $\mathbb{F}_q e_1$ est l'intersection des espaces propres des éléments de TSU_n. Soit $u \in TSU_n$, alors comme m normalise TSU_n, il existe v dans TSU_n tel que $u(m(e_1)) = m(v(e_1)) = m(e_1)$. Conclusion, $m(e_1)$ appartient à l'intersection des espaces propres des éléments de TSU_n, et donc est de la forme ae_1, $a \neq 0$. En quotientant $\mathbb{F}_q^n$ par $\mathbb{F}_q e_1$ (on vient de voir que m passe au quotient !), on obtient par recurrence que m est triangulaire supérieure.
On a donc $\mathcal{S}$ en bijection avec G/TS_n qui est lui-même en bijection avec la variété de drapeau.

□

Remarque :
On vérifie que le nombre de q-Sylow est bien congru à 1 modulo q.

2 Applications aux isomorphismes exceptionnels de groupes finis

On sait que les groupes finis sont classifiés, et cela grâce à un tour de force acharné de mathématiciens du vingtième siècle. Cette classification commence par celle des groupes finis dits simples, ie n'ayant aucun sous-groupe distingué. Parmi les groupes finis simples non abéliens, on peut compter deux séries : les groupes alternés $\mathcal{A}_n$, $n \geq 5$, et les groupes $PSL_n(\mathbb{F}_q)$, $(n,q) \neq (2,2), (2,3)$.
Il est naturel de se demander si les groupes de ces deux séries peuvent accidentellement être isomorphes (ou même à l'intérieur d'une même série). La réponse est "en général non, mais exceptionnellement oui". Ceci amène à la notion d'isomorphismes exceptionnels. Cette notion possède aussi une importance pratique, d'homme de terrain : si on sait par exemple que $PSL_2(\mathbb{F}_4)$ est isomorphe à $\mathcal{A}_5$ lui-même isomorphe à $PSL_2(\mathbb{F}_5)$, alors on a trois façon distinctes d'approcher ce groupe, et on le connaitra donc trois fois mieux.

Voici le cadre général : soit G un groupe agissant sur un ensemble X de cardinal n.
Alors on a un morphisme $\begin{array}{rccc} \phi : & G & \longrightarrow & \mathfrak{S}_X \simeq \mathfrak{S}_n \\ & g & \longmapsto & (\phi_g : X \to X) \end{array}$
Donc $G/\mathrm{Ker}(\phi) \simeq \mathrm{Im}\,\phi \subset \mathfrak{S}_n$

Remarque :
En particulier, l'action de $GL_n(\mathbb{K})$ sur les droites projectives $\mathbb{P}^{n-1}(\mathbb{K})$ par translation a pour stabilisateur $\mathrm{Ker}\,\phi = \mathbb{K}^*$

le groupe des homothéties (un endomorphisme qui stabilise toutes les droites est une homothétie), d'où l'on définit le groupe $PGL_n(\mathbb{K}) := {}^{GL_n(\mathbb{K})}\!/_{\mathbb{K}^*} \subset \mathfrak{S}_{\mathbb{P}^{n-1}(\mathbb{K})}$.
Une permutation de droites peut ainsi être réalisée par une transformation projective.

Voici une liste d'isomorphismes exceptionnels classique de groupes finis :

Proposition 36 :

i) $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

ii) $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4 \subset PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$

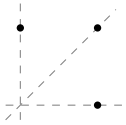
iii) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$

iv) $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5 \subset PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$

Démonstration :

i) $GL_2(\mathbb{F}_2) \circlearrowleft \mathbb{P}^1(\mathbb{F}_2)$:
Comme $\mathbb{F}_2^* = \{1\}$, $PGL_2(\mathbb{F}_2) := {}^{GL_2(\mathbb{F}_2)}\!/_{\mathbb{F}_2^*} = GL_2(\mathbb{F}_2)$. De même, $PSL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$ et puisque sur $\mathbb{F}_2$ on a aussi $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2)$, les premières égalités sont claires.
Enfin puisque $PGL_2(\mathbb{F}_2) \subset \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_2)} = \mathfrak{S}_3$ et $|PGL_2(\mathbb{F}_2)| = \frac{(2^2-1)(2^2-2)}{2-1} = 6 = |\mathfrak{S}_3|$, on en conclut que $PGL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.

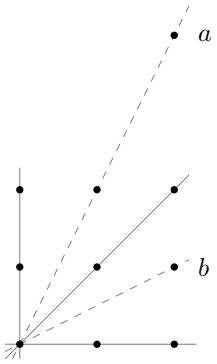
Remarque :
Le nombre de droites éléments de $\mathbb{P}^1(\mathbb{F}_2)$ peut se déterminer graphiquement à partir des droites de $\mathbb{F}_2^2$.



Points de $\mathbb{F}_2^2 \backslash_{\{0\}}$ et droites de $\mathbb{P}^1(\mathbb{F}_2)$.

ii) $GL_2(\mathbb{F}_3) \circlearrowleft \mathbb{P}^1(\mathbb{F}_3)$:
$PGL_2(\mathbb{F}_3) \subset \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_3)} = \mathfrak{S}_4$ et $|PGL_2(\mathbb{F}_3)| = \frac{(3^2-1)(3^2-3)}{3-1} = 24 = |\mathfrak{S}_4|$, on en conclut que $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$.
$PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$ car c'est le seul sous groupe d'indice 2 dans $\mathfrak{S}_4$.

Remarque :
Le nombre de droites éléments de $\mathbb{P}^1(\mathbb{F}_3)$ peut se déterminer graphiquement à partir des droites de $\mathbb{F}_3^2$.



Points de $\mathbb{F}_3^2$ et droites de $\mathbb{P}^1(\mathbb{F}_3)$.
Les droites pointillées en forment une seule car $a = b$ (on rappelle que par deux points passe une droite et une seule !).

iii) Mêmes arguments. Laissé en exercice.

iv) $GL_2(\mathbb{F}_5) \circlearrowleft \mathbb{P}^1(\mathbb{F}_5)$:
$PGL_2(\mathbb{F}_5) \subset \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_5)} = \mathfrak{S}_6$ et $|PGL_2(\mathbb{F}_5)| = \frac{(5^2-1)(5^2-5)}{5-1} = 120$.
Ainsi $[\mathfrak{S}_6 : PGL_2(\mathbb{F}_5)] = 6$, on en conclut que $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ car tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$, (voir Perrin).

Remarque :
On a donc une action de $PGL_2(\mathbb{F}_5) \subset \mathfrak{S}_5$ sur les six droites $\{1,2,3,4,5,6\}$ (donc un plongement de $\mathfrak{S}_5$ dans $\mathfrak{S}_6$) qui ne stabilise aucun élément (ceci est dû à l'existence d'un automorphisme extérieur dans $\mathrm{Aut}(\mathfrak{S}_6)$).

□

Remarque :
On aura aussi remarqué que le groupe linéaire agit sur le groupe projectif de façon générale, ie. pour tout corps $\mathbb{K}$: $GL_{n+1}(\mathbb{K}) \circlearrowleft \mathbb{P}^n(\mathbb{K})$ et c'est même une action transitive (exercice !) de stabilisateur $P_{1,n}(\mathbb{K}) = \begin{bmatrix} \mathbb{K}^* & \mathbb{K} \\ 0 & GL_n(\mathbb{K}) \end{bmatrix}$ un sous-groupe parabolique.
De plus, en vérifiant que ses hypothèses sont bien vérifiées, on a d'après le théorème d'homéomorphisme $\mathbb{P}^n(\mathbb{K}) \cong GL_{n+1}(\mathbb{K})/P_{1,n}(\mathbb{K})$.
Notons au passage que $P_{1,2}(\mathbb{K}) = B_2(\mathbb{K})$ est un groupe de Borel.

Dans le même ordre d'idée, voici un isomorphisme qui en a étonné plus d'un. Pourtant, cette proposition ne fait que remarquer que le "cercle" est "cyclique" (le scoop !). La seconde partie de la preuve est instructive car on y utilise un dessin sur le plan réel pour raisonner sur de la géometrie de corps finis.

Proposition 37 :

En caractéristique différente de 2, on a l'isomorphisme $SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & si\ -1 \in \mathbb{F}_q^{*2} \quad (i.e.\ si\ -1\ est\ un\ carré) \\ \mathbb{Z}/(q+1)\mathbb{Z} & si\ -1 \notin \mathbb{F}_q^{*2} \end{cases}$

Démonstration :
Cas $-1 \in \mathbb{F}_q^{*2}$ Soit $\omega \in \mathbb{F}_q^*$ tel que $-1 = \omega^2$.

$$\begin{aligned} SO_2(\mathbb{F}_q) &= \{A = \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] : \det A = 1,\ {}^tAA = I_2\} \\ &= \{A = \left[\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right] : ad - bc = 1,\ a^2 + b^2 = 1,\ c^2 + d^2 = 1,\ ac + bd = 0\} \end{aligned}$$

Or $ac + bd = 0 \iff \begin{vmatrix} a & -d \\ b & c \end{vmatrix} = 0 \iff \begin{bmatrix} -d \\ c \end{bmatrix} = k \begin{bmatrix} a \\ b \end{bmatrix}$, si par exemple $(a,b) \neq (0,0)$.

Ainsi, $c^2 + d^2 = 1 \iff (kb)^2 + (-ka)^2 = 1 \iff k^2(a^2 + b^2) = 1 \iff k^2 = 1$.
Si $k = 1$ alors $ad - bc = 1 \iff d^2 + c^2 = -1$ absurde en caractéristique différente de 2. Donc $k = -1$.

Donc $SO_2(\mathbb{F}_q) = \{\left[\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right] : a^2 + b^2 = 1\} \simeq S^1(\mathbb{F}_q) := \{(a,b) \in \mathbb{F}_q^2,\ a^2 + b^2 = 1\}$

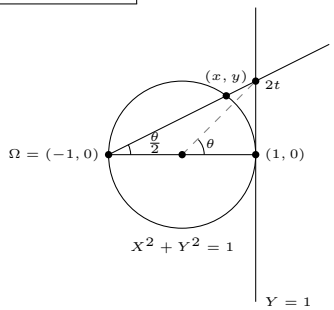
$$\begin{aligned} |SO_2(\mathbb{F}_q)| = |S^1(\mathbb{F}_q)| &= |\{(a,b) \in \mathbb{F}_q^2,\ a^2 + b^2 = 1\}| \\ &= |\{(a,b) \in \mathbb{F}_q^2,\ (a - \omega b)(a + \omega b) = 1\}| \\ &= |\{(x,y) \in \mathbb{F}_q^2,\ xy = 1\}| \end{aligned} .$$

Le morphisme $\psi : \begin{array}{ccc} SO_2(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_q^* \\ \left[\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right] & \longmapsto & a+\omega b \end{array}$ est injectif car si $\psi(A)=1$ alors $a+\omega b = 1$

et puisque $a^2+b^2 = (a+\omega b)(a-\omega b) = 1$ on a $a-\omega b = 1$ et donc, après résolution d'un système, $a=1$ et $b=0$, soit $\operatorname{Ker}\psi = \{I_2\}$.

$SO_2(\mathbb{F}_q)$ s'injecte dans le groupe cyclique $\mathbb{F}_q^*$, il est donc cyclique. Conclusion : $SO_2(\mathbb{F}_q) \simeq {}^{\mathbb{Z}}\!/_{(q-1)\mathbb{Z}}$

Cas $-1 \notin \mathbb{F}_q^{*2}$



$t = \tan(\frac{\theta}{2})$
Si il y a q points sur la droite $Y=1$, la projection stéréographique nous donne une bijection entre le cercle privé du point $(-1,0)$ et la droite.

Notons cette bijection $b : \begin{array}{ccc} \{Y=1\} & \longrightarrow & S^1(\mathbb{F}_q)\backslash_\Omega \\ M & \longmapsto & \Omega M \cap S^1(\mathbb{F}_q) \end{array}$

On obtient une équation (exercice !) de la forme $ax^2+bx+c=0$ avec $a = 1+t^2 \neq 0$ car -1 n'est pas un carré, $x = \dfrac{1-t^2}{1+t^2}$ et $y = \dfrac{2t}{1+t^2}$.

Donc si -1 n'est pas un carré alors b est une bijection et, avec q points sur la droite plus le point "oublié" Ω,

$$|SO_2(\mathbb{F}_q)| = |S^1(\mathbb{F}_q)| = q+1.$$

Le reste est identique sauf que l'on injecte $SO_2(\mathbb{F}_q)$ dans $\mathbb{F}_{q^2}^*$ qui est une extension dans laquelle -1 possède une racine carrée.

□

3 Décomposition cellulaire

On notera $\mathbb{A}^n$ (ou $\mathbb{A}^n(\mathbb{K})$ s'il y a ambiguïté [11]) l'espace affine $\mathbb{K}^n$.

Nous profitons du calcul de cardinalité de l'espace projectif pour introduire la décomposition cellulaire.
La formule $\frac{q^n-1}{q-1} = q^{n-1}+\ldots+1$ suggère que l'espace projectif $\mathbb{P}^{n-1}$ se décompose en union disjointe d'espaces vectoriels. De façon plus naturel, nous allons voir qu'il s'agit en fait d'espaces affines. Pour donner un exemple simple, il arrive fréquemment que l'on scinde en deux l'ensemble des droites vectorielles du plan : celles qui sont de la forme $y=ax$ et la droite "verticale" $x=0$. C'est une illustration de la décomposition cellulaire $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{A}_1 \sqcup \mathbb{A}_0$, ou de la formule $\frac{q^2-1}{q-1} = q^1+1$.
Ces décompositions possèdent un double interêt. D'une part, elles vont permettre de voir que la géométrie projective "prolonge" (il vaut mieux dire "complète") la géométrie affine. D'autre part, sur $\mathbb{R}$ et $\mathbb{C}$, les implications topologiques seront importantes, puisque l'on sera capable de décomposer l'espace topologique complexe (au sens de compliqué) $\mathbb{P}^n$ en union d'espaces topologiques simplicimes (un espace affine est simplement connexe).

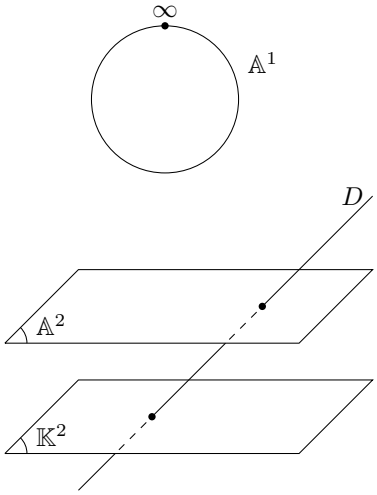
[11] On préferera parfois l'abus de notation $\mathbb{K}^n$.

Proposition 38 :

$$\mathbb{P}^n(\mathbb{K}) \simeq \mathbb{A}^n \sqcup \mathbb{P}^{n-1}(\mathbb{K}) \simeq \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^1 \sqcup \mathbb{A}^0$$

Nous laissons le soin au lecteur de compléter la preuve. En voici l'illustration pour les cas $n = 1$, $n = 2$.

Exemples :
Dans les exemples qui suivent, on réalise $\mathbb{A}_n$ dans $\mathbb{K}^{n+1}$ comme étant l'hyperplan d'équation $z_{n+1} = 1$, où z_{n+1} désigne la dernière coordonnée. L'ensemble $\mathbb{P}^n$ se divise alors en deux parties disjointes, celle des droites coupant A_n, et celle des droites ne le coupant pas, assimilée à l'ensemble des droites de $\mathbb{K}^n$.



$$\begin{aligned}\mathbb{P}^1(\mathbb{K}) = \{\text{droites de } \mathbb{K}^2\} &= \mathbb{A}^1 \sqcup \mathbb{P}^0(\mathbb{K}) \\ &= \{\text{droites coupant } \mathbb{A}^1\} \sqcup \{\text{point à l'infini}\}\end{aligned}$$

$$\begin{aligned}\mathbb{P}^2(\mathbb{K}) = \{\text{droites de } \mathbb{K}^3\} &= \mathbb{A}^2 \sqcup \mathbb{P}^1(\mathbb{K}) \\ &= \{\text{droites coupant } \mathbb{A}^2\} \sqcup \{\text{droites de } \mathbb{K}^2\}\end{aligned}$$

En conclusion, l'espace projectif est l'union disjointe de l'espace affine correspondant et d'un espace projectif de taille inférieure appelé "hyperplan à l'infini". On pourra donc assimiler les droites d'un espace vectoriel à un point d'un espace affine.

Cours d'algèbre, chap. IV, Daniel Perrin, **Ellipses**.
Pour l'espace projectif (sur $\mathbb{R}$) : *Géométrie*, Chap. V, Michèle Audin, **Belin**.
Pour $SO_2(\mathbb{F}_q)$: *Oraux X-ens Algèbre 1*, page 16, Serge Francinou, Hervé Gianella, Serge Nicolas, **Cassini**.

Chapitre VII

Le corps des quaternions

« Je préviens, on a des flingues de concours et la puissance de feu d'un croiseur »

Les Tontons flingueurs, Michel Audiard, 1963.

Introduction

Depuis la maternelle, nous connaissons $\mathbb{N}$ puis est venu $\mathbb{Z}$ inclus dans les corps $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. On sait qu'il n'y a plus de surcorps (commutatif) d'indice fini au-dessus de $\mathbb{C}$. Si on s'autorise au non-commutatif, alors le corps $\mathbb{H}$ des quaternions vient terminer la liste (même s'il existe d'autres corps intermédiaires intéressants comme par exemple la clôture algébrique de $\mathbb{Q}$). On verra que sa construction est très naturelle si on sait construire $\mathbb{C}$ à partir du groupe $SO(2)$ assimilé au cercle S^1 : la construction de $\mathbb{H}$ est analogue en remplaçant $SO(2)$ par $SU(2)$ assimilé à la sphère S^3. Comme applications au corps des quaternions, on montrera qu'ils permettent de réaliser de façon agréable $SU(2)$, reps. $SU(2) \times SU(2)$, comme revêtement universel (bien que cette notion ne soit pas définie dans le cours) de $SO(3)$, resp. $SO(4)$.
Voici la définition qu'a gravé Hamilton sur le Broome Bridge à Dublin.

Définition 23 :
$\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$ *avec* $i^2 = j^2 = k^2 = -1$ *et* $ijk = -1$.

Ce corps n'est pas commutatif : $ij = k \quad jk = i \quad ki = j$
$ji = -k \quad kj = -i \quad ik = -j$

On note $I = i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$ (imaginaires de $\mathbb{H}$, de dimension 3). Si $h = x + yi + zj + tk$, on pose $\bar{h} = x - yi - zj - tk$, et $N(h) = h\bar{h}$, on a les propositions suivantes :

Propositions :
- $h \in \mathbb{R} \Longrightarrow \overline{h} = h$
- $h \in I \Longleftrightarrow h^2 \in \mathbb{R}^- \Longleftrightarrow \overline{h} = -h$
- $N(h) = h\bar{h} = \bar{h}h = x^2 + y^2 + z^2 + t^2$.
- $N(hh') = N(h)N(h')$.

Démonstration :
Laissé en exercice.

□

Remarque :
On fait de la géométrie plane sur $\mathbb{C}$ et de la géométrie en dimension 3 ou 4 sur $\mathbb{H}$.

L'introduction de $\mathbb{H}$ comme nous venons de la faire n'est pas à proprement parler illuminante. Elle fournira, comme toute présentation par générateurs et relations, un moyen pratique de faire des calculs. Mais pour comprendre la construction de $\mathbb{H}$, la raison de ses propriétés particulières (corps non commutatif, norme, conjugaison...), nous allons présenter une construction plus parlante. Avant tout, faisons un petit saut en arrière et rappelons la construction de $\mathbb{C}$. En fait, cela ne fait pas de mal d'en rappeler deux.

1 Construction de $\mathbb{C}$:

Méthode 1 : $\mathbb{C} := \mathbb{R}[X]\diagup_{(X^2+1)}$

En effet, toute classe de polynôme de $\mathbb{R}[X]$ non multiple de X^2+1, donc premier avec X^2+1, possède un inverse d'après Bezout :
$\forall P \in \mathbb{R}[X] \quad \exists U, V \in \mathbb{R}[X]$ tels que $UP + V(X^2+1) = 1$
En quotientant, on obtient $\overline{U}\,\overline{P} = \overline{1}$.
Ceci signifie que tout élément non nul de $\mathbb{R}[X]/(X^2+1)$ est inversible et donc que l'anneau est un corps.
Selon un procédé général dans le cadre des extensions galoisiennes, le corps des complexes ainsi obtenu est bien muni de l'automorphisme $\bar{}: z \longmapsto \overline{z}$
et de la norme multiplicative $N(z) = z\overline{z}$.

Méthode 2 : $\mathbb{C}^* \cong \mathbb{R}^{+*} \times SO(2)$

$\mathbb{C}$ est le cône engendré par $SO(2) = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a^2+b^2 = 1 : a, b \in \mathbb{R} \right\} \simeq S^1$

Remarque :
Ce cône est aussi un espace vectoriel, ce qui est n'est pas habituel.

De plus, le fait que $SO(2)$ est un groupe abélien confère une structure de groupe à $\mathbb{C}^* \cong \mathbb{R}^{+*} \times SO(2)$.

On identifie de cette manière un nombre complexe $z = x + iy$

à une matrice $Z = 1x + iy = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$ avec $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ et $i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

L'espace des complexes muni de cette multiplication constitue bien un corps et ce corps ainsi obtenu est muni de l'automorphisme (on rappelle que la multiplication est commutative) $\bar{}: Z \longmapsto {}^tZ$
(transposée) et de la norme multiplicative $N(Z) = \det Z$.

2 Construction de $\mathbb{H}$:

C'est la méthode 2 qui va primer pour construire $\mathbb{H}$:
$\mathbb{H}$ est le corps des "cumplexes", dans le sens qu'il suffit de remplacer un O par un U, et donc le groupe abélien $SO(2)$ par $SU(2)$, non-abélien.

Pas cun le mec !

On définit $\mathbb{H}^* \simeq \mathbb{R}^{+*} \times SU(2)$ comme produit direct de groupes, avec :

$$SU(2) = \Big\{ \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix} \,:\, |a|^2 + |b|^2 = 1 \,:\, a, b \in \mathbb{C} \Big\},$$

$$\text{Ainsi} \quad \mathbb{H} = \Big\{ \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix} \,:\, a, b \in \mathbb{C} \Big\}.$$

Forme $\mathbb{C}$-matricielle : avec $a = x + iy, \quad b = -z + it \qquad x, y, z, t \in \mathbb{R}$

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

On note $h = 1x + Iy + Jz + Kt = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}$ les éléments de $\mathbb{H}$.

Le corps des quaternions ainsi obtenu est muni de l'antiautomorphisme $^- : h \longmapsto h^*$ (adjoint) et de la norme multiplicative $N(h) = h\overline{h} = \overline{h}h = |a|^2 + |b|^2 = \det h$.

Forme $\mathbb{R}$-matricielle : La forme (on dit plutôt représentation) $\mathbb{C}$-matricielle de $\mathbb{H}$, jointe à la représentation $\mathbb{R}$-matricielle de $\mathbb{C}$ fournit une représentation $\mathbb{R}$-matricielle de $\mathbb{H}$. $\qquad x, y, z, t \in \mathbb{R}$

$$1 = \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 0 & -1 & & \\ 1 & 0 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} & & -1 & 0 \\ & & 0 & -1 \\ 1 & 0 & & \\ 0 & 1 & & \end{bmatrix}, \quad K = \begin{bmatrix} & & 0 & -1 \\ & & 1 & 0 \\ 0 & -1 & & \\ 1 & 0 & & \end{bmatrix}$$

$$h = 1x + Iy + Jz + Kt = \left[\begin{array}{cc|cc} x & -y & -z & -t \\ y & x & t & -z \\ \hline z & -t & x & y \\ t & z & -y & x \end{array}\right] = \begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix} \qquad \text{avec } a = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \text{ et } b = \begin{bmatrix} z & -t \\ t & z \end{bmatrix}$$

Forme Cartésienne : Pour finir, voici la forme cartésienne, toujours très rassurante, mais pas toujours très adaptée.

$$h = x + iy + jz + kt \qquad x, y, z, t \in \mathbb{R}$$

$\bar{h} = x - iy - jz - kt$
$h\bar{h} = x^2 + y^2 + z^2 + t^2 = N(h)$

3 L'ours mal peigné

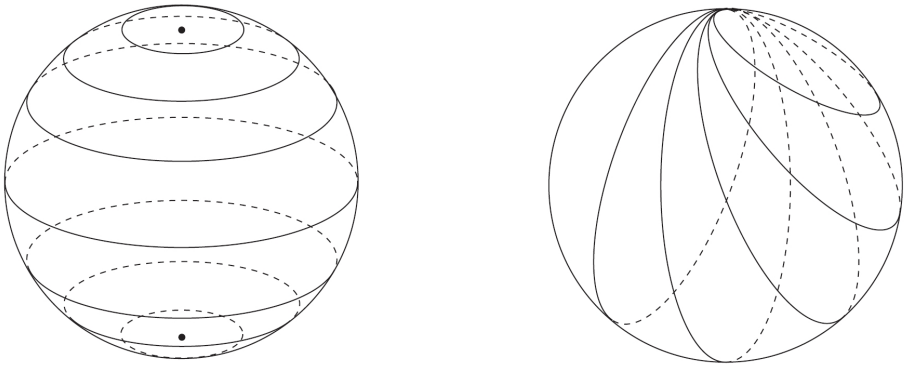
Voici un interlude qui semble à première vue plus proche de la cosmétologie appliquée que du corps des quaternions. On verra que la question qui suit aboutit à la représentation matricielle que l'on vient de rencontrer.

Peut-on peigner un ours dans un espace de dimension n quelconque sans épi ?

Bien entendu, l'ours doit être vu comme une sphère de dimension $n-1$. Une réponse complète est donnée par le théorème d'Adams. On peut se souvenir que dans notre espace à trois dimension, c'est impossible, et plus généralement dans tout espace de dimension impaire.
De plus, il existe $n-1$ façons indépendantes seulement en dimensions 2, 4 et 8.

Dans $\mathbb{C}$: Topologiquement, la fourrure d'un ours de dimension 2 est la sphère (cercle) S^1.
Il est possible d'associer au cercle un champ de vecteurs tangents uniforme, l'ours est alors bien peigné :
On prend pour chaque vecteur non nul $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ le vecteur tangent $\left[\begin{smallmatrix} -y \\ x \end{smallmatrix}\right]$ qui ne s'annule pas.
Y en a-t-il qui me voient venir ? Un vecteur muni du choix particulier (section de fibré) de vecteur tangent fournit une matrice $\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$ qui est exactement celle de la représentation réelle des complexes.

Dans $\mathbb{R}^3$: Topologiquement, la fourrure d'un ours de dimension 3 est la sphère S^2.
Il est impossible de lui associer un champ de vecteurs tangent uniformes sans créer un pôle nul, l'ours a alors au moins un épi. D'ailleurs, si c'est un drame pour le plantigrade, c'est un bonheur pour le mathématicien, puisqu'on montre grâce à cela que $\mathbb{C}$ est algébriquement clos.



Deux champs de vecteurs tangent avec respectivement deux pôles et un pôle.

Remarque :
Une projection stéréographique centrée sur l'unique pôle de la seconde sphère, permettrait de retrouver toutes les droites du plan d'une direction donnée.

Dans $\mathbb{H}$: Topologiquement, la fourrure d'un ours de dimension 4 est l'hypersphère S^3.
Il est possible de lui associer de trois manières différentes un champ de vecteurs tangents uniforme, l'ours est alors bien peigné :
On prend pour chaque vecteur non nul $\begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix}$ le vecteur tangent $\begin{bmatrix} -y \\ x \\ -t \\ z \end{bmatrix}$ ou $\begin{bmatrix} -z \\ t \\ x \\ -y \end{bmatrix}$ ou $\begin{bmatrix} -t \\ -z \\ y \\ x \end{bmatrix}$ qui ne s'annulent pas.

Supplément : Le cas $n = 8$ du théorème d'Adams peut être réalisé dans l'espace de dimension 8 des octonions, terme inspirateur de jeux de mots divers, mais qui force le respect quand on le sait muni d'une multiplication non commutative et non associative...

4 Applications à $SO(3)$

On va voir que si $\mathbb{C}$ est un bon objet pour faire de la géométrie plane, $\mathbb{H}$ en est également un pour faire de la géométrie en dimension 3. Il s'agissait là en fait du but de son auteur Hamilton, qui s'est fourvoyé des années à chercher un corps de dimension trois sur $\mathbb{R}$, que nul n'a jamais trouvé, encouragé par son enfant qui lui demandait quotidiennement "Daddy, can you multiply triplets ?"[12]. La norme $N(h) = h\bar{h}$ est une forme quadratique réelle sur $\mathbb{H}$, de forme bilinéaire symétrique associée

$$\varphi(h, h') = \frac{1}{2}(h\bar{h}' + h'\bar{h}).$$

(Montrez le sans calcul à l'aide de l'unicité de la forme bilinéaire symétrique associée).
Notons que I est l'orthogonal de $\mathbb{R}$ et que $SU(2) = S^3$ agit sur $\mathbb{H}$ par automorphisme :

$$\begin{array}{rccccc} \phi: & SU(2) & \longrightarrow & \mathrm{Aut}(\mathbb{H}) & & \\ & h & \longmapsto & \phi_h: & \mathbb{H} \longrightarrow \mathbb{H} \\ & & & & u \longmapsto huh^{-1} \end{array}$$

ϕ_h est linéaire et respecte la norme de $\mathbb{H}$ car $N(huh^{-1}) = N(u)$. Comme l'action de $SU(2)$ respecte $\mathbb{R}$, elle respecte son orthogonal I. Considérons donc :

$$\begin{array}{rccccc} \phi: & SU(2) & \longrightarrow & \mathrm{Aut}(I) & & \\ & h & \longmapsto & \phi_h: & I \longrightarrow I \\ & & & & u \longmapsto huh^{-1} \end{array} .$$

Conclusion : $\phi\big(SU(2)\big) \subset O(3)$.

Par continuité (on n'utilise que des additions, des multiplications et des inverses non nuls), on a même que $\phi\big(SU(2)\big)$ est connexe et contient l'identité, donc $\phi\big(SU(2)\big) \subset SO(3)$.

Finalement, on a que $\phi : SU(2) \longrightarrow SO(3)$. Montrons qu'elle est surjective.

Rappel :

- Les générateurs de $O(n)$ sont les réflexions orthogonales, de matrices similaires à $\begin{bmatrix} I_{n-1} & \\ & -1 \end{bmatrix}$ dans une base orthonormée.
- Les générateurs de $SO(n)$ sont les retournements (demi-tours), de matrices similaires à $\begin{bmatrix} I_{n-2} & \\ & -I_2 \end{bmatrix}$ dans une base orthonormée.

Il suffit de montrer que tous les retournements de $SO(3)$ sont dans $\phi\big(SU(2)\big)$.
Soit r_h, $\quad h \in I \cap S^3 \quad$ le retournement d'axe $\mathbb{R}h$, i.e. $mat(r_h) = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}$ dans une base orthonormée.
Il faut alors montrer que $r_h = \phi_h$. Pour cela, il suffit de montrer que $\phi_h(h) = h \quad (1)$
et $\phi_h(h') = -h'$ si $h' \perp h \quad (2)$.

[12] It's a true story.

(1) est clair, $\phi_{_h}(h) = hhh^{-1} = h$.

(2) $h' \perp h$ donc $\frac{1}{2}(h'\bar{h} + h\bar{h}') = 0 \quad \Longrightarrow h'(-h) + h(-h') = 0$
$\Longrightarrow h'h = -hh'$
$\Longleftrightarrow hh'h^{-1} = -h'$

Donc $\phi : SU(2) \longrightarrow\!\!\!\!\!\rightarrow SO(3)$ surjective.

De plus, $Ker\,\phi = \{\pm 1\}$, d'où l'isomorphisme par passage au quotient :

$$\overline{\phi} : SU(2)\diagup_{\{\pm 1\}} \simeq SO(3).$$

Et de la même mainère avec abus de notation : De plus, $Ker\,\phi = \{\pm 1\}$, d'où l'isomorphisme par passage au quotient :

$$\overline{\phi} : \mathbb{H}\diagup_{\mathbb{R}^*} \simeq SO(3).$$

Remarques :

- On a en prime une interprétation topologique : $SO(3)$ est homéomorphe à $\mathbb{P}^3(\mathbb{R})$.
- Application en calcul formel, dans les logiciels de simulation de vol où les calculs de rotations sont effectués dans $\mathbb{H}$ plutôt que dans $SO(3)$ directement.

$$\{\pm 1\} \longrightarrow SU(2) \longrightarrow SO(3)$$

- En supplément pour ceux qui ont quelques bases de topologie algébrique :
  Comme $SU(2)$ est la sphère S^3, donc simplement connexe, et comme $\{1, -1\}$ est discret, cela prouve que $SU(2)$ est le revêtement universel de $SO(3)$ et donc que le groupe fondamental de $SO(3)$ est $\{1, -1\}$.
  En application, on a le fameux principe de l'assiette à soupe : si on pose sur sa main une assiette et que l'on fait faire à son bras deux rotations de 360^o dans le même sens en maintenant l'assiette horizontale, le bras ne se tord pas deux fois, mais revient à sa position initiale. En aucun cas, la direction n'est responsable d'accidents survenus en expérimentant ce beau théorème de topologie.

5 Fibration de Hopf

On considère la sphère S^2, resp. S^3, que l'on réalise comme la sphère unité dans I, resp. $\mathbb{H}$. Encore une fois, le groupe $SU(2)$ est vu comme la sphère S^3 de $\mathbb{H}$. Considérons l'action

$$\begin{array}{ccc} SU(2)\times S^2 & \longrightarrow & S^2 \\ (h,z) & \longmapsto & hz \end{array}$$

On voit facilement que SU(2) agit transitivement sur la sphère, puisque son action est celle de $SO(3)$ d'après ce qui précède.
De plus, un calcul simple montre que le stabilisateur de $i \in S^2$ est le groupe $\{h = x + yi,\ x^2 + y^2 = 1\}$, c'est à dire le cercle S^1. Ce qui veut dire, par le théorème d'homéomorphisme que

$$S^3 \diagup S^1 \simeq S^2,$$

très utile quand on veut comprendre la topologie de S^3. Cela s'appelle la fibration de Hopf, pour en savoir plus sur ce qu'est une fibration, vous pouvez consulter le [Mneimné-Testard].

6 Applications à $SO(4)$

Nous allons voir qu'avec un tout petit effort supplémentaire, nous allons aussi réaliser $SO(4)$. Bien sûr, cette fois-ci, $SU(2)$ tout seul, trop petit, ne va pas suffire, on va considérer l'action $SU(2)\times SU(2) \circlearrowleft \mathbb{H}$ par automorphisme :

$$\begin{array}{rccccl} \psi: & SU(2)\times SU(2) & \longrightarrow & \mathrm{Aut}(\mathbb{H}) & & \\ & (h,k) & \longmapsto & \psi_{h,k}: & I \longrightarrow I & \\ & & & & u \longmapsto huk^{-1} & \end{array}$$

Comme précédemment, il vient $\quad \psi\big(SU(2)\times SU(2)\big) \subset SO(4)$.

Montrons qu'elle est surjective.
Soit P un plan quelconque de $\mathbb{H}$, on veut montrer que le retournement par rapport à P est dans l'image de ψ. Pour cela, choisissons une base orthonormée (p,q) de P.
Cela implique donc $\overline{p^{-1}q} = \overline{q}\,\overline{p^{-1}} = \overline{q}\,p = -\overline{p}\,q = -p^{-1}q$. Conclusion, $v := p^{-1}q \in I$.
D'après la section sur $SO(3)$, cela implique que $\psi_{v,v}$ est un retournement, et donc que son conjugué $\psi_{p,1}\psi_{v,v}\psi_{p^{-1},1} = \psi_{pvp^{-1},v}$ est aussi un retournement.
De plus, on vérifie facilement que $\psi_{pvp^{-1},v}(p) = p$ et $\psi_{pvp^{-1},v}(q) = q$. C'est donc bien le retournement cherché.
On voit facilement que le noyau de ψ est $\{(1,1),(-1,-1)\}$.

On a donc l'**isomorphisme exceptionnel**

$$\phi : SU(2)\times SU(2) \diagup_{\{(1,1),(-1,-1)\}} \simeq SO(4).$$

Cela implique que l'on a un isomorphisme $PSO(4) \simeq SU(2)\times SU(2) \diagup_{\{(1,1),(1,-1),(-1,1),(-1,-1)\}}$
lui-même isomorphe à $SU(2) \diagup_{\{1,-1\}} \times SU(2) \diagup_{\{1,-1\}}$.
Et finalement, on obtient l'**isomorphisme exceptionnel**

$$PSO(4) \simeq SO(3)\times SO(3).$$

Topologiquement, c'est remarquable. Il convient de fêter dignement l'évènement en tenant deux assiettes à soupe, une dans chaque main, en hommage au groupe fondamental de PSO(4).
Algébriquement, c'est une tragédie. Contrairement à tous ses copains ($PSO(n)$, $n \geq 3$), $PSO(4)$ n'est pas simple. Il possède des sous-groupes distingués non triviaux.

Question :
A quoi sert la simplicité au fait ?

Dans la pratique, un morphisme non trivial d'un groupe simple vers un autre est injectif. Bien sûr, puisque son noyau est distingué.

Question :
Quels sont les groupes simples qu'on connait à l'agrégation ?

Le groupe alterné $\mathfrak{A}_n$ pour $n \geq 5$, $\quad PSL_n(\mathbb{K})$ pour $(n, \mathbb{K}) \neq (2, \mathbb{F}_2), (2, \mathbb{F}_3)$ $\quad$ et $PSO(n)$ pour $n \geq 3$, $n \neq 4$.

Cours d'algèbre, Chap. VII, Daniel Perrin, **Ellipses**.
Algèbre linéaire, Rémi Goblot, **Ellipses**.
Pour $SU(2) \to SO(3)$ et la fibration de Hopf, sans utiliser les quaternions, on pourra consulter :
Introduction à la théorie des groupes classiques, Chap. 4, Rached Mneimné, Frédéric Testard, **Hermann**.

Chapitre VIII

Groupes de Lie classiques et isomorphismes exceptionnels

« I didn't say it would be easy, Neo. I just said it would be the truth. »

Matrix, Andy & Larry Wachowski, 1999.

A ce stade du cours, l'utilité de mettre une structure topologique sur un groupe devrait être bien comprise. Maintenant, nous allons ajouter une structure de variété différentielle. A fin d'illustrer l'apport de cette structure, regardons l'exemple de l'isomorphisme $SU(2)/_{\{1,-1\}} \simeq SO(3)$ prouvé dans le chapitre sur les quaternions. On a construit cet isomorphisme à partir du morphisme $SU(2) \to O(3)$ fourni par l'action de congugaison dans les quaternions.
Puis, des considérations topologiques nous amènent à un morphisme $\phi : SU(2) \to SO(3)$. Mais sa surjectivité a été montrée par une méthode ad hoc. Une méthode plus simple et plus générale est de montrer que $\mathrm{Im}\,\phi$ contient un voisinage ouvert de l'identité, ce qui assure bien la surjectivité par connexité de $SO(3)$. Il se trouve que mettre une structure de variété différentielle sur les groupes $SU(2)$ et $SO(3)$ permet justement de vérifier l'existence d'un tel voisinage, via un théorème d'inversion locale. Nous avons mis en appendice quelques résultats admis de calcul différentiel qui seront utilisés dans cette leçon.

1 Groupes de Lie classiques

Définition 24 :
On appelle groupe de Lie un groupe topologique muni d'une structure de sous-variété de $\mathbb{R}^n$ telle que la multiplication et l'inversion soient $\mathcal{C}^1$.

retour p15

Le fameux théorème de Cartan assure que tout sous-groupe fermé de $GL_n(\mathbb{K})$ est un groupe de Lie, mais il est plus sportif de montrer sans le théorème que les sous-groupes étudiés dans les exemples qui suivent vérifient bien les hypothèses. L'utilisation du théorème de submersion est alors essentielle.

Proposition 39 :
$GL_n(\mathbb{R})$ est une sous-variété de $\mathbb{R}^{n^2} \simeq M_n(\mathbb{R})$. C'est un groupe de Lie.

Démonstration :
$GL_n(\mathbb{R})$ étant un ouvert de l'espace $M_n(\mathbb{R})$, il est clairement localement difféomorphe à $\mathbb{R}^{n^2}$ (tous les ouverts d'une variété sont des sous-variétés)...

□

Proposition 40 :
Son espace tangent est $T_e(GL_n(\mathbb{R})) = M_n(\mathbb{R})$.

Démonstration :
$\forall X \in M_n(\mathbb{R}), \quad \exists f : \mathbb{R} \longrightarrow GL_n(\mathbb{R})$ courbe de classe $\mathcal{C}^1$ telle que $f(0) = I_n$ et $f'(0) = X$.
Par exemple, $f(t) = \exp(tX)$.

□

Notons que l'utilisation de l'exponentielle dans cette preuve n'est absolument pas nécessaire, mais elle est instructive.
Avant d'aller plus loin, faisons quelques echauffements avec des exemples de calculs de différentielles :

i) $\begin{array}{rccc} f: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & A & \longmapsto & 2A \end{array}$ linéaire $\Longrightarrow$ $\begin{array}{rccc} df_0: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & 2H \end{array}$

ii) $\begin{array}{rccc} f: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & A & \longmapsto & A^2 \end{array}$

On calcule $f(I+H) = (I+H)^2 = I+2H+H^2$ et df_I correspond à la partie linéaire : $\begin{array}{rccc} df_I: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & 2H \end{array}$

Pour obtenir df_A, on prend la partie linéaire de $f(A+H)$,
soit $(A+H)^2 = A+AH+HA+H^2$, qui nous donne $\begin{array}{rccc} df_A: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & AH+HA \end{array}$

iii) $\begin{array}{rccc} f: & GL_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ & A & \longmapsto & A^{-1} \end{array}$

$(I+H)^{-1} = I - H + H^2 - H^3 + \ldots \Longrightarrow$ $\begin{array}{rccc} df_I: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & -H \end{array}$

$(A+H)^{-1} = [A(I+A^{-1}H)]^{-1} = (I+A^{-1}H)^{-1}A^{-1} = A^{-1}-A^{-1}HA^{-1}+\ldots \Longrightarrow$ $\begin{array}{rccc} df_A: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & -A^{-1}HA^{-1} \end{array}$

iv) $\begin{array}{rccc} f: & M_n(\mathbb{R}) & \longrightarrow & \mathrm{End}(M_n(\mathbb{R})) \\ & A & \longmapsto & f_A : X \longrightarrow AX \end{array}$ linéaire donc $\begin{array}{rccc} df_I: & M_n(\mathbb{R}) & \longrightarrow & \mathrm{End}(M_n(\mathbb{R})) \\ & H & \longmapsto & f_H : X \longrightarrow HX \end{array}$

v) $\begin{array}{rccc} f: & GL_n(\mathbb{R}) & \longrightarrow & \mathrm{Aut}(M_n(\mathbb{R})) \\ & A & \longmapsto & f_A : X \longrightarrow AXA^{-1} \end{array}$ (non-linéaire)

$(I+H)X(I+H)^{-1} = I + HX - XH + \ldots \Longrightarrow$ $\begin{array}{rccc} df_I: & M_n(\mathbb{R}) & \longrightarrow & M_n(\mathbb{R}) \\ & H & \longmapsto & HX - XH \end{array}$

Proposition 41 :
$O_n(\mathbb{R})$ est une sous-variété de $\mathbb{R}^{n^2}$.

Démonstration :
Soit $f : \begin{array}{ccc} M_n(\mathbb{R}) & \longrightarrow & \mathcal{S}_n(\mathbb{R}) \\ M & \longmapsto & {}^tMM \end{array}$
On sait que $O_n(\mathbb{R}) = f^{-1}(I_n)$. Soit $A \in O_n(\mathbb{R})$.

$$ {}^t(A+H)(A+H) = {}^tAA + {}^tAH + {}^tHA + \cdots $$

d'où $df_A : \begin{array}{ccc} M_n(\mathbb{R}) & \longrightarrow & \mathcal{S}_n(\mathbb{R}) \\ H & \longmapsto & {}^tAH + {}^tHA \end{array}$

Soit $S \in \mathcal{S}_n(\mathbb{R})$ et posons $H = \frac{AS}{2}$. Alors ${}^tAH + {}^tHA = {}^tA\frac{AS}{2} + \frac{S\,{}^tA}{2}A = \frac{S}{2} + \frac{S}{2} = S$

Donc df_A est surjective. D'après le théorème de submersion, $O_n(\mathbb{R})$ est une sous-variété de $M_n(\mathbb{R})$ de dimension

$$\dim M_n(\mathbb{R}) - \dim \mathcal{S}_n(\mathbb{R}) = n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2} \text{ et } \begin{array}{ll} T_I(O_n(\mathbb{R})) & = \mathrm{Ker}(df_I) \\ & = \{H \in M_n(\mathbb{R}) \ : \ H + {}^tH = 0\} \\ & = \mathcal{A}_n(\mathbb{R}) \end{array}$$

□

On notera par la lettre gothique $\mathfrak{g}$ correspondante l'espace tangent $T_e(G)$ en l'identité. Par exemple, on note $\mathfrak{o}_n(\mathbb{R}) := T_e(O_n(\mathbb{R}))$.

Exercice :
Vérifier que $\mathfrak{o}(p,q) = \{H \in M_n(\mathbb{R}) \ : \ {}^tHI_{p,q} + I_{p,q}H = 0\}$
$\mathfrak{u}(n) = \{H \in M_n(\mathbb{R}) \ : \ H^* + H = 0\} = \mathcal{A}H_n(\mathbb{R})$ (espace vectoriel des matrices anti-hermitiennes)
$\mathfrak{su}(p,q) = \{H \in M_n(\mathbb{R}) \ : \ H^* + H = 0, \ \mathrm{Tr}(H) = 0\}$

Proposition 42 :
$SL_n := SL_n(\mathbb{R})$ est une sous-variété de $\mathbb{R}^{n^2}$ et $\mathfrak{sl}_n = \{M \in M_n(\mathbb{R}), Tr(M) = 0\}$.

Démonstration :
$SL_n(\mathbb{R}) = \det^{-1}(\{1\})$ avec $f := \det : M_n(\mathbb{R}) \longrightarrow \mathbb{R}$. Soit $A \in SL_n(\mathbb{R})$. Alors $df_A : M_n(\mathbb{R}) \longrightarrow \mathbb{R}$.
Notons $(A_i)_{1\leq i\leq n}$ les colonnes de A et $(H_i)_{1\leq i\leq n}$ les colonnes de H.
Si on note $\det A = A_1 \wedge A_2 \wedge \cdots \wedge A_n$, alors $f(A+H) = \det(A+H) = (A_1+H_1) \wedge (A_2+H_2) \wedge \cdots \wedge (A_n+H_n)$, d'où par multilinéarité et antisymétrie on a la partie linéaire

$$df_A(H) = H_1 \wedge A_2 \wedge \cdots \wedge A_n + A_1 \wedge H_2 \wedge A_3 \wedge \cdots \wedge A_n + \cdots + A_1 \wedge \cdots \wedge A_{n-1} \wedge H_n$$

Si on développe le déterminant $A_1 \wedge \cdots \wedge H_i \wedge \cdots \wedge A_n$ par rapport à la i-ième colonne,
en notant ${}^t\,\mathrm{com}(A) = \tilde{A} = (m_{ij})_{\substack{1\leq i\leq n \\ 1\leq j\leq n}}$, il vient $df_A(H) = \sum_{\substack{1\leq i\leq n \\ 1\leq j\leq n}} h_{ij}m_{ji} = \mathrm{Tr}(\tilde{A}H)$
Comme $A \in SL_n(\mathbb{R})$ est inversible, $\tilde{A} = A^{-1} \neq 0$ et donc, on voit facilement que $df_A \neq 0$ (et donc surjective car c'est une forme linéaire).
D'où par le théorème de submersion, $SL_n(\mathbb{R})$ est une sous-variété de $\mathbb{R}^{n^2}$ de dimension $n^2 - 1$ et de plus

$$\mathfrak{sl}_n(\mathbb{R}) = \{H \in M_n(\mathbb{R}) \ : \ \mathrm{Tr}(H) = 0\}$$

□

2 Applications aux isomorphismes exceptionnels

On va voir que le formalisme des groupes de Lie est efficace pour montrer la surjectivité dans les isomorphismes qui suivent.

Proposition 43 :
$PSL_2(\mathbb{C}) \simeq SO_3(\mathbb{C})$.

Démonstration :
$SL_2(\mathbb{C})$ agit sur $\mathfrak{sl}_2(\mathbb{C})$ par conjugaison $\begin{array}{rccc} \phi : & SL_2(\mathbb{C}) & \longrightarrow & \mathrm{Aut}(\mathfrak{sl}_2(\mathbb{C})) \\ & A & \longmapsto & \phi_A : X \longmapsto AXA^{-1} \end{array}$
C'est bien une action car $\mathrm{Tr}(AXA^{-1}) = \mathrm{Tr}(X) = 0$. On a $\dim \mathfrak{sl}_2(\mathbb{C}) = 3$, car $\mathfrak{sl}_2(\mathbb{C})$ est un hyperplan de $M_2(\mathbb{C})$.
Puisque ϕ_A est bien linéaire et bien sûr bijective, $\phi(SL_2(\mathbb{C})) \subset GL_3(\mathbb{C})$.
Mais plus précisément, puisque $\det(\phi_A(X)) = \det(X)$, on a même $\phi(SL_2(\mathbb{C})) \subset O(\det)$, le groupe orthogonal de la forme déterminante (qui est bien une forme quadratique en dimension 2).

Soit $A \in SL_2(\mathbb{C})$. Alors on peut l'écrire $A = \left[\begin{smallmatrix} a & c \\ b & -a \end{smallmatrix}\right]$ avec $a, b, c \in \mathbb{C}$ et comme les formes quadratiques sur $\mathbb{C}$ sont classifiées par le rang, on calcule $\det(A) = -a^2 - bc = -a^2 - \frac{1}{4}(b+c)^2 + \frac{1}{4}(b-c)^2$.
Ces formes sont linéairement indépendantes donc la forme quadratique est non-dégénérée, et de rang (maximal) 3.
Ainsi $\phi(SL_2(\mathbb{C})) \subset O_3(\mathbb{C})$. Puisque ϕ est continue et $SL_2(\mathbb{C})$ est connexe, $\phi(SL_2(\mathbb{C}))$ est aussi connexe dans $O_3(\mathbb{C})$ tout en contenant l'identité, et donc $\phi(SL_2(\mathbb{C})) \subset SO_3(\mathbb{C})$.
Montrons l'inclusion inverse. Composée de fractions rationnelles, ϕ est différentiable :

$$\begin{array}{rccc} d\phi_I : & \mathfrak{sl}_2(\mathbb{C}) & \longrightarrow & \mathfrak{so}_3(\mathbb{C}) \\ & H & \longmapsto & d\phi_I(H) : X \longmapsto HX - XH \end{array}$$

On a $\mathfrak{so}_3(\mathbb{C}) = \mathfrak{o}_3(\mathbb{C})$ (exercice !).
De plus, $d\phi_I$ est injective car
$$\begin{aligned} \mathrm{Ker}\, d\phi_I &= \{H \in \mathfrak{sl}_2(\mathbb{C}) \ : \ \forall X,\, HX - XH = 0\} \\ &= \{H,\, Tr(H) = 0, H = \lambda I_2\} \\ &= \{0\} \end{aligned}$$
Comme $\dim \mathfrak{sl}_2(\mathbb{C}) = \dim \mathfrak{so}_3(\mathbb{C}) = 3$, on conclut que $d\phi_I$ est un isomorphisme. Ainsi d'après le théorème d'inversion locale ϕ est un homéomorphisme local et donc $\phi(SL_2(\mathbb{C}))$ contient un ouvert. Le sous-groupe $\phi(SL_2(\mathbb{C}))$ est ouvert par principe de translation, et ainsi forcément fermé également.
A la fois ouvert et fermé connexe, non trivial dans $SO_3(\mathbb{C})$ connexe, on a donc finalement $\phi(SL_2(\mathbb{C})) = SO_3(\mathbb{C})$.
Puisque $\mathrm{Ker}\, \phi = \mathbb{K}^* I_n$ (les homothéties), on peut conclure que $PSL_2(\mathbb{C}) \simeq SO_3(\mathbb{C})$.

□

Exercice :
Montrer que $PSL_2(\mathbb{R}) \simeq SO_0(2,1)$ par l'action de $SL_2(\mathbb{R})$ sur $\mathfrak{sl}_2(\mathbb{R})$ par conjugaison.
Montrer que $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$ par l'action de $SU_2(\mathbb{C})$ sur l'espace (réel) des matrices hermitiennes de trace nulle $H_2(\mathbb{C}) \cap \mathfrak{sl}_2(\mathbb{C}) = \{H \in M_2(\mathbb{C}) \ : \ H^* = H,\ \mathrm{Tr}(H) = 0\}$ par congruence hermitienne.

Proposition 44 :
$PSL_2(\mathbb{C}) \simeq SO_0(3,1)$.

retour p102

Démonstration :
Identique à la précédente démo. $SL_2(\mathbb{C})$ agit sur $H_2(\mathbb{C})$ (qui est un espace réel, et non pas complexe !) par congruence hermitienne :

$$\begin{array}{rccc} \phi : & SL_2(\mathbb{C}) & \longrightarrow & \mathrm{End}(H_2(\mathbb{C})) \\ & A & \longmapsto & \phi_A : X \longmapsto AXA^* \end{array} .$$

Pour faire cette preuve vous-même en quelques étapes, voici la méthode à suivre :

1. Vérifier que c'est bien une action,
2. Montrer que ϕ stabilise le déterminant,
3. Calculer sa signature, i.e. celle de $\begin{vmatrix} a & b-ic \\ b+ic & d \end{vmatrix} = ad - (b^2+c^2)$. On doit trouver $(1,3)$. Bien sûr si l'on prend $-\det$ on trouve $(3,1)$ ce qui revient au même par congruence,
4. Montrer que $\phi(SL_2(\mathbb{C})) \subset SO_0(3,1)$ par un argument topologique,
5. Montrer que $\begin{array}{rccc} d\phi_I : & \mathfrak{sl}_2(\mathbb{C}) & \longrightarrow & \mathfrak{so}_0(3,1) \\ & H & \longmapsto & d\phi_I(H) : X \longmapsto HX - XH^* \end{array}$
6. Montrer qu'elle est injective ($\mathrm{Ker} = 0$),
7. Montrer qu'elle est surjective ($\dim \mathfrak{sl}_2(\mathbb{C}) = \dim \mathfrak{so}_0(3,1)$),
8. Enfin, conclure en utilisant le théorème d'inversion locale et les propriétés des groupes topologiques. □

3 Notion d'algèbre de Lie

Cette notion est hors-programme parce qu'il faut bien faire des choix et que l'esprit de l'oral d'agrégation est prioritaire dans ce cours. Toutefois, j'engage vivement la lecture de ce passage. Elle apporte un éclairage sur ce qui fait l'efficacité de la théorie des groupes de Lie : la linéarisation des problèmes sur le groupe G en considérant son espace tangent $\mathfrak{g}$ en l'identité, espace sur lequel on rajoute une structure d'algèbre non-associative appelée structure d'algèbre de Lie. L'algèbre de Lie $\mathfrak{g}$ devient un recueil d'informations sur le groupe G. Recueil illustré par le "dictionnaire Algèbre de Lie-Groupe de Lie" que l'on trouvera en fin de section et qui utilise le célèbre théorème de Cartan qui assure que l'exponentielle permet de retrouver G à partir de $\mathfrak{g}$.

Définition 25 :
Un $\mathbb{K}$-espace vectoriel est une algèbre de Lie si on peut le munir d'une application bilinéaire (crochet de Lie) :

$$(x,y) \longmapsto [x,y]$$

telle que (antisymétrie) $[x,y] = -[y,x]$ *et (identité de Jacobi)* $\sum_{cycles} [[x,y],z] = [[x,y],z] + [[z,x],y] + [[y,z],x] = 0$

Remarque :
L'algèbre $M_n(\mathbb{K})$, et plus généralement toute algèbre associative, définit une algèbre de Lie pour le commutateur $[A,B] = AB - BA$.

Le commutateur d'une algèbre est $[A,B] = AB - BA$,
mais celui d'un groupe est $[A,B] = ABA^{-1}B^{-1}$.

Proposition 45 :
Soit G un sous-groupe de Lie de $GL_n(\mathbb{K})$ ($\mathbb{K}$ réel ou complexe). Alors, $\mathrm{Lie}\, G = \mathfrak{g} := T_e(G) \subset M_n(\mathbb{K})$ *possède une structure de sous-algèbre de Lie de $M_n(\mathbb{K})$. Dit autrement :*

$$\forall X, Y \in \mathfrak{g}, \quad [X, Y] = XY - YX \in \mathfrak{g}.$$

On dit que $\mathfrak{g}$ est stable par le crochet $[,]$.

Définition 26 :
On dit que $(\mathfrak{g}, +, [\,])$, ou plus simplement $\mathfrak{g}$ est l'algèbre de Lie du groupe G.

Exercice :
Le vérifier directement sur $\mathfrak{sl}_n(\mathbb{K}), \mathfrak{so}_n(\mathbb{K}), \mathfrak{so}(p,q)$ à l'aide des exemples calculés dans la section qui précède.

Démonstration :
Le groupe G agit sur lui-même par conjugaison en stabilisant I_n. pour être plus explicite :

$$\begin{array}{rccccc} \mathrm{Ad}: & G & \longrightarrow & \mathrm{Aut}(G) & & \\ & g & \longmapsto & \mathrm{Ad}_g: & G \longrightarrow G & \\ & & & & h \longmapsto ghg^{-1} & \end{array}$$

En prenant la différentielle de $\mathrm{Ad}(g)$, on obtient un action linéaire de G sur $\mathfrak{g}$ que l'on appelle encore Ad :

$$\begin{array}{rccccc} \mathrm{Ad}: & G & \longrightarrow & GL(\mathfrak{g}) & & \\ & g & \longmapsto & \mathrm{Ad}_g: & \mathfrak{g} \longrightarrow \mathfrak{g} & \\ & & & & h \longmapsto ghg^{-1} & \end{array}$$

On a $\phi(I) = I_n$ donc $d\phi_I: \begin{array}{ccc} \mathfrak{g} & \longrightarrow & M_n(\mathfrak{g}) \\ X & \longmapsto & d\phi_I(X) \end{array}$

On a $\phi(I) = I_n$ donc, en prenant la différentielle de Ad, on obtient $d\mathrm{Ad}_I: \begin{array}{ccc} \mathfrak{g} & \longrightarrow & M_n(\mathfrak{g}) \\ X & \longmapsto & d\phi_I(X) \end{array}$

Cette différentielle est la partie linéaire en X de $Y \longmapsto (I+X)Y(I+X)^{-1}$ $\begin{array}{l} = (Y + XY)(I - X + X^2 + \cdots) \\ = Y + YX - XY + \cdots \end{array}$

On a donc $d\phi_I(X) : Y \longmapsto YX - XY$. Ainsi $\mathfrak{g}$ est bien stable par le crochet puisque $d\phi_I(X) : \mathfrak{g} \longrightarrow \mathfrak{g}$.

□

On vient de rencontrer une nouvelle structure, celle d'algèbre de Lie, qui apparait donc naturellement sur l'espace tangent au neutre e d'un groupe de Lie. Avec une nouvelle structure arrive toujours la notion de morphisme.

Définition 27 :
Soit $\mathfrak{g}$ et $\mathfrak{h}$ deux algèbres de Lie un morphisme d'algèbre de Lie ϕ : $\mathfrak{g} \to \mathfrak{h}$ est un morphisme d'espaces vérifiant

$$[\phi(x), \phi(y)] = \phi([x, y]),\ x, y \in \mathfrak{g}.$$

La notion de sous-algèbre de Lie est naturelle : $\mathfrak{h}$ est une sous-algèbre de l'algèbre de Lie $\mathfrak{g}$, si $\mathfrak{h}$ est un sous-espace de $\mathfrak{g}$ stable par le crochet.
Pour définir la notion d'algèbre de Lie quotient, il faut d'abord définir celle d'idéal de Lie :

Définition 28 :
Un espace $\mathfrak{h}$ *est un idéal de Lie de l'algèbre de Lie* $\mathfrak{g}$ *si* $\mathfrak{h}$ *est un sous-espace de* $\mathfrak{g}$ *vérifiant*

$$\forall x \in \mathfrak{g},\ \forall y \in \mathfrak{h},\ \ [x,y] \in \mathfrak{h}.$$

On montre alors facilement que si $\mathfrak{h}$ est un idéal de Lie de l'algèbre de Lie $\mathfrak{g}$, alors l'espace quotient $\mathfrak{g}/\mathfrak{h}$ a une structure d'algèbre de Lie par le crochet de $\mathfrak{g}$ passé au quotient.
Soit ϕ un morphisme entre deux algèbres de Lie $\mathfrak{h}$ et $\mathfrak{g}$ On montre alors que $\operatorname{Ker}\phi$ est un idéal de Lie de $\mathfrak{h}$, que $\operatorname{Im}(\phi)$ est une sous-algèbre de Lie de $\mathfrak{g}$. Tout est prêt pour l'isomorphisme canonique d'algèbres de Lie

$$\mathfrak{h}/\operatorname{Ker}\phi \simeq \operatorname{Im}(\phi).$$

Nous allons maintenant admettre quelques résultats important de la théorie. On recommande Mneimné-Testard, chap. 3, pour des preuves.

Cette proposition est somme toute bien naturelle.

Proposition 46 :
La différentielle en l'identité d'un morphisme de groupes de Lie $\phi : G \longrightarrow H$ *induit un morphisme d'algèbre de Lie* $d\phi : \mathfrak{g} \longrightarrow \mathfrak{h}$.

Ce théorème est fondamental pour faire "remonter" les informations de l'algèbre de Lie à son groupe de Lie.

Théorème 17 :
Soit $G \subset GL_n(\mathbb{C})$ *un groupe de Lie.*
Alors son algèbre de Lie est donnée par $\operatorname{Lie} G = \mathfrak{g} = \{X \in GL_n(\mathbb{C}) \ : \ \exp(tX) \in G, \quad \forall t \in \mathbb{R}\}$.

Ce théorème ouvre la voie à un "dictionnaire" de traduction entre algèbre de Lie et groupes de Lie. Plus précisément, soit G un groupe de Lie fermé connexe (dans $GL_n(\mathbb{K})$) et $\mathfrak{g}$ son algèbre de Lie. Alors, il y a correspondance biunivoque entre les sous-algèbres de Lie $\mathfrak{h}$ de $\mathfrak{g}$ et les sous-groupes fermés connexes H de G. La flèche $\longrightarrow$ correspond à $H \longrightarrow \mathfrak{h} := \operatorname{Lie}(H)$. La flèche $\longleftarrow$ correspond à $H :=< \exp(\mathfrak{h}) >_{grp} \longrightarrow \mathfrak{h}$, le groupe H étant le groupe engendré par l'exponentielle de l'algèbre de Lie $\mathfrak{h}$.

Sous-algèbres de Lie de $\mathfrak{g}$:	$\longleftrightarrow$	**Sous-groupes fermés connexes de** G :
Idéal de Lie	$\longleftrightarrow$	Sous-groupe distingué
Centre $Z(\mathfrak{g}) := \{z,\ [z,x] = 0, \forall x \in \mathfrak{g}\}$	$\longleftrightarrow$	Composante connexe de e du centre de G.
Algèbre de Lie dérivée $D(\mathfrak{g}) =< [x,y], x, y \in \mathfrak{g} >_{ev}$	$\longleftrightarrow$	Sous-groupe dérivé topologique $D(G)$
Sous-algèbre de Lie abélienne (commutateurs nuls)	$\longleftrightarrow$	Sous-groupes abéliens

Introduction à la théorie des groupes classiques, Chap. 3, 4, 5, Rached Mneimné, Frédéric Testard, **Hermann**.
Calcul differentiel, André Avez, **Masson**.

4 Annexe 8 : Rappels de calcul différentiel

Si f est une application linéaire de $\mathbb{R}^n$ dans $\mathbb{R}^m$, on sait, à l'aide de théorèmes d'algèbre linéaire, montrer si f est injective, surjective, calculer son rang...
Le calcul différentiel permet de généraliser ces caractérisations au cas où f est une application de classe $\mathcal{C}^1$ de $\mathbb{R}^n$ dans $\mathbb{R}^m$ (on note $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^m)$ munis de leur topologie usuelle). On utilise un principe fécond de linéarisation. La seule différence est que l'on obtient des résultats locaux. Le théorème qui règne en maître est le théorème d'inversion locale dont les hypothèses généralisent celles du système de Cramer :

Théorème 18 (d'inversion locale):
Soit $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^m)$ et $a \in \mathbb{R}^n$.
Si df_a est un isomorphisme, alors il existe un voisinage V de a tel que la restriction de f à V soit un difféomorphisme de V vers un ouvert de $f(a)$.

retour p61

Comme on va travailler sur des groupes et non pas sur $\mathbb{R}^n$, le bon cadre général est de travailler sur des variétés différentiables, ou plutôt dans le cadre un peu plus simple des sous-variétés de $\mathbb{R}^n$.

Définition 29 :
Une partie X de $\mathbb{R}^n$ est une sous-variété de dimension m de $\mathbb{R}^n$ si pour tout x de X, il existe un ouvert V de x, un sous-espace F de $\mathbb{R}^n$, un ouvert U de $\mathbb{R}^n$ et un difféomorphisme ϕ de U sur V tels que $\phi(U \cap F) = V \cap X$.

Le caractère "localement $\mathbb{R}^m$" de la définition d'une sous-variété va faire que le théorème d'inversion locale n'a aucun mal à s'y généraliser. Maintenant, cette définition peut en rebuter quelques-uns, mais pour rassurer les uns et informer les autres : d'une part, elle est assez naturelle (si, si !), puisqu'une structure de variété sur X n'est rien d'autre qu'un atlas avec changement de cartes $\mathcal{C}^1$, une structure de sous-variété de $\mathbb{R}^n$ sur X est donc donnée par un atlas (les $\phi|_{U\cap F}$), mais cette structure doit provenir d'un atlas sur $\mathbb{R}^n$ (donné par $\phi \mid U$). D'autre part, on ne va pas s'en servir concrètement grâce au théorème de submersion, qui est un corollaire du théorème d'inversion locale. On l'admettra, voir [Avez].

Théorème 19 (de submersion):
Soit $f \in \mathcal{C}^1(\mathbb{R}^n, \mathbb{R}^m)$ et $X := f^{-1}(y)$, où $y \in \mathbb{R}^m$.
Si f est une submersion en tout point de X, (ie si df_x est surjective en tout point x de X), alors X est une sous-variété de $\mathbb{R}^n$ de dimension $n - m$.

Instructif : on n'a pas l'équivalent en immersion, c'est à dire que si df_x est injective en tout point de $\mathbb{R}^n$, l'image de f n'est pas une sous-variété (pensez à un lemniscate et méditez).

On travaille sur des sous-variétés parce qu'il y est plus simple d'y définir des espaces tangents, objets fondamentaux pour linéariser :

Définition 30 :
Soit X une sous-variété de $\mathbb{R}^n$ et $x \in X$.
On appelle $T_x(X)$ (espace tangent a x en X), l'ensemble des vecteurs tangents à toutes les courbes $\mathcal{C}^1$ passant par x et incluses dans X, (courbes que l'on peut voir comme des fonctions $f \in \mathcal{C}^1(\mathbb{R}, \mathbb{R}^n)$ à image dans X et telles que $f(0) = x$).

On vérifie que l'espace tangent est bien un sous-espace vectoriel dont la dimension est celle de la variété. Le théorème d'inversion locale devient dans le cadre des sous-variétés de $\mathbb{R}^n$:

Théorème 20 (d'inversion locale *bis*):
Soient X et Y des sous-variétés de $\mathbb{R}^n$ et $\mathbb{R}^m$ respectivement. Soient $f \in \mathcal{C}^1(X,Y)$ et $a \in X$.
Si df_a est un isomorphisme de $T_a(X)$ sur $T_{f(a)}(Y)$, alors il existe un voisinage $V \subset X$ de a tel que la restriction de f à V soit un difféomorphisme de V vers un ouvert $W \subset Y$ de $f(a)$.

Cette version du théorème d'inversion locale confère au théorème de submersion un supplément non négligeable :

Théorème 21 (de submersion (suite)):
De plus, $T_x(X) = \mathrm{Ker}(df_x)$.

C'est assez intuitif finalement : si une fonction est constante sur une variété, ses différentielles y sont nulles sur les espaces tangents, la conclusion est une question de dimension.

Chapitre IX

Trois problèmes de géométrie

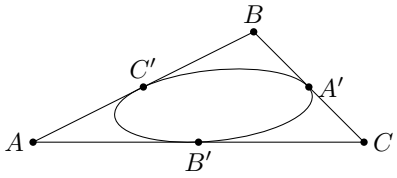
« On est tombées sur la tête ! On en pince pour un type qu'est mort il y a deux mille ans. »

Thérèse, Alain Cavalier, 1986.

Nous allons voir un lien entre géométrie plane et groupes de transformations sur trois exemples. On aura d'ailleurs bien conscience que ces exemples, (ellipse de Steiner, théorème de Desargues, alternative de Steiner) ne seront pas important en soi dans le cadre du cours.
L'importance est surtout dans la méthode, comment et pourquoi interviennent les groupes (groupe affine, groupe projectif réel, groupe projectif complexe). Dans les situations qui suivent, le problème géométrique est posé en terme d'invariants (droite, cercles, barycentre, alignement, parallélisme). La solution est finalement semblable dans les trois cas. Il s'agit de trouver un groupe de transformations respectant les invariants du problème (par exemple, le groupe affine respecte les droites, le barycentre, le parallélisme, mais pas les cercles). Ensuite, on montre à l'aide de ce groupe que l'on peut se ramener à une situation plus simple. Bien entendu, le lecteur pourra trouver dans la littérature (ou par lui-même) d'autres méthodes pour résoudre le problème, mais ici, c'est l'unité de la démarche qui compte.
Maintenant, le choix du groupe demande un minimum de subtilité. Si le groupe est trop grand, il n'aura pas assez d'invariants et donc ne conservera pas les données du problème. S'il est trop petit, alors l'orbite sur la configuration sera elle-même trop petite alors, on aura du mal à se retrouver dans une situation beaucoup plus agréable.
Notons pour finir que le troisième problème utilise les isomorphismes exceptionnels obtenus au chapitre précédent. Nous avons pensé qu'il serait intéressant de voir ces isomorphismes à l'œuvre.

1 L'ellipse de Steiner

Enoncé :
Soit ABC un triangle du plan, A', B', C' les milieux de $[BC], [AC], [AB]$.
Montrer qu'il existe une ellipse tritangente au triangle aux points A', B', C'.



Voici un exercice de géométrie faisant intervenir le groupe affine $GA_2(\mathbb{R})$. Nous présentons ce groupe, ainsi que ses invariants avant de le voir en action pour la résolution de ce problème.

Proposition 47 :
Le groupe affine $GA_2(\mathbb{R}) = \{ \begin{bmatrix} a & c & x_0 \\ b & d & y_0 \\ 0 & 0 & 1 \end{bmatrix} \ : \ a,b,c,d,x_0,y_0 \in \mathbb{R},\ ad-bc \neq 0\} \subset GL_3(\mathbb{R})$ *agit sur* $\mathbb{A}^2$ *par action naturelle (en assimilant le point affine* (x,y) *au vecteur* $\begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$*) :*

$$\begin{bmatrix} a & c & x_0 \\ b & d & y_0 \\ 0 & 0 & 1 \end{bmatrix} \cdot (x,y) = \begin{bmatrix} a & c & x_0 \\ b & d & y_0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = (ax+cy+x_0, bx+dy+y_0)$$

Ses invariants sont
- *l'alignement (trois points alignés ont pour image trois points alignés),*
- *le parallélisme :* $D \parallel D'$ *et* $g \in GA_2 \Longrightarrow g(D) \parallel g(D')$*. On vérifie que la direction de* $g(D)$ *est bien* $\overrightarrow{g}(\overrightarrow{D})$*.*
- *le barycentre :* G *barycentre de* $(A_1,a_1),\cdots,(A_n,a_n) \Longrightarrow g(G)$ *barycentre de* $(g(A_1),a_1),\cdots,(g(A_n),a_n)$*. On applique à* $\overrightarrow{g}$ *l'écriture vectorielle du barycentre* $\overrightarrow{g}(\overrightarrow{AB}) = \overrightarrow{g(A)g(B)}$*.*

Exercice :
Montrer qu'on a la suite exacte $1 \longrightarrow \tau_n(\mathbb{K}) \hookrightarrow GA_n(\mathbb{K}) \underset{\text{section}}{\overset{\longrightarrow}{\leftarrow}} GL_n(\mathbb{K}) \longrightarrow 1$
Avec $\tau_n(\mathbb{K}) \simeq \mathbb{K}^n$ le groupe des translations du $\mathbb{K}$-espace affine $\mathbb{A}^n$, et où la surjection est l'application $g \mapsto \overrightarrow{g}$.
Montrer que tout point A de l'espace affine définit une section s_A telle que $s_A(\overrightarrow{g})(B) = A + \overrightarrow{g}(\overrightarrow{AB})$.

Définition 31 :
Un repère de $\mathbb{A}^2$ *est un triplet* (O,I,J) *de points de* $\mathbb{A}^2$ *non-alignés (ou tels que* $(\overrightarrow{OI},\overrightarrow{OJ})$ *soit une base de* $\mathbb{R}^2$*).*

Proposition 48 :
$GA_2(\mathbb{R})$ *agit simplement et transitivement sur les repères de* $\mathbb{A}^2$*.*
Autrement dit, pour toute paire de repères (O,I,J) *et* (O',I',J')*, il existe un unique* $g \in GA_2(\mathbb{R})$ *tel que* $\begin{aligned} g(O) &= O', \\ g(I) &= I', \\ g(J) &= J' \end{aligned}$

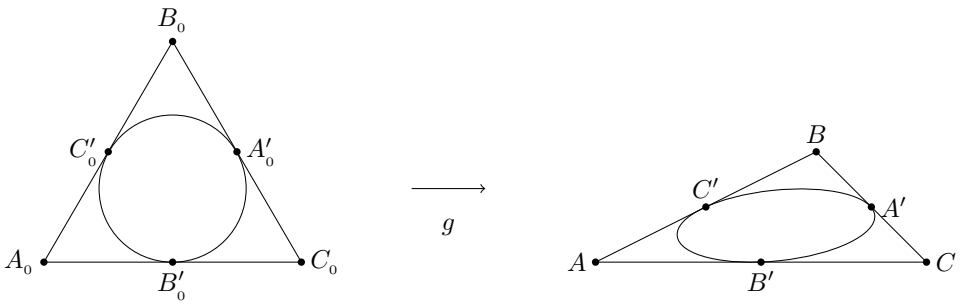
Démonstration :
Nécéssairement $g(O) = O'$ et $\overrightarrow{g}$ est caractérisé de façon unique par $\overrightarrow{g}(\overrightarrow{OI}) = \overrightarrow{O'I'}$ et $\overrightarrow{g}(\overrightarrow{OJ}) = \overrightarrow{O'J'}$.

□

Exercice :
Calculer de deux manières différentes $|GA_2(\mathbb{F}_q)|$. Une, en utilisant sa définition, une autre en comptant les repères affines.

Solution de l'énoncé :
Le problème est clair si $A_0B_0C_0$ est équilatéral. L'ellipse est dans ce cas le cercle inscrit au triangle. Les points A, B, C formant un repère du plan affine, la proposition précédente assure qu'il existe $g \in GA_2(\mathbb{R})$
tel que $g(A_0) = A,\ g(B_0) = B,\ g(C_0) = C$ (l'unicité étant ici inutile). Alors

1. Les milieux sont conservés $g(A'_0) = A',\ g(B'_0) = B',\ g(C'_0) = C'$ par conservation du barycentre,
2. l'image du cercle par g est une conique (puisqu'un changement de variables linéaire préserve le degré) compacte, c'est donc une ellipse,
3. g est différentiable donc la tangence est conservée.

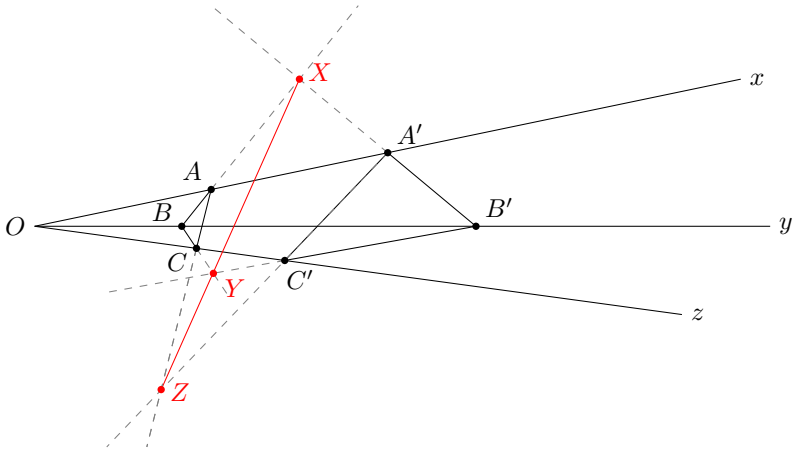


2 Le théorème de Desargues

Girard Desargues (1591 - 1661), Lyonnais.

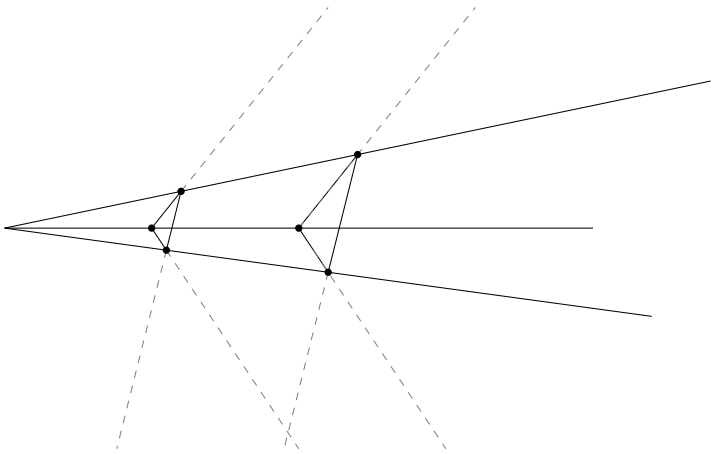
Le théorème de Desargues est le théorème de base de la géométrie projective. Il est intéressant de savoir qu'il ne peut pas se retrouver à l'aide des axiomes de la géométrie affine. On sait aussi que dans la formalisation de la géométrie par la théorie des espaces vectoriels, "l'axiome de Desargues" est équivalent à l'associativité de la multiplication dans le corps de base. En quelques sortes, si on veut faire de la géométrie moderne où Desargues ne marche pas, il faut travailler dans un espace vectoriel sur un corps non associatif (on vous laisse deviner la définition), par exemple sur les octonions.

Théorème 22 (Desargues):
Deux triangles ABC et $A'B'C'$ du plan sont en perspective $\iff$ X, Y, Z sont alignés.
Où $X = AB \cap A'B', \quad Y = BC \cap B'C', \quad Z = AC \cap A'C'$



Ce problème de géométrie fait intervenir le groupe projectif $PGL_3(\mathbb{R})$. Comme précédemment, nous allons présenter ce groupe, ainsi que ses invariants.

Remarque :
Dans le cas où les triangles ABC et $A'B'C'$ sont "parallèles",
les points X, Y et Z sont à l'infini :



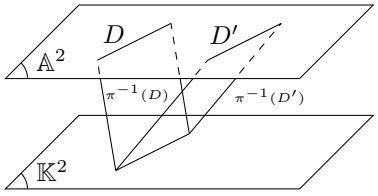
L'idée est donc d'envoyer X, Y, Z en l'infini pour obtenir cette configuration plus sympathique qui est en fait la réunion de trois configurations de Thalès. Mais le groupe $GA_2(\mathbb{R})$ conserve le parallélisme et il ne permet donc pas de se ramener à cette situation.
Nous allons donc introduire le groupe projectif $PGL_3(R)$ qui agit sur le plan projectif $\mathbb{P}^2(R)$.

Proposition 49 :
Le groupe projectif linéaire $PGL_3(\mathbb{R}) = {}^{GL_3(\mathbb{R})}\!/_{\mathbb{R}^*}$*, agit naturellement et fidèlement sur l'espace projectif* $\mathbb{P}^2(\mathbb{R}) = \mathbb{P}^1(\mathbb{R}) \sqcup \mathbb{A}^2$*, ensemble des droites de* $\mathbb{R}^3$.

Son invariant est l'alignement, il ne conserve ni le barycentre, ni le parallelisme.

Remarque :
Ces définitions et cette proposition peuvent être généralisées en dimension quelconque.

Un point de $\mathbb{P}^2$ est assimilé à une droite vectorielle de $\mathbb{R}^3$ et une droite de $\mathbb{P}^2$ est assimilée à un plan vectoriel de $\mathbb{R}^3$, par la projection $\pi : \mathbb{R}^3 \backslash_{\{0\}} \longrightarrow \mathbb{P}^2$ qui associe à un vecteur non nul de l'espace la droite qu'il engendre.
Ainsi on montre que $PGL_3(\mathbb{R})$ préserve l'alignement des points de $\mathbb{P}^2$ en remarquant par relèvement que $GL_3(\mathbb{R})$ préserve la "coplanarité" des droites.
Maintenant, nous devons plonger le plan affine sur lequel on travaille dans le plan projectif comme dans le chapitre VI. Le plan affine devient une partie ouverte et dense du plan projectif pour la topologie quotient.
L'inconvenient de $PGL_3(\mathbb{R})$ est qu'il ne stabilise pas $\mathbb{A}^2 \subsetneq \mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$. En revanche, il est intuitivement plus gros que $GA_2(\mathbb{R})$ (de dimension $9-1=8$ contre la dimension 6 de GA_2), donc plus "puissant" : il permet de se ramener à de plus nombreuses situations.
En l'occurrence, deux droites parallèles D et D' de $\mathbb{A}^2$ se coupent en l'infini, comme l'indique le dessin :



$$\begin{aligned}\mathbb{P}^2(\mathbb{K}) &= \mathbb{A}^2 \sqcup \mathbb{P}^1(\mathbb{K}) \\ &= \{\text{droites coupant } \mathbb{A}^2\} \sqcup \{\text{droites de } \mathbb{K}^2\}\end{aligned}$$

Pour être plus précis, ce dessin représente $\mathbb{P}^2$ qui est l'union du plan affine correspondant au plan d'équation $z = 1$ et la droite projective correspondant aux droites du plan vectoriel $z = 0$. Voici comment penser que deux droites parallèles se coupent en l'infini : Si D et D' sont deux droites affines parallèles, alors elles définissent deux plans $\pi^{-1}(D)$, $\pi^{-1}(D')$ dans $\mathbb{R}^3$. Et comme elles sont parallèles, ces deux plans se coupent en une droite vectorielle du plan $z = 0$ qui définit elle-même un point P de $\mathbb{P}^2$. On dit donc que les droites D et D' se coupent en P.

Définition 32 :
Soit $(e_i)_{0\leq i\leq 2}$ *une base de* $\mathbb{R}^3$.
On appelle repère projectif (P_0, P_1, P_2, P_3) *de* $\mathbb{P}^2$ *un quadruplet de points de* $\mathbb{P}^2$ *tels que*
(1) $(P_0, P_1, P_2) = \pi(e_0, e_1, e_2)$
(2) $P_3 = \pi(1, 1, 1)$ *dans cette base.*

On vérifie que c'est équivalent à la définition suivante :

Définition 33 (*bis*):
On appelle repère projectif (P_0, P_1, P_2, P_3) *de* $\mathbb{P}^2$ *un quadruplet de points de* $\mathbb{P}^2$ *dont trois quelconques d'entre eux ne sont pas alignés.*

Effectivement, la première définition implique clairement la seconde. Pour la réciproque, il suffit de partir des points P_i, $0 \leq i \leq 3$ et de choisir des relevés respectifs e'_i, $0 \leq i \leq 3$. Par hypothèse, e'_i, $0 \leq i \leq 2$, forme une base de l'espace et de plus, e'_3 possède des coordonnées toutes non nulles (λ_i) dans cette base. Il suffit de poser $e_i = \lambda_i e'_i$, $0 \leq i \leq 2$, pour se ramener à la construction de la première définition.

Proposition 50 :
$PGL_3(\mathbb{R})$ *agit transitivement et simplement sur l'ensemble des repères projectifs de* $\mathbb{P}^2$.

Remarque :
Ces définitions et cette proposition peuvent être généralisées en dimension quelconque.

Démonstration :
D'après la définition *bis*, trois droites non coplanaires ont leurs images par un élément de $GL_3(\mathbb{R})$ non coplanaires, d'où l'action de $PGL_3(\mathbb{R})$ sur l'ensemble des repères projectifs de $\mathbb{P}^2$.

Soient $(P_i)_{0\leq i\leq 3}$ et $(P'_i)_{0\leq i\leq 3}$ deux repères projectifs. On veut montrer qu'il existe un unique $g \in PGL_3(\mathbb{R})$ tel que $g(P_i) = P'_i$ pour tout i. On veut donc trouver $\tilde{g} \in GL_3(\mathbb{R})$ tel que $\tilde{g}(e_i) = \lambda e'_i$, pour $0 \leq i \leq 3$ et $\lambda_i \neq 0$, et où e_i, e'_i sont les vecteurs directeurs de $\pi^{-1}(P_i), \pi^{-1}(P'_i)$.
Fixons λ_i, soit $\tilde{g}$ l'unique automorphisme tel que $\forall 0 \leq i \leq 2, \quad \tilde{g}(e_i) = \lambda_i e'_i$. Il reste à voir que $\tilde{g}(e_3) = \lambda_3 e'_3$. Donc

$$\lambda_0 e'_0 + \lambda_1 e'_1 + \lambda_2 e'_2 = \lambda_3 e'_3 = \lambda_3(e'_0 + e'_1 + e'_2),$$

et donc les λ_i sont tous égaux. Conclusion, il existe un unique $\tilde{g} \in GL_3(\mathbb{R})$ à homothétie près, donc g est unique dans $PGL_3(\mathbb{R})$.

□

Toujours pareil, on teste notre compréhension sur les corps finis où tout se compte :

Exercice :
En dimension n, un repère projectif de $\mathbb{P}^n$ comprend $n+2$ points tels que $n+1$ points parmi eux n'appartiennent pas au même hyperplan. Montrer (géométriquement !) en utilisant les deux définitions du repère géométrique que :

$$\begin{aligned} |PGL_n(\mathbb{F}_q)| &= (q^n-1)\cdots(q^2-1)q^{\frac{n(n-1)}{2}} \\ &= (1+q+\cdots+q^{n-1})(q+q^2+\cdots+q^{n-1})\cdots q^{n-1}(q-1)^{n-1} \\ &= |\{\text{repères projectifs de } \mathbb{P}^n\}| \end{aligned}$$

Démonstration :
(du théorème de Desargues)

$\boxed{\Longrightarrow}$ Condition nécessaire ("si") :
On va se ramener grâce au groupe projectif réel, au cas où les triangles sont "parallèles".
Supposons que ABC et $A'B'C'$ soient en perspective, et montrons que X, Y, Z sont alignés. D'après ce qui précède, il existe $g \in GL_3(\mathbb{R})$ qui envoie X, Y sur deux points à l'infini (rappelons que l'infini est une droite projective et que deux points distincts peuvent toujours être complétés en un repère projectif).
Ainsi, les droites BC et $B'C'$ sont parallèles et de même AC et $A'C'$ sont parallèles.

Par conservation de l'alignement, montrer que X, Y, Z sont alignés revient à montrer que Z est aussi à l'infini, c'est à dire AC et $A'C'$ parallèles. C'est le théorème de Thales :

$$\begin{cases} AC \parallel A'C' \\ BC \parallel B'C' \end{cases} \Longrightarrow \begin{cases} \frac{OA}{OB} = \frac{OA'}{OB'} \\ \frac{OB}{OC} = \frac{OB'}{OC'} \end{cases} \Longrightarrow \frac{OA}{OC} = \frac{OA'}{OC'} \Longrightarrow AC \parallel A'C'$$

$\boxed{\Longleftarrow}$ Condition suffisante ("seulement si") :
La condition suffisante découle de la condition nécessaire par *autodualité projective*. On munit $\mathbb{R}^3$ d'une forme bilinéaire non-dégénérée et on remarque qu'ainsi l'orthogonalité envoie les points de $\mathbb{P}^2$ sur les droites de $\mathbb{P}^2$ et inversement.
L'orthogonalité fournit donc une bijection involutive qui inverse les inclusions et on vérifie que :

(1) P est un point $\Longleftrightarrow P^\perp$ est une droite,

(2) p est une droite $\Longleftrightarrow p^\perp$ est un point,

(3) $P \in p \Longleftrightarrow p^\perp \in P^\perp$,

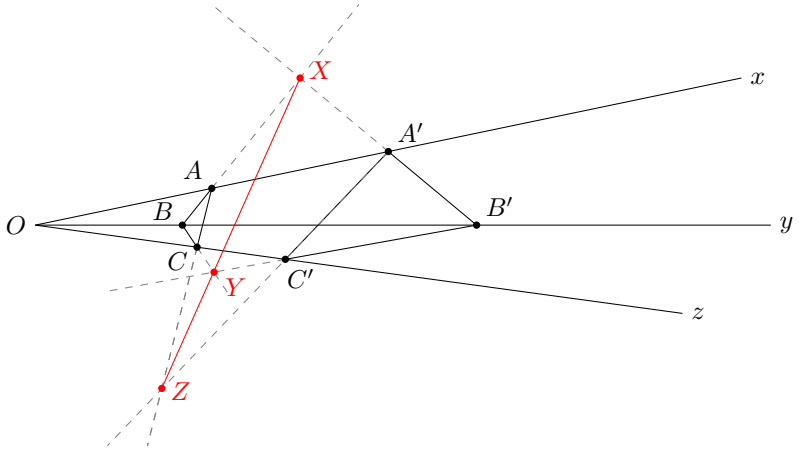
(4) les points P_0, P_1, P_2 sont alignés $\Longleftrightarrow$ les droites $P_0^\perp, P_1^\perp, P_2^\perp$ sont concourantes,

(5) $p \cap q = R \Longleftrightarrow R^\perp = (PQ)$ avec $P = p^\perp$ et $Q = q^\perp$.

Remarque :
On peut, si on n'aime pas le choix d'une forme, utiliser l'orthogonalité "canonique" dans l'espace dual.

En dualisant le "si" que nous venons de montrer, nous obtenons le "seulement si". C'est l'autodualité de la configuration de Desargues. Pour le voir plus précisément :

De trois droites x, y, z, on définit deux points sur chacune : $A, A' \in x$ puis $B, B' \in y$ et $C, C' \in z$.
En construisant les droites $a = BC$, $b = AC$, $c = AB$ ainsi que $a' = B'C'$, $b' = A'C'$, $c' = A'B'$, on obtient trois points $X = a \cap a'$, $Y = b \cap b'$, $Z = c \cap c'$ que l'on sait alignés sur une droite.
On suppose les points X, Y, Z alignés. Alors, en utilisant les points 1 à 5 qui précèdent, on obtient que les droites $X^\perp$, $Y^\perp$, $Z^\perp$ sont concourantes. Donc, par le "si" de la proposition, il vient que $x^\perp$, $y^\perp$, $z^\perp$, sont alignés. Ce qui donne que $x = AA'$, $y = BB'$, $z = CC'$ sont concourantes.

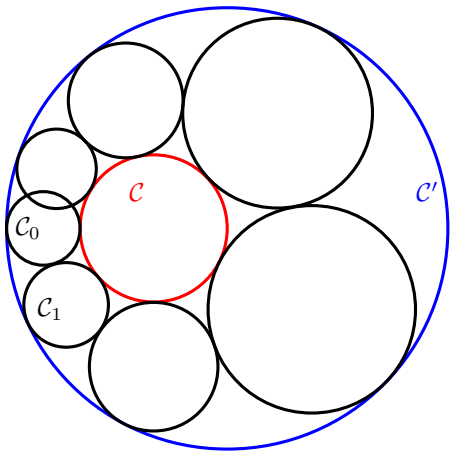


□

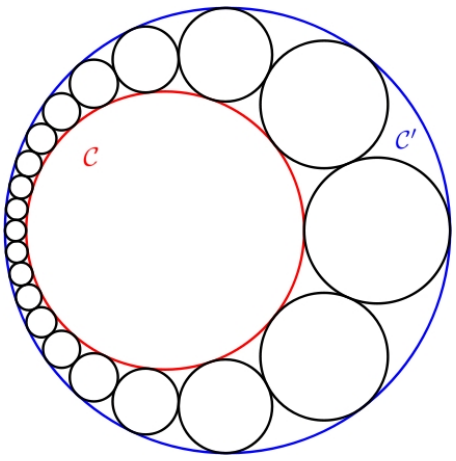
3 L'alternative de Steiner

Cette fois-ci la résolution va provenir du groupe de transformations $PSL_2(\mathbb{C})$ et d'un isomorphisme exceptionnel vu dans le chapitre précédent. Pour une autre preuve utilisant les inversions, on recommande le Audin.

Enoncé :
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux cercles du plan tels que $\mathcal{C}$ est à l'intérieur de $\mathcal{C}'$. On construit un cercle $\mathcal{C}_0$ tangent à $\mathcal{C}$ et $\mathcal{C}'$, puis un cercle $\mathcal{C}_1$ tangent à $\mathcal{C}_0, \mathcal{C}, \mathcal{C}'$, et par itération un cercle $\mathcal{C}_n$ tangent à $\mathcal{C}_{n-1}, \mathcal{C}, \mathcal{C}'$.
Alors soit il existe, soit il n'existe pas de $n_0 \in \mathbb{N}$, tel que $\mathcal{C}_{n_0} = \mathcal{C}_0$, ET CETTE ALTERNATIVE NE DÉPEND PAS DU CERCLE $\mathcal{C}_0$ CHOISI.



Cas $\mathcal{C}_0 \neq \mathcal{C}_7$



Cas $\mathcal{C}_0 = \mathcal{C}_{20}$

Remarque :
Sur la figure, pour des raisons de lisibilité, les cercles $\mathcal{C}_i$ se rebouclent en un seul tour, mais ils pourraient se reboucler en plus de tours.

L'idée est de se ramener au cas où les cercles $\mathcal{C}$ et $\mathcal{C}'$ sont concentriques où le problème est beaucoup plus simple. Il est clair que le groupe affine ne va pas nous y amener car il conserve le barycentre. On va introduire le groupe $PGL_2(\mathbb{C})$ qui transforme la droite projective complexe $\mathbb{C} \cup \{\infty\}$ et dans lequel le plan affine réel est un ouvert dense.

Proposition 51 :
Le groupe projectif linéaire $PGL_2(\mathbb{C}) = {GL_2(\mathbb{C})}/{\mathbb{C}^*}$ *agit naturellement sur le groupe projectif* $\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \sqcup \mathbb{P}^0(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \sqcup \{\infty\}$, *ensemble des droites (complexes) de* $\mathbb{C}^2$ *(c'est la sphère de Riemann) :*

$$\begin{array}{ccc} PGL_2(\mathbb{C}) \times \mathbb{P}^1(\mathbb{C}) & \longrightarrow & \mathbb{P}^1(\mathbb{C}) \\ \left(\begin{bmatrix} a & c \\ b & d \end{bmatrix}, (z : z')\right) & \longmapsto & (bz + dz' : az + cz') \end{array}$$

Ne pas confondre $\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \sqcup \{\infty\}$ et $\mathbb{P}^2(\mathbb{R}) = \mathbb{A}^2(\mathbb{R}) \sqcup \mathbb{P}^1(\mathbb{R}) = \mathbb{A}^2(\mathbb{R}) \sqcup \mathbb{A}^1(\mathbb{R}) \sqcup \{\infty\}$

Définition 34 :
On va identifier $\mathbb{P}^1(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) \sqcup \{\infty\}$ *avec* $\mathbb{C} \sqcup \{\infty\}$ *par transport de structure, grâce à la bijection :*

$$\begin{array}{rccc} \varphi : & \mathbb{P}^1(\mathbb{C}) & \xhookrightarrow{\sim} & \mathbb{C} \sqcup \{\infty\} \\ & (z : z') & \longmapsto & \begin{cases} \frac{z'}{z} & si\ z \neq 0 \\ \infty & si\ z = 0 \end{cases} \end{array}$$

On peut alors reformuler l'action :

Proposition 52 :
Le groupe projectif linéaire $PGL_2(\mathbb{C})$ *agit sur* $\mathbb{C} \sqcup \{\infty\}$ *par :*

$$\begin{array}{ccc} PGL_2(\mathbb{C}) \times (\mathbb{C} \sqcup \{\infty\}) & \longrightarrow & \mathbb{C} \sqcup \{\infty\} \\ \left(\begin{bmatrix} a & c \\ b & d \end{bmatrix}, z\right) & \longmapsto & \begin{cases} \frac{a+cz}{b+dz} & si\ z \neq \infty\ et\ b + dz \neq 0 \\ \frac{c}{d} & si\ z = \infty\ et\ d \neq 0 \\ \infty & si\ b + dz = 0 \end{cases} \end{array}$$

Ses invariants ne sont ni l'alignement réel, ni le rapport $\frac{z_2 - z_1}{z_2 - z_0}$ *(contrairement à l'action de* $GA_1(\mathbb{C})$ *qui conserve le rapport par Thalès), mais le birapport (ou rapport des rapports)* $[z_0, z_1, z_2, z_3] = \dfrac{z_2 - z_1}{z_2 - z_0} : \dfrac{z_3 - z_1}{z_3 - z_0}$.

Démonstration :
Montrons l'invariance du birapport. On pose $g \cdot z_i = z'_i, \quad \forall 0 \leq i \leq 3$, avec $g \in PGL_2(\mathbb{C})$ et $z_i \in \mathbb{C} \sqcup \{\infty\}$.

Alors $\dfrac{z'_2 - z'_1}{z'_2 - z'_0} = \dfrac{\frac{a+cz_2}{b+dz_2} - \frac{a+cz_1}{b+dz_1}}{\frac{a+cz_1}{b+dz_1} - \frac{a+cz_0}{b+dz_0}} = \frac{z_2 - z_1}{z_2 - z_0} : \frac{b+dz_0}{b+dz_1}$

Et donc $[z'_0, z'_1, z'_2, z'_3] = [g \cdot z_0, g \cdot z_1, g \cdot z_2, g \cdot z_3] = \frac{z'_2 - z'_1}{z'_2 - z'_0} : \frac{z'_3 - z'_1}{z'_3 - z'_0} = \frac{z_2 - z_1}{z_2 - z_0} : \frac{z_3 - z_1}{z_3 - z_0} = [z_0, z_1, z_2, z_3]$

□

Définition 35 :
Un repère projectif de $\mathbb{P}^1(\mathbb{C})$ *est un triplet de points* (z_0, z_1, z_2) *deux à deux distincts. Un "bon" repère est* $(0, 1, \infty)$.

Proposition 53 :
$PGL_2(\mathbb{C})$ agit de façon simplement transitive sur l'ensemble des repères projectifs de $\mathbb{P}^1(\mathbb{C})$.

Démonstration :
Il suffit de calquer la preuve valable sur $\mathbb{R}$ sur tout corps et adaptable en toute dimension.

□

Proposition 54 :
Soient (z_0, z_1, z_2, z_3), (z'_0, z'_1, z'_2, z'_3) deux quadruplets de points distincts.
Alors $\exists g \in PGL_2(\mathbb{C})$ tel que $g \cdot z_i = z'_i \iff [z'_0, z'_1, z'_2, z'_3] = [z_0, z_1, z_2, z_3]$

Démonstration :

$\boxed{\Longrightarrow}$ Déjà montré.

$\boxed{\Longleftarrow}$ L'équation en z'_3 $\quad [z'_0, z'_1, z'_2, z'_3] = [z_0, z_1, z_2, z_3]$ est de degré 1 donc possède une unique solution. De plus si on pose g tel que $g \cdot z_i = z'_i$, qui existe d'après ce qui précède,
alors $[z'_0, z'_1, z'_2, g \cdot z_3] = [g \cdot z_0, g \cdot z_1, g \cdot z_2, g \cdot z_3] = [z_0, z_1, z_2, z_3]$ d'où par unicité $g \cdot z_3 = z'_3$.

□

Corollaire 9 :
$PGL_2(\mathbb{C})$ stabilise l'ensemble $\mathcal{DC}$ des droites et cercles du plan réel.
L'action de $PGL_2(\mathbb{C})$ sur $\mathcal{DC}$ est transitive.

Démonstration :
Il est bien connu (voir Terminale S) que (z_0, z_1, z_2, z_3) sont les affixes de points alignés ou cocycliques (appartenant à un même cercle) $\iff [z_0, z_1, z_2, z_3] \in \mathbb{R}$.
D'où l'invariance des droites et cercles, la transitivité provenant de la transitivité sur les repères.

□

Remarque :
Lorsqu'une action est transitive, on peut regarder la double transitivité, puis la n-transitivité pour la saturer, jusqu'à assurer sa simplicité, si cela est possible.
Nous allons étudier la double transitivité de l'action $PGL_2(\mathbb{C}) \circlearrowleft \mathcal{DC}$ via une correspondance judicieuse entre $\mathcal{DC}$ et les matrices hermitiennes 2×2 de signature $(1,1)$, à homothétie près. :

D'une part, on considére l'ensemble $H_2^{(1,1)}(\mathbb{C})$ des matrices hermitiennes 2×2 de signature $(1,1)$ sur lequel ont fait agir $PSL_2(\mathbb{C})$ par l'action de congruence (inverse) $g \cdot H = g^{*-1} H g^{-1}$. D'autre part, on considère l'ensemble $\mathcal{DC}$ sur lequel $PSL_2(\mathbb{C})$ agit naturellement.

Proposition 55 :
On a une bijection

$$b : \mathcal{DC} \hookrightarrow H_2^{(1,1)}(\mathbb{C}) \Big/ \mathbb{R}^*$$

qui a la droite ou cercle d'équation $\quad ax^2 + ay^2 + 2bx + 2cy + d = 0 \quad$ où $a, b, c, d, x, y \in \mathbb{R}$, associe la classe de la matrice $\begin{bmatrix} a & b+ic \\ b-ic & d \end{bmatrix}$.
De plus, cette bijection est compatible avec l'action de $PSL_2(\mathbb{C})$, ie $b(g \cdot \mathcal{C}) = g \cdot b(\mathcal{C})$.

Démonstration :
Une droite ou cercle est donnée par une équation de la forme :
- $ax^2 + ay^2 + 2bx + 2cy + d = 0$ où $a, b, c, d, x, y \in \mathbb{R}$, ou de façon équivalente
- $az\overline{z} + (b - ic)z + (b + ic)\overline{z} + d = 0$ où $a, b, c, d \in \mathbb{R}$ et $z \in \mathbb{C}$.

Le quadruplet (a, b, c, d) étant unique à facteur scalaire près.

Réciproquement, (a, b, c, d) définit un élément de $\mathcal{DC}$ si et seulement si $b^2 + c^2 - ad > 0$ (afin que le carré du rayon soit positif).
On considère $H_2(\mathbb{C}) = \{\begin{bmatrix} a & b+ic \\ b-ic & d \end{bmatrix} \in M_2(\mathbb{C}) \ : \ a, b, c, d \in \mathbb{R}\}$.
Soit $h \in H_2(\mathbb{C})$. Alors $b^2 + c^2 - ad > 0 \iff \det h < 0$

$$\iff h \equiv I_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\iff h \text{ est de signature } (1, 1)$$

D'où l'isomorphisme

$$\begin{array}{ccc} H_2^{(1,1)}(\mathbb{C})\big/_{\mathbb{R}^*} & \longrightarrow & \mathcal{DC} \\ \begin{bmatrix} a & b+ic \\ b-ic & d \end{bmatrix} & \longmapsto & \{(x, y) \in \mathbb{R}^2 \ : \ ax^2 + ay^2 + 2bx + 2cy + d = 0\} \end{array}$$

Ou de façon plus subtile

$$H_2^{(1,1)}(\mathbb{C})\big/_{\mathbb{R}^*} \quad \longrightarrow \quad \mathcal{C}_{_H} = \{X = \left[\begin{smallmatrix} z \\ w \end{smallmatrix}\right] \in \mathbb{C}^2 \ : \ X^*HX = 0\} \quad \longrightarrow \quad \mathcal{C}_{_H} \cap \{w = 1\}$$

On vérifie que :

1. $\mathcal{C}_{_H}$ est un cône de $\mathbb{C}^2$ et $SL_2(\mathbb{C}) \circlearrowleft \mathcal{DC}$
2. $g \cdot \mathcal{C}_{_H} = \mathcal{C}_{_{g \cdot H}}$ où $g \cdot H = g^{*-1}Hg^{-1}$, cette action de $SL_2(\mathbb{C})$ stabilisant le déterminant de signature $(3, 1)$ (remarque : $PGL_2(\mathbb{C}) = PSL_2(\mathbb{C})$)
3. $SL_2(\mathbb{C}) \cdot H_2^{(1,1)}(\mathbb{C})\big/_{\mathbb{R}^*} \subset SO_{_0}(3, 1)$

Conclusion :
$PSL_2(\mathbb{C}) \circlearrowleft \mathcal{DC} \iff SO_{_0}(3, 1) \circlearrowleft H_2^{(1,1)}(\mathbb{C})\big/_{\mathbb{R}^*}$ (car $PSL_2(\mathbb{C}) \simeq SO_{_0}(3, 1)$ d'après la proposition 44)

□

Voici la proposition qui va permettre de trivialiser l'alternative de Steiner :

Proposition 56 :
Soient $\mathcal{C}$ et $\mathcal{C}'$ deux cercles tels que $\mathcal{C}'$ soit strictement intérieur à $\mathcal{C}$.
Alors il existe $f \in PSL_2(\mathbb{C})$ tel que $f(\mathcal{C})$ et $f(\mathcal{C}')$ soient deux cercles concentriques.

Démonstration :
Posons $q = -\det$ forme quadratique sur $H_2(\mathbb{C})$.
On associe à $\mathcal{C}$ et $\mathcal{C}'$ des matrices $H, H' \in H_2^{(1,1)}(\mathbb{C})$, uniques à un scalaire (réel) près.

Soient $H = \begin{bmatrix} a & b+ic \\ b-ic & d \end{bmatrix}$ et $H' = \begin{bmatrix} a' & b'+ic' \\ b'-ic' & d' \end{bmatrix}$ avec $a, a', d, d' \neq 0$.

On vérifie facilement que $q(H) = -(ad - b^2 - c^2) = a^2\left[\left(\frac{b}{a}\right)^2 + \left(\frac{c}{a}\right)^2 - \frac{d}{a}\right] = a^2R^2$ avec R rayon de $\mathcal{C}$,

que $q(H') = a'^2R'^2$ de la même manière et en notant φ sa forme bilinéaire symétrique associée,

$2\varphi(H, H') = q(H+H') - q(H) - q(H') = aa'(R^2 + R'^2 - \Omega\Omega'^2)$ où Ω et Ω' sont les centres respectifs de $\mathcal{C}$ et $\mathcal{C}'$.

$$\begin{aligned} \mathcal{C}' \text{ strictement intérieur à } \mathcal{C} &\iff R - R' > \Omega\Omega' \\ &\implies (R-R')^2 > \Omega\Omega'^2 \\ &\implies \varphi(H,H') > q(H)q(H') \end{aligned}$$

On cherche deux matrices $H_0 = \begin{bmatrix} a_0 & 0 \\ 0 & d_0 \end{bmatrix}$ et $H'_0 = \begin{bmatrix} a'_0 & 0 \\ 0 & d'_0 \end{bmatrix}$ hermitiennes telles que $q(H_0) = q(H)$, $q(H'_0) = q(H')$ et $\varphi(H_0, H'_0) = \varphi(H, H')$ d'où le système :

$$\left\{\begin{array}{l} -a_0d_0 = q(H) \\ -a'_0d'_0 = q(H') \\ ad'_0 + a'_0d_0 = -2\varphi(H,H') \end{array}\right. \Bigg| \implies (a_0d'_0)(a'_0d_0) = q(H)q(H') \text{ résoluble si } \Delta > 0 \text{ i.e. si } \varphi(H,H')^2 > q(H)q(H')$$

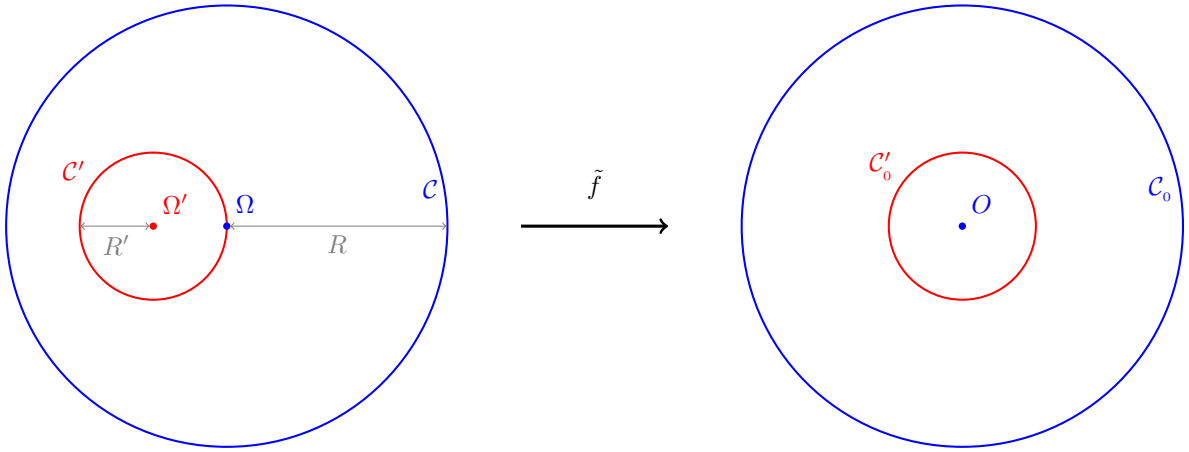
d'où H_0 et H'_0 existent. D'après le théorème de Witt, il existe $\tilde{f} \in O(q)$ telle que $\begin{cases} \tilde{f}(H) = H_0 \\ \tilde{f}(H') = H'_0 \end{cases}$

Or on a vu que $\tilde{f} \in O(3,1) \simeq SO_0(3,1) \sqcup gSO_0(3,1) \sqcup hSO_0(3,1) \sqcup ghSO_0(3,1)$

avec $g = \begin{bmatrix} -1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & 1 \end{bmatrix}$ et $h = \begin{bmatrix} -1 & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & -1 \end{bmatrix}$

Or $\begin{array}{l} g : (a,b,c,d) \longmapsto (-a,b,c,d) \\ h : (a,b,c,d) \longmapsto (-a,b,c,-d) \end{array}$ préservent le centre.

Donc il existe $\tilde{f} \in SO_0(3,1) \simeq PSL_2(\mathbb{C})$ qui transforme $\mathcal{C}$ et $\mathcal{C}'$ en $\mathcal{C}_0$ et $\mathcal{C}'_0$ concentriques de centre O. L'alternative est alors claire par symétrie circulaire.



□

Géométrie, Chap. 3, 5, Michèle Audin, **Belin**.

Pour le birapport, on peut aussi jeter un coup d'oeil à :

Eléments de géométrie, actions de groupes, Note 0-B, Rached Mneimné, **Cassini**.

Chapitre X

Solides platoniciens

« And now for something completly different »

Flying Circus, Monty Python, 1969.

1 Présentation

Voici une leçon simple, mais très utile pour illustrer l'importance des groupes et des actions de groupes sur des objets concrets de l'espace : les solides platoniciens, c'est à dire les polytopes réguliers convexes de notre espace euclidien de dimension trois. L'intérêt de cette leçon réside justement dans le fait qu'on y retrouve dans un cadre concret des notions comme les groupes, les sous-groupes de Sylow, la dualité... C'est un exemple phare de leçon transversale entre géométrie et algèbre.

Même si d'un point de vue topologique, les "graphes" de tous les solides platoniciens seront retrouvés, nous admettrons leur existence au sens métrique. En fait, leur existence peut être montrée, soit par une succession de données (par exemple les coordonnées des sommets) pas très illuminante, soit alors à l'aide de la théorie des représentations, beaucoup plus spectaculaire, mais un peu hors de portée dans ce cursus.

Définition 36 :
Dans $\mathbb{R}^3$, un solide Platonicien est un polyèdre de dimension 3 *régulier (faces identiques et régulières) convexe.*

Définition 37 :
On appelle symbole de Schläfli le couple $\{p, q\}$, où p est le nombre d'arêtes de chaque face et q le degré de chaque sommet (nombre d'arêtes ayant ce sommet pour extrémité).

On admettra la classification des solides platoniciens, modulo l'action des similitudes. Voici le tableau synthétique de ce que nous allons étudier dans ce chapitre.

Polyèdre	X	**Figure**	**Dual**	**Sommets**	**Arêtes**	**Faces**	**Schläfli**	$\mathrm{Is}(X)$	$\mathrm{Is}^+(X)$
Tétraèdre	Δ_4		Δ_4	4	6	4	$\{3,3\}$	$\mathfrak{S}_3$	$\mathfrak{A}_4$
Hexaèdre[11]	C_6		Δ_8	8	12	6	$\{4,3\}$	$\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{S}_4$
Octaèdre	Δ_8		C_6	6	12	8	$\{3,4\}$	$\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{S}_4$
Dodécaèdre	P_{12}		Δ_{20}	20	30	12	$\{5,3\}$	$\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{A}_5$
Icosaèdre	Δ_{20}		P_{12}	12	30	20	$\{3,5\}$	$\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{A}_5$

[12]Parfois appelé "cube" chez les vachequiritphiles.

2 Approche topologique

Nous allons voir un résultat étonnant. En dimension trois, la seule contrainte sur les solides platoniciens est une contrainte topologique :

1. De tout sommet part le même nombre d'arêtes.
2. Toute face possède le même nombre d'arête.
3. Le solide est homéomorphe à une sphère.

Finalement, une fois passées ces obstructions topologiques, les conditions métriques (toutes les arêtes ainsi que les faces sont isométriques) seront automatiquement vérifiées.

Définition 38 :
On note A le nombre d'arêtes d'un polyèdre, S le nombre de sommets et F le nombre de faces.

Définition 39 :
On appelle caractéristique d'Euler-Poincaré d'un polyèdre la quantité $\chi = S - A + F$.

Remarque :
On peut généraliser cette quantité à bon nombre d'espaces topologique.

Théorème 23 (de Descartes-Euler):
Tout polyèdre de genre 0 est de caractéristique d'Euler-Poincaré $\chi = 2$.

Remarque :
Le genre d'une surface connexe est le nombre maximum de courbes fermées simples qui ne se coupent pas pouvant être tracées à l'intérieur de cette surface sans qu'elle perde sa connexité si on la découpait le long de ces courbes. On peut le voir comme le nombre de "trous" sur cette surface. C'est un invariant topologique partiel (deux surfaces de genre différent ne peuvent pas être homéomorphes).
On se contentera de remarquer qu'un polyèdre convexe est de genre 0, d'où :

Corollaire 10 :
Tout polyèdre convexe vérifie $S - A + F = 2$.

Théorème 24 :
Il existe exactement cinq solides Platoniciens.

Démonstration :
Nous admettrons l'existence de cinq solides platoniciens et le fait qu'un solide platonicien est entièrement caractérisé par ses nombres A, S, F, p, q sous les contraintes topologiques :

$$\begin{cases} 2A = Sq & \text{car à chaque arête correspondent deux sommets } [13] \\ 2A = Fp & \text{car chaque arête est commune à deux faces} \\ S - A + F = 2 & \\ p \geq 3 & \text{car une face est définie à partir d'au moins trois arêtes} \\ q \geq 2 & \text{car aucun sommet n'est l'extrémité d'une arête seulement} \end{cases}$$

[13] Remarque : Plus précisément, ceci provient du fait que les polyèdres sont réguliers (tous les sommets ont même degré) et du lemme des poignées de mains : si l'on note d_i les degrés des sommets, on peut montrer que $2A = \sum_{i=1}^{S} d_i$.

Donc $\frac{2A}{q}+\frac{2A}{p}=2+A \iff \frac{1}{q}+\frac{1}{p}=\frac{1}{A}+\frac{1}{2}$

$$\overset{p\geq 3}{\Longrightarrow} \frac{1}{q}=\frac{1}{A}+\frac{1}{2}-\frac{1}{p}>\frac{1}{2}-\frac{1}{p}\geq\frac{1}{2}-\frac{1}{3}=\frac{1}{6}$$

$$\Longrightarrow q<6$$

Si $q=2$ alors $\frac{1}{2}+\frac{1}{p}=\frac{1}{2}+\frac{1}{A}\Longrightarrow p=A$ et on aurait dans ce cas qu'une seule face. Un polygone n'est pas un solide platonicien, donc $q\geq 3$ et par symétrie $p<6$.
D'où $3\leq p\leq 5$ et $3\leq q\leq 5$, on a ainsi toutes les possibilités du tableau.

□

Remarque :
Pour une construction métrique des solides platoniciens et donc une preuve complète du théorème, il faut ajouter aux contraintes la formule $\sin(\frac{\theta}{2})=\frac{\cos(\frac{\pi}{q})}{\sin(\frac{\pi}{p})}$ où θ est l'angle entre deux faces adjacentes. Sinon, on peut utiliser les preuves suggérées dans l'introduction.

3 Groupes d'isométries

Le groupe des isométries d'un objet "mesure" ses symétries (en plus d'avoir une structure de groupe).

Définition 40 :
Le groupe $\mathrm{Is}(X)$ *des isométries d'un objet* $X\subset\mathbb{R}^3$ *est le sous groupe des isométries de l'espace affine* $\mathbb{R}^3$ *qui stabilisent* X.

Il faut faire attention à ce que l'on dit quand on parle de groupe d'isométrie d'un solide platonicien puisque celui-ci a été défini à similitude près. On va voir que deux objets en similide ont le même groupe d'isométries (à isomorphisme près bien sûr) :

Proposition 57 :
Soit $\varphi\in GO(\mathbb{R}^3)$ *une similitude. Alors* $\mathrm{Is}(X)\simeq\mathrm{Is}\big(\varphi(X)\big)$.

Démonstration :
Soit $\begin{array}{ccc}\mathrm{Is}(X) & \longrightarrow & \mathrm{Is}\big(\varphi(X)\big)\\ g & \longmapsto & \varphi g\varphi^{-1}\end{array}$ morphisme bien défini car si $g\in\mathrm{Is}(X)$,

alors $\varphi g\varphi^{-1}\big(\varphi(X)\big)=\varphi\big(g(X)\big)=\varphi(X)$
or $\varphi g\varphi^{-1}=(\lambda\psi)g(\lambda\psi^{-1})=\psi g\psi^{-1}\in\mathrm{Is}(\mathbb{R}^3)$ car $\psi\in\mathrm{Is}(\mathbb{R}^3)$.
Ce morphisme est clairement injectif et surjectif.

□

Voici maintenant une proposition qui va d'une part ramener l'etude de $\mathrm{Is}(X)$ à celle de $\mathrm{Is}^+(X)$ (le sous-groupe des déplacements de $\mathrm{Is}(X)$), d'autre part ramener l'étude de $\mathrm{Is}^+(X)$ à l'étude de permutations de sommets. On commence pour cela par une définition[14] :

Définition 41 :
Soit $\mathcal{S}$ *un ensemble de points. L'enveloppe convexe* X *de* $\mathcal{S}$ *est l'ensemble des barycentres de* $\mathcal{S}$ *à coefficients positifs. Un point* S *de* X *est dit extrémal si* S *n'est pas barycentre à coefficients positifs de* $X\backslash\{S\}$.

[14]Il n'est pas totalement inutile de rappeler ici le théorème de Krein-Milman : Tout convexe compact d'un espace affine de dimension finie est enveloppe convexe de l'ensemble de ses points extrémaux.

Proposition 58 :
Soit $X \subset \mathbb{R}^3$.

(1) *Si* O *est centre de symétrie de* X *et* $g \in \mathrm{Is}(X)$, *alors* $g(O) = O$. *De plus,* $\mathrm{Is}(X) \simeq \mathrm{Is}^+(X) \times \mathbb{Z}/2\mathbb{Z}$.

(2) *Si* X *est fixé par une réflexion orthogonale, alors* $\mathrm{Is}(X) \simeq \mathrm{Is}^+(X) \ltimes \mathbb{Z}/2\mathbb{Z}$.

(3) *Si* $\mathcal{S}$ *est un ensemble fini de sommets et* X *l'enveloppe convexe de ces sommets. On suppose que les points de* $\mathcal{S}$ *sont extremaux, alors* $\mathrm{Is}(X)$ *stabilise* $\mathcal{S}$ *et en particulier l'isobarycentre de* $\mathcal{S}$.

retour p109

Démonstration :

(1) Puisque g conserve le centre de symétrie (tout élément de $GA_3(\mathbb{R})$ conserve le barycentre), il est clair que $g(O) = O$.
On a l'isomorphisme
$$\begin{array}{ccccc} \mathrm{Is}(X) & \longrightarrow & \mathrm{Is}^+(X) \times \mathbb{Z}/2\mathbb{Z} & & \\ g & \longmapsto & \begin{cases} (g,1) & \text{si } g \in \mathrm{Is}^+(X) \\ (gs_0, s_0) & \text{sinon, avec } s_0 \in \mathrm{Is}^-(X) \text{ symétrie centrale en } O \end{cases} \end{array}$$
s_0 commute avec tout élément de $\mathrm{Is}^+(X)$ (vectoriellement, il s'agit de l'homothétie de rapport -1), donc le produit est direct.

Remarque :
X possède un centre de symétrie $O \iff s_0 \in \mathrm{Is}(X)$.
Ainsi, puique le tétraèdre n'a pas de centre de symétrie, son groupe d'isométrie ne contient pas de symétrie centrale et $\mathrm{Is}(\Delta_4) \not\simeq \mathrm{Is}^+(\Delta_4) \times \mathbb{Z}/2\mathbb{Z}$. En effet, $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4 \simeq \mathfrak{A}_4 \ltimes \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Is}^+(\Delta_4) \ltimes \mathbb{Z}/2\mathbb{Z}$, le produit n'est pas direct.

(2) idem mais s_0 ne commute pas avec $\mathrm{Is}^+(X)$ donc le produit est semi-direct car Is^+ est distingué.

(3) $\mathrm{Is}(X)$ est dans $GA(\mathbb{R}^3)$, donc stabilise le barycentre. Donc si $g \in \mathrm{Is}(X)$, $S \in \mathcal{S}$, alors $g(S) \in \mathcal{S}$ par construction.

□

Exercice :
Montrer que

- si X est un triangle quelconque du plan, alors $\mathrm{Is}(X) \simeq \{1\}$.

- si X est un triangle isocèle, alors $\mathrm{Is}(X) \simeq \mathbb{Z}/2\mathbb{Z}$.

- si X est un triangle équilatéral, alors $\mathrm{Is}(X) \simeq \mathfrak{S}_3$ (puisque $\mathrm{Is}(X)$ stabilise aussi les sommets de X, ie. l'action est libre, on a $\mathrm{Is}(X) \subset \mathfrak{S}_3$; et puisque $\mathrm{Is}(X)$ contient tous ses générateurs, on conclut).
  Remarque : par définition, $\mathfrak{S}_n \simeq \mathfrak{A}_n \ltimes \mathbb{Z}/2\mathbb{Z}$, mais $\mathfrak{S}_2$ et $\mathfrak{S}_3$ sont aussi des produits directs.

- plus généralement, si X est un polygone régulier à n côtés alors $\mathrm{Is}(X) \simeq D_n \simeq \mathbb{Z}/n\mathbb{Z} \ltimes \mathbb{Z}/2\mathbb{Z}$.
  On remarque bien sûr que $\mathfrak{S}_3 \simeq D_3$.

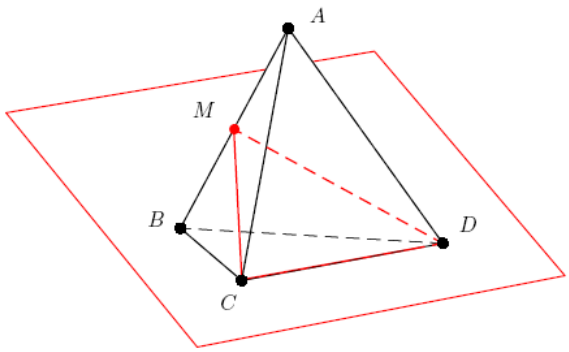
L'oscar de la symétrie revient bien sûr au cercle :

- si X est un cercle, alors $\mathrm{Is}^+(X) \simeq S^1$ et $\mathrm{Is}(X) \simeq S^1 \times \mathbb{Z}/2\mathbb{Z}$. Ici, Is^+ est carrément un groupe de Lie.

Proposition 59 :
Groupes d'isométries du tétraèdre :
$$\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4 \quad \textit{et} \quad \mathrm{Is}^+(\Delta_4) \simeq \mathfrak{A}_4$$

Démonstration :
On fait agir $\mathrm{Is}(\Delta_4)$ sur $\mathcal{S} = \{A, B, C, D\}$ l'ensemble des sommets du tétraèdre par la proposition précédente.
Ainsi $\varphi : \begin{array}{ccc} \mathrm{Is}(\Delta_4) & \longrightarrow & \mathfrak{S}_4 \\ g & \longmapsto & g_{|\mathcal{S}} \end{array}$ est un morphisme de groupes

L'action est libre car si $\varphi(g) = \mathrm{id}_{\mathcal{S}}$, alors g stabilise $\mathcal{S}$ qui est un repère de l'espace affine d'où $g = \mathrm{id}_{\mathbb{R}^3}$.
Donc $\mathrm{Is}(\Delta_4) \subset \mathfrak{S}_4$.
De plus, la réflexion par rapport au plan MCD avec M milieu de AB réalise la transposition $(A\,B)$:



Donc toutes les tranpositions sont dans $\mathrm{Is}(\Delta_4)$ et a fortiori tout $\mathfrak{S}_4 \subset \mathrm{Is}(\Delta_4)$.
Donc finalement, φ est un isomorphisme et $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.

$\mathrm{Is}^+(\Delta_4)$ étant d'indice 2 dans $\mathrm{Is}(\Delta_4)$, on a aussi $\mathrm{Is}^+(\Delta_4) \simeq \mathfrak{A}_4$.

□

Proposition 60 :
Groupe d'isométries directes du cube : $\mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4$.
Groupe d'isométries du cube : $\mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration :
On fait agir $\mathrm{Is}^+(C_6)$ sur $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube.
Ainsi

$$\varphi : \begin{array}{ccc} \mathrm{Is}^+(C_6) & \longrightarrow & \mathfrak{S}_4 \\ g & \longmapsto & g_{|\mathcal{D}} \end{array}$$ est un morphisme de groupes car les distances sont conservées

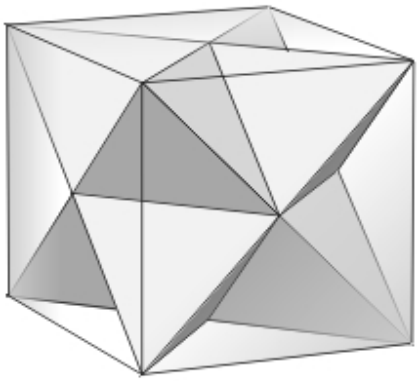
L'action est libre car si $\varphi(g) = \mathrm{id}_{\mathcal{D}}$, alors en notant $D_i = A_iG_i$, $\begin{cases} g(A_i) = A_i \\ g(G_i) = G_i \end{cases}$ et $g = \mathrm{id}_{\mathbb{R}^3}$ ou bien $\begin{cases} g(A_i) = G_i \\ g(G_i) = A_i \end{cases}$
et $g = s_0$ la symétrie centrale en O ce qui est impossible puisque $g \in \mathrm{Is}^+(C_6)$. Donc $\mathrm{Ker}(\varphi) = \{\mathrm{id}_{\mathbb{R}^3}\}$ et l'action est bien libre : $\mathrm{Is}^+(C_6) \subset \mathfrak{S}_4$.

Comme dans la démonstration précédente, on peut voir que les transpositions sont toutes réalisées (ici grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales), et donc que $\mathrm{Is}^+(C_6) \simeq \mathfrak{S}_4$. La seconde assertion est claire car le cube admet un centre de symétrie, cf proposition 58.

□

Au milieu des solides relations entre algèbre et géométrie, on peut remarquer que la suite exacte $(*)$ et la figure ci-dessous sont très liées :

Dans un cube, on peut inscrire deux tétraèdres T_1 et T_2 inscrits, de sommets distincts :



$\mathrm{Is}(C_6)$ agit sur $\{T_1, T_2\} \simeq \mathbb{Z}/_{2\mathbb{Z}}$ et le noyau de l'action est exactement le stabilisiteur du tétraèdre :

$$1 \longrightarrow \mathrm{Is}(\Delta_4) \hookrightarrow \mathrm{Is}(C_6) \twoheadrightarrow \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow 1 \qquad (*)$$

D'où, en particulier, $\mathrm{Is}(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/_{2\mathbb{Z}}$, puisque $\mathrm{Is}(\Delta_4) \simeq \mathfrak{S}_4$.

Remarque :
On peut resteindre l'action et obtenir la suite exacte :

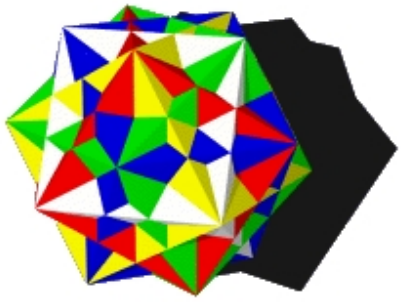
$$1 \longrightarrow \mathrm{Is}^+(\Delta_4) \hookrightarrow \mathrm{Is}^+(C_6) \underset{s}{\overset{\epsilon}{\rightleftarrows}} \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow 1$$

dont la section continue est aussi un morphisme d'où le produit semi-direct $\mathrm{Is}^+(C_6) \simeq \mathrm{Is}^+(\Delta_4) \ltimes \mathbb{Z}/_{2\mathbb{Z}}$
$\iff \mathfrak{S}_4 \simeq \mathfrak{A}_4 \ltimes \mathbb{Z}/_{2\mathbb{Z}}$

Proposition 61 :
Groupes d'isométries du dodécaèdre :

$$\mathrm{Is}(P_{12}) \simeq \mathfrak{A}_5 \times \mathbb{Z}/_{2\mathbb{Z}} \quad \textit{et} \quad \mathrm{Is}^+(P_{12}) \simeq \mathfrak{A}_5$$

Démonstration :
On admet que cinq cubes distincts sont inscrits dans le dodécaèdre :



$\mathrm{Is}^+(P_{12})$ agit sur $\mathcal{C} = \{C_1, C_2, C_3, C_4, C_5\}$ l'ensemble des cubes inscrits d'où le morphisme $\mathrm{Is}^+(P_{12}) \longrightarrow \mathfrak{S}_5$.
Soit g tel que $g(C_i) = C_i$. Alors $g = \mathrm{id}_{\mathbb{R}^3}$ (car il fixe les grandes diagonales du dodécaèdre et n'est pas une symétrie centrale) d'où l'action est libre et $\mathrm{Is}^+(P_{12}) \subset \mathfrak{S}_5$.
Or, combien y a-t-il d'éléments de $\mathrm{Is}^+(P_{12})$? Comme ce sont des rotations, on va compter les axes possibles, puis les angles possibles.

Axe de sommet à sommet opposé. $\frac{20}{2} = 10$ axes possibles, les angles (non nuls) $\frac{2\pi}{3}$, $\frac{4\pi}{3}$.

Axe de milieu d'arête à milieu d'arête opposée. $\frac{30}{2} = 15$ axes possibles, les angles (non nuls) π.

Axe de sommet à sommet opposé. $\frac{12}{2} = 6$ axes possible, les angles (non nuls) $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$.

Et l'identité, bien sûr !
En tout, cela nous fait $10 \times 2 + 15 \times 1 + 6 \times 4 + 1 = 60$ éléments. Le compte est bon et $\mathrm{Is}^+(P_{12}) = \mathfrak{S}_5$.

Enfin, le dodécaèdre ayant un centre de symétrie, on conclut à l'aide de la proposition 58 que $\mathrm{Is}(P_{12}) \simeq \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$.

□

4 La "toy" dualité

Nous allons définir une notion de dualité adaptée à la situation des polyèdres réguliers convexes de $\mathbb{R}^3$. C'est une dualité de pacotille, qui va juste nous permettre de comprendre ce que l'on a besoin de comprendre dans l'immédiat, mais avec laquelle on ne va pas bien loin. On l'appellera "toy dualité" ou "dualité Fisher price" pour la distinguer de la vraie dualité chez les ensembles compacts convexes de $\mathbb{R}^n$.
Pour le lecteur assidu, voire le candidat à l'agreg, nous parlerons de cette dualité plus profonde en appendice. Nous y généraliserons les propriétés étudiées et nous verrons pourquoi la "toy dualité" en est un cas particulier.

Définition 42 :
Soit X un solide convexe. On définit son dual X^* par :

$$S^* = F, \quad F^* = S, \quad A^* = A, \quad q^* = p, \quad p^* = q$$

Si X est un solide Platonicien, alors $X^{**} = X$.

Proposition 62 :
Soit X un solide Platonicien. Alors $\mathrm{Is}(X^*) \simeq \mathrm{Is}(X)$.

Démonstration :

$\boxed{\Longleftarrow}$ Soit $g \in \mathrm{Is}(X)$. Alors g fixe les sommets de X^* puisqu'il préserve le barycentre. Donc $\mathrm{Is}(X) \subset \mathrm{Is}(X^*)$.
$\boxed{\Longrightarrow}$ Par dualité, $\mathrm{Is}(X^*) \subset \mathrm{Is}(X^{**}) \simeq \mathrm{Is}(X)$.

□

Définition 43 :
Soit X un solide convexe. On peut aussi définir son dual X^* par : $X^* = \{v \in \mathbb{R}^3 \ : < u, v > \leq 1, \ \forall u \in X\}$.

C'est une dualité qui tient la route. Il est conseillé de regarder en annexe les propriétés de cette dualité qui a pour cas particulier la "toy dualité" dans le cadre des polyèdres réguliers convexes.

5 Sous-groupes de Sylow d'un groupe d'isométries.

Les groupes d'isométries des solides platoniciens ont l'avantage d'avoir des p-Sylow "visibles à l'oeil nu". Voici quelques exemples temoins de l'interaction omniprésente entre groupes et géométrie :

Exemple :
Combien $\mathcal{A}_4$ possède-t-il de 3-Sylow ?
Bien sûr, nous avons la méthode arithmétique qui consiste à regarder les valeurs possibles 1,4, et à éliminer selon des considérations plus ou moins orthodoxes. Mais ici, nous pouvons utiliser une méthode algébrique puisque $\mathcal{A}_4$ se réalise comme groupe d'isométries directes du tétraèdre. Comme ses 3-Sylow ont pour ordre 3, ce sont des rotations d'ordre 3 et la seule possibilité est la rotation autour d'un axe passant par le milieu des faces. Il y a donc 4 3-Sylow correspondant aux 4 faces d'un tétraèdre.

Exemple :
Combien $\mathcal{S}_4$ possède-t-il de 3-Sylow ?
Même méthode, mais cette fois-ci le groupe $\mathcal{S}_4$ se réalise comme groupe d'isométrie directe de deux manières : celui du cube et celui de l'octaèdre. Il semble que visuellement, c'est en tant que groupe de l'octaèdre qu'on verra le mieux les 3-Sylow car ils sont en bijection avec ses paires de faces opposées (triangulaires).

Exemple :
Combien $\mathcal{A}_5$ possède-t-il de 3-Sylow ?
Réponse : 10 correspondant aux paires de faces opposées de l'icosaèdre.

Exemple :
Combien $\mathcal{A}_5$ possède-t-il de 5-Sylow ?
Réponse : 6 correspondant aux paires de faces opposées du dodécaèdre.

Exercice :
Combien $\mathcal{S}_4$ possède-t-il de 2-Sylow ?
Réponse : 3. Pourquoi ? (géométriquement bien sûr).

6 Annexe 9 : Dualité des ensembles compacts convexes de $\mathbb{R}^n$.

« Je suis votre miroir la belle, reflechissez pour moi, je reflechirai pour vous »

La Belle et la Bête, Jean Cocteau, 1946.

Pour cette section, on peut se référer au [Fresnel, Méthodes modernes en géométrie, 5.1, 5.2] ou aux exercices partiellement corrigés dans le [Audin, Géométrie, Exercices IV 27, IV 28, IV 29, IV 30]. On commence par un mini-Hahn-Banach (dans le sens qu'on est en dimension finie). Dans la suite, les espaces vectoriels seront munis de leur structure affine canonique.

Proposition 63 :
Soit C un convexe compact d'un espace vectoriel euclidien E et soit A un point hors de C. Alors, la fonction qui à tout point M de C associe sa distance $d(A,M)$ possède un minimum $d>0$ pour un point M_0 de C.
Soit $\mathcal{H}$ l'hyperplan affine défini par

$$\mathcal{H} := \{M \in E,\ \overrightarrow{AM} \cdot \overrightarrow{AM_0} = \frac{d^2}{2}\}.$$

Alors A est dans un des demi-espaces ouverts défini par $\mathcal{H}$ et C est dans l'autre.

Démonstration :
L'existence d'une distance minimum vient de la compacité de C et de l'existence du minimum (atteint !) d'une fonction continue sur un compact[15]. Cette distance est strictement positive puisque sinon, on aurait $A \in C$, ce qui est contraire à l'hypothèse.
Montrons la dernière assertion. On note

$$\mathcal{H}^+ := \{M \in E,\ \overrightarrow{AM} \cdot \overrightarrow{AM_0} > \frac{d^2}{2}\}, \qquad \mathcal{H}^- := \{M \in E,\ \overrightarrow{AM} \cdot \overrightarrow{AM_0} < \frac{d^2}{2}\}$$

les deux demi-espaces ouverts définis par $\mathcal{H}$. Clairement, A est dans $\mathcal{H}^-$.
Montrons par l'absurde que C est inclus dans $\mathcal{H}^+$. Pour cela supposons qu'un point M_1 de C soit dans $\mathcal{H}^-$ et posons $k := \overrightarrow{AM_1} \cdot \overrightarrow{AM_0} < \frac{d^2}{2}$. Alors, la fonction $h(M) := \overrightarrow{AM} \cdot \overrightarrow{M_1M_0}$ est continue sur le segment $[MM_0]$ qui est inclus dans C. Comme

$$h(M_1) = \overrightarrow{AM_1} \cdot \overrightarrow{M_1M_0} = \overrightarrow{AM_1} \cdot (\overrightarrow{M_1A} + \overrightarrow{AM_0}) = k + AM_1^2 < -\frac{d^2}{2},$$

et comme

$$h(M_0) = \overrightarrow{AM_0} \cdot \overrightarrow{M_1M_0} = \overrightarrow{AM_0} \cdot (\overrightarrow{M_1A} + \overrightarrow{AM_0}) = -k + d^2 > \frac{d^2}{2}$$

il résulte l'existence d'un point H dans le segment (donc dans C) tel que $h(M) = 0$. Par Pythagore, $AM_0^2 = AH^2 + HM_0^2$, donc $AH < AM_0$ ce qui est impossible.

□

Voici maintenant une notion plus sérieuse, et surtout plus maniable, de dualité :

Définition 44 :
Soit C un convexe de E. On définit son dual

$$C^* := \{u \in E,\ u \cdot v \leq 1,\ \forall v \in C\}.$$

On peut bien sûr transposer ce dual dans E^* via la forme euclidienne et ainsi voir C^* dans le dual de E.

Proposition 64 :
Soit C un convexe de E.

1. *C^* est convexe.*
2. *Si C contient 0 dans son intérieur, alors C^* est compact.*
3. *Si C est compact avec 0 en son intérieur, alors $(C^*)^* = C$.*

Démonstration :

1. C^* est une intersection de demi-espaces fermés donc est un convexe fermé.
2. Posons ϵ tel que la boule ouverte $B(O, \epsilon)$ de centre O et de rayon ϵ est incluse dans C. Montrons alors que $C^* \subset B(O, \frac{1}{\epsilon})$.
   En effet, soit $u \in C^*$, alors en particulier, $u \cdot v \leq 1$, $\forall v \in B(O, \epsilon)$. Posons $v := \epsilon \frac{u}{||u||}$, alors $u \cdot \epsilon \frac{u}{||u||} \leq 1$. Donc, en prenant la norme, on obtient $|| u || \leq 1$. C^* est donc fermé borné, donc compact.

[15] D'ailleurs la convexité implique l'unicité de M_0. Laissé en exercice.

3. Il est clair par construction que $C \subset (C^*)^*$. Montrons l'inclusion inverse par la contraposée.
   Soit $a \notin C$, montrons que $a \notin (C^*)^*$. Soit $\mathcal{H}$ un hyperplan séparant a et C come dans la proposition précédente. Alors, $O \notin \mathcal{H}$ et on peut donc trouver x_0 tel que $\mathcal{H} = \{x, < x_0, x >= 1\}$. Tout x de C vérifie $< x_0, x >< 1$, et de plus, on a $< x_0, a >> 1$ par construction. La première inégalité prouve que $x_0 \in C^*$ et la seconde que $a \notin (C^*)^*$, qui était la proposition voulue.

□

Comme on l'a vu dans la section sur la "toy dualité", il est intéressant de constater que les groupes d'isométries de deux compacts convexes duaux sont isomorphes, et même égaux !

Proposition 65 :
Soit C un compact convexe de $\mathbb{R}^n$, alors

$$\mathrm{Is}(C) = \mathrm{Is}(C^*).$$

Démonstration :
Soit u dans $GL_n(\mathbb{R})$, alors $u(C)$ est un compact convexe et on montre facilement que $(u(C))^* = (u^*)^{-1}(C^*)$. Donc si $u \in O(n)$, il vient $u(C)^* = u(C^*)$. Ceci implique que $\mathrm{Is}(C) = \mathrm{Is}(C^*)$.

□

Il reste enfin à montrer que cette dualité est bien une généralisation de celle que nous avons utilisé sur les polyèdres réguliers convexes de $\mathbb{R}^3$.

Proposition 66 :
Soit P un polyèdre convexe régulier de $\mathbb{R}^3$ de centre O. Notons C_i, pour $1 \leq i \leq f$, les centres de ses faces et soit P' l'enveloppe convexe des C_i. Supposons $OC_i = 1$ pour tout i. Alors, $P^* = P'$.

Démonstration :
Comme $OC_i^2 = 1$, les faces de P ont pour équation $\overrightarrow{OM} \cdot \overrightarrow{OC_i} = 1$ pour tout i,
donc $P = \{M, \overrightarrow{OM} \cdot \overrightarrow{OC_i} \leq 1, 1 \leq i \leq f\}$.
Maintenant, le dual de P' est donné par l'inéquation $\overrightarrow{OM} \cdot \overrightarrow{ON} \leq 1$ pour tout N dans P',
et donc $\overrightarrow{OM} \cdot (\sum_i \lambda_i \overrightarrow{OC_i}) \leq 1$ pour tout f-uplet de λ_i positifs. Ce qui revient à dire $\overrightarrow{OM} \cdot \overrightarrow{OC_i} \leq 1$ pour tout i.
On obtient donc par ce qui précède $P = (P')^*$ et comme P' est compact avec O en son intérieur : $P^* = ((P')^*)^* = P'$ comme demandé.

□

Géométrie, Chap. IV, Michèle Audin, **Belin**.
Pour la dualité (la vraie et la toy !) :
Méthodes modernes en géométrie, 5.1, 5.2, Jean Fresnel, **Hermann**.
Géométrie, Exercices IV-27-28-29-30, Michèle Audin, **Belin**.

Annexe 10 : Formes quadratiques

On peut définir une forme quadratique sur tout corps, y compris de caractéristique 2 via une théorie spéciale, mais leur classification est différente.

Définition 45 :
Une forme quadratique est un polynôme homogène de degré 2 *en les coefficients d'un vecteur dans une certaine base. Exemple :* $q(u) = x^2 + y^2$ *avec* $u = \left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ *dans la base canonique* [16] *de* $\mathbb{R}^2$.

Définition 46 :
L'application qui à un vecteur de E *associe une de ses coordonnées est appelée forme linéaire coordonnée, c'est un élément de l'espace dual* E^*.
Remarque : toute forme linéaire non nulle est une forme coordonnée.

Exemple :
Soit E un $\mathbb{K}$-espace vectoriel de dimension n, et $f \neq 0$ un élément de E^*.
Alors $f_1 := f$ se complète en une base $(f_1, f_2, \cdots, f_n)$ de E^* d'où $(f_1^*, f_2^*, \cdots, f_n^*)$ forme une base de $E^{**} = E$.
Dans cette base, f_1 est la forme coordonnée qui à un vecteur de E (dans cette base) associe sa première coordonnée.

Exercice :
Soient $f, g \in E^*$ non proportionelles et $u \in E$. Montrer que $q(u) = f(u)g(u)$ est une forme quadratique et déterminer son rang.

Solution : (f, g) formant un système libre de E^*, on peut le compléter en une base $(l_1, l_2, \cdots, l_n)$ de E^*, avec $l_1 := f$ et $l_2 := g$.
Dans la base duale $(l_i^*)_{1 \leq i \leq n}$, on a $f(u) = f(x_1 l_1^* + \cdots + x_n l_n^*) = l_1(x_1 l_1^* + \cdots + x_n l_n^*) = x_1$
De même, $g(u) = l_2(x_1 l_1^* + \cdots + x_n l_n^*) = x_2$, donc $q(u) = x_1 x_2 = \frac{1}{4}\left[(x_1 + x_2)^2 - (x_1 - x_2)^2\right]$ de rang 2 car $(x_1 + x_2, x_1 - x_2)$ est libre.

$\frac{1}{2}\left[(x_1 + x_2)^2 - x_1^2 - x_2^2\right]$ est de rang 2 et non pas 3 car $(x_1 + x_2, x_1, x_2)$ est lié.

Proposition 67 :
Puisque chaque forme quadratique peut être associée à une unique forme bilinéaire symétrique, leurs classifications sont les mêmes :
- *Sur* $\mathbb{C}$ *le rang,*
- *sur* $\mathbb{R}$ *le rang et la signature,*
- *sur* $\mathbb{F}_q$ *le rang et le discriminant* δ *(voir chapitre IV).*

[16] On écrira $q(x, y)$ au lieu de $q(\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right])$.

Exemple :
les deux formes quadratiques $q(a,b) = a^2 - b^2$ et $q'(a,b) = (a-b)(a+b)$,
qui peuvent être réécrites $q(x,y) = x^2 - y^2$ et $q(x,y) = xy$ dans une autre base, sont égales :

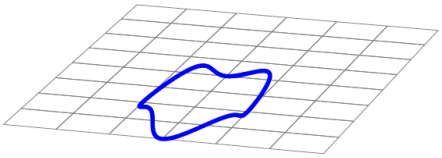
- sur $\mathbb{C}$ car $\mathrm{rg}(q) = \mathrm{rg}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = 2 = \mathrm{rg}\begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} = \mathrm{rg}(q')$,
- sur $\mathbb{R}$ car toutes deux de signature $(1,1)$,
- sur $\mathbb{F}_q$ car $\delta(q') = \left(\frac{-\xi^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\xi^2}{p}\right) = \left(\frac{-1}{p}\right) = \delta(q)$.

Exemple :
De même, les deux formes quadratiques $q(a,b) = a^2+2ab+b^2$ et $q'(a,b) = (a+b)^2$, qui peuvent être réécrites $q(x,y) = x^2 + 2xy + y^2$ et $q(x,y) = x^2$ dans une autre base, sont égales :

- sur $\mathbb{C}$ car $\mathrm{rg}(q) = \mathrm{rg}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = 1 = \mathrm{rg}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \mathrm{rg}(q')$,
- sur $\mathbb{R}$ car toutes deux de signature $(1,0)$,
- sur $\mathbb{F}_q$ car $\delta(q') =? = \delta(q)$.

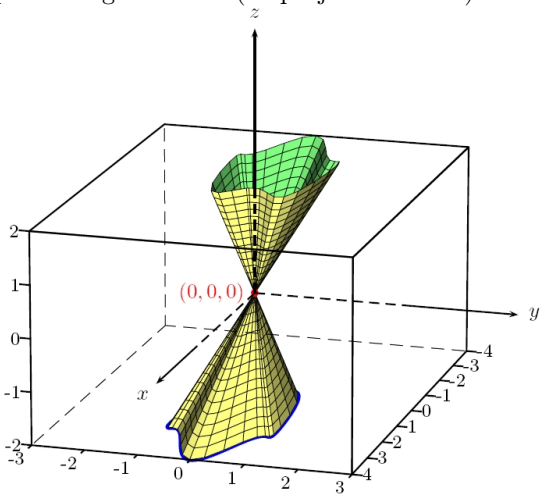
1 Classification en dimension 2

Soit la forme quadratique $q(x,y) = ax^2 + by^2 + 2cxy + 2dx + 2ey + f$. On veut étudier et classifier les solutions dans $\mathbb{R}^2$ de $q(x,y) = 0$:



Attention ! image non contractuelle

Tout d'abord, on regarde le cône d'équation $q\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^2 = aX^2 + bY^2 + 2cXY + 2dXZ + 2eYZ + fZ^2$ engendré dans $\mathbb{R}^3$ par homogénéisation (en projetant sur $\mathbb{P}^2$) :



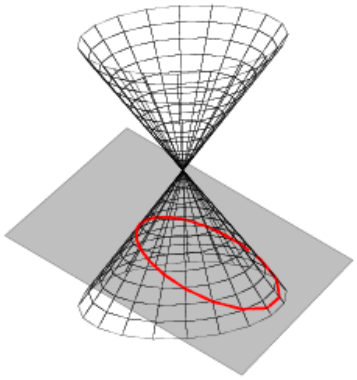
Attention ! image non contractuelle

Ensuite, on regarde la signature de la forme quadratique dans $\mathbb{R}^3$ si celle-ci est non-dégénérée,

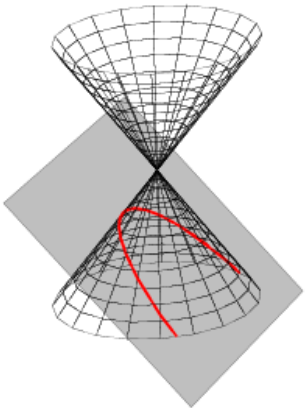
ie. si $\det A = \begin{vmatrix} a & c & d \\ c & b & e \\ d & e & f \end{vmatrix} \neq 0$.

Si q est de signature $(3,0)$ ou $(0,3)$ (les deux étant équivalentes car le polynôme homogénéisé est symétrique, et $A \equiv I_3$), alors c'est terminé puisqu'elle équivaut à un changement de base près à $q(u,v,w) = u^2+v^2+w^2$ qui n'a pas de solution non triviale, $S = \{(0,0,0)\}$.
On rappelle qu'un tel changement de base est possible par l'action $\begin{array}{ccc} GL_3(\mathbb{R}) \times \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ (P, \begin{bmatrix} x \\ y \\ z \end{bmatrix}) & \longmapsto & \begin{bmatrix} u \\ v \\ w \end{bmatrix} = {}^tP^{-1} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \end{array}$

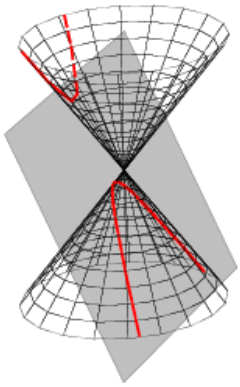
Si q est de signature $(2,1)$ ou $(1,2)$ cad $A \equiv \begin{bmatrix} 1 & & \\ & 1 & \\ & & -1 \end{bmatrix}$, alors elle équivaut à un changement de base près au cône $q(u,v,w) = u^2+v^2-w^2$ dont les solutions sont bien cônnues :
Ce sont les intersections du cône avec un plan quelconque (qui ne passe pas par le sommet).



Ellipse



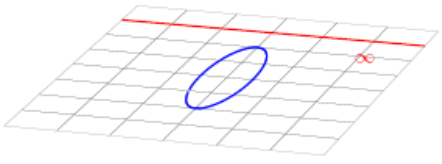
Parabole



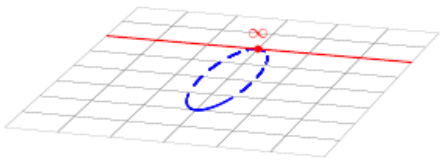
Hyperbole

Remarque :
Puisqu'on a projeté la forme sur $\mathbb{P}^2$, le changement de base correspond à l'action de $PGL_3(\mathbb{R})$ sur $\mathbb{P}^2$ et il est donc normal que la classification ne distingue pas hyperbole et ellipse.

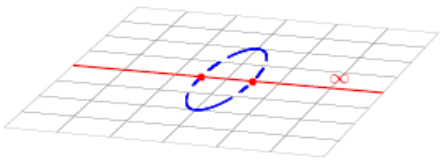
Pour obtenir la classification habituelle, on fait agir $GA_2(\mathbb{R})$ sur $\mathbb{A}^2$. Dans ce cas c'est au contraire si on la projette sur $\mathbb{P}^2$ que l'on ne distingue plus les coniques, leur seule différence étant le nombre d'intersections avec la droite infinie :



ellipse



parabole



hyperbole

Raffinons encore cette classification :
On veut connaître les propriétés métriques de chaque ensemble solution. Pour cela, il faut faire agir le groupe des isométries $\mathrm{Is}(\mathbb{R}^2)$ pour obtenir une classification plus fine.

Par exemple dans l'espace vectoriel $\mathbb{R}^3$, quelles sont les propriétés de l'ensemble solution de l'équation $Y^2 = XZ$?

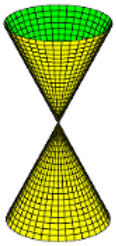
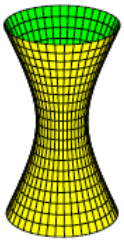
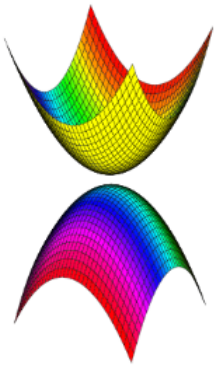
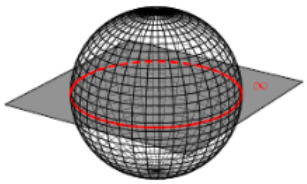
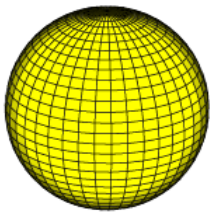
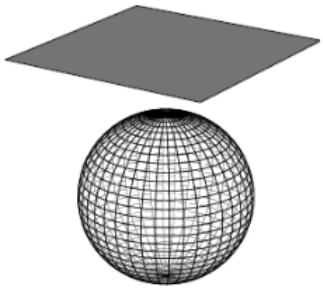
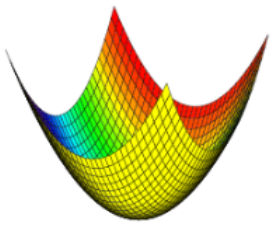
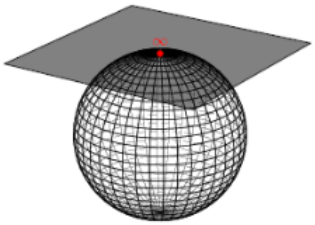
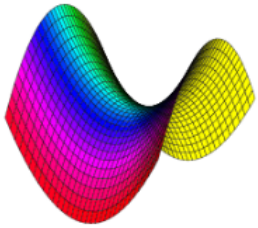
Il s'agit d'une forme quadratique dont la forme bilinéaire symétrique associée à pour matrice $A = \begin{bmatrix} 0 & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \\ -\frac{1}{2} & 0 & 0 \end{bmatrix}$ A étant semblable à la matrice $\begin{bmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{2} \end{bmatrix}$ elle est donc congruente à la matrice $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ et ainsi de rang 3 et de signature $(2, 1)$.

Par un changement de variable linéaire $V = Y, \quad U = \frac{X-Z}{2}, \quad W = \frac{X+Z}{2}$, on obtient $U^2 + V^2 - W^2 = 0$. Ainsi l'ensemble solution est un cône à action de $GL_3(\mathbb{R})$ près. On veut maintenant le comprendre à $O(3)$ près.

Rappel :
Toute matrice symétrique réelle d'un espace euclidien est diagonalisable en base orthonormée. Autrement dit, toute matrice de symétrique réelle est semblable (ou congrue puisque c'est la même chose dans une base orthonormée car $P \in O(n) \iff {}^tP = P^{-1}$) à une matrice diagonale.

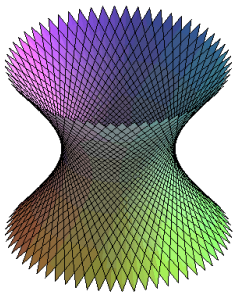
Ainsi une telle matrice diagonale nous donnera le cône isométrique au cône solution. Dans notre exemple, il s'agit de $\begin{bmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{2} \end{bmatrix}$ d'où le cône $\frac{1}{2}U^2 + V^2 - \frac{1}{2}W^2 = 0$.

2 Classification en dimension 3

Point de vue affine		Point de vue projectif	
$X^2+Y^2-W^2=0$ Cône		dégénéré	
$X^2+Y^2-W^2=1$ Hyperboloïde		signature $(2,2)$	
$X^2+Y^2-W^2=-1$ Hyperboloïde à 2 nappes		signature $(1,3)$ ou $(3,1)$	
$X^2+Y^2+W^2=1$ Sphère		signature $(1,3)$ ou $(3,1)$	
$X^2+Y^2-W=0$ Paraboloïde		signature $(1,3)$ ou $(3,1)$	
$X^2-Y^2-W=0$ Paraboloïde hyperbolique		signature $(2,2)$	

3 Etude de l'hyperboloïde

Il existe une famille $\mathcal{L} = \mathcal{L}_1 \sqcup \mathcal{L}_2$ de droites affines solutions de l'équation $X^2 + Y^2 - W^2 - 1 = 0$:



Ces droites affines correspondent à des plans vectoriels de $\mathbb{R}^4$.
Après homogénéisation, la forme devient $q(X, Y, W, Z) = X^2 + Y^2 - W^2 - Z^2$ et on cherche la famille $\mathcal{L}$ des plans P tels que $q_{|P} \equiv 0$.

Proposition 68 :
Soit F un sous-espace vectoriel de $\mathbb{R}^n$ tel que $q_{|F} \equiv 0$ (on appelle F un sous-espace totalement isotrope ou SETI). Alors $\dim F \leq \frac{n}{2}$.

Démonstration :

$$\begin{aligned} q_{|F} \equiv 0 &\implies \operatorname{mat} q_{|F} = 0_4 \\ &\implies F \subset F^\perp \\ &\implies \dim F \leq \dim F^\perp = n - \dim F \\ &\implies \dim F \leq \tfrac{n}{2} \end{aligned}$$

□

Dans notre cas, $\mathbb{R}^4$, les sous-espaces F sont donc de dimension ≤ 2. Les plans P existent car :

Proposition 69 :
Soit q une forme quadratique et F un sous-espace de $\mathbb{R}^n$ totalement isotrope (SETI).
Alors il existe des sous-espaces totalement isotropes maximaux (donc de dimension $\frac{n}{2}$) appelés Lagrangiens (l'ensemble $\mathcal{L}$ des Lagrangiens n'est pas nul).

Démonstration :
Laissé en exercice.

□

Remarque :
Les Lagrangiens viennent toujours par paires. Ici, on a $\begin{bmatrix} 0 & 0 & 1 & \\ 0 & 0 & & 1 \\ 1 & & 0 & 0 \\ & 1 & 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}$ où chaque bloc nul correspond à un Lagrangien (on rappelle que la matrice de droite est celle de la forme bilinéaire symétrique associée à q).

Proposition 70 :
$O(p, q)$ agit transitivement sur l'ensemble $\mathcal{L}$ des Lagrangiens de $\mathbb{R}^n$.

Démonstration :
Soient $F, F' \in \mathcal{L}$ deux Lagrangiens de $\mathbb{R}^n$. On a $\dim F = \dim F' = \frac{n}{2}$.

$\forall f \in F, \quad q(g \cdot f) = q(f) = 0$ d'où $q_{|_{g(F)}} \equiv q_{|_F} \equiv 0$. Donc tout isomorphisme linéaire de F dans F' est une isométrie. Ainsi, d'après le théorème de Witt (théorème 14) il existe $\tilde{\sigma} \in O(p,q)$ telle que $\tilde{\sigma}(F) = F'$ et l'action est bien transitive.

□

Remarque :
Dans notre cas, on en conclut que $\mathcal{L} \simeq O(2,2) \diagup \mathrm{Stab}_{O(2,2)}(F)$.
De plus, comme $\mathcal{L}$ est fermé et inclu dans $Gr_{2,4}(\mathbb{R})$ qui est compact, on peut munir l'espace (homogène) des Lagrangiens d'une topologie compacte.
Avec $\mathrm{Stab}_{O(2,2)}(F) = \{g \in O(2,2) \ : \ g \cdot F = F\}$

$$= \{ \begin{bmatrix} A & C \\ 0 & D \end{bmatrix} \ : \ \begin{bmatrix} A & C \\ 0 & D \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} {}^tA & 0 \\ {}^tC & D \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ A, D \in GL_2(\mathbb{R}), \ C \in M_2(\mathbb{R}) \}$$

$$= \{ \begin{bmatrix} A & C \\ 0 & D \end{bmatrix} \ : \ A\,{}^tC + CA = 0, \ A, D \in \mathcal{S}_2(\mathbb{R}) \cap GL_2(\mathbb{R}), \ C \in M_2(\mathbb{R}) \}$$

Proposition 71 :
L'espace $\mathcal{L}$ des Lagrangiens de $\mathbb{R}^n$ est compact de dimension $\frac{n(n-1)}{2}$ et possède 2 composantes connexes.

Démonstration :
C'est l'examen de GCG de 2009...

□