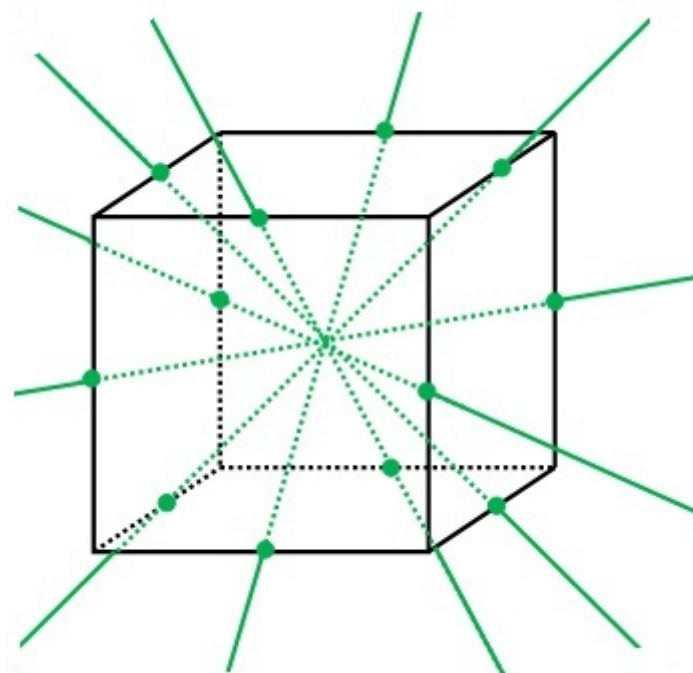


Université Grenoble Alpes

Rapport de TER

Groupe des rotations de l'espace euclidien et quelques sous-groupes.



Baptiste Lambert

Tuteur :
Mme. Garotta

Année 2018-2019

Table des matières

1	Propriétés de base du groupe SO_3	2
1.1	Engendrement, connexité, non commutativité	2
1.2	Simplicité et action sur la sphère unité	3
2	Sous-groupes finis de SO_3	4
2.1	Groupe Diédral	5
2.2	Groupe des isométries du tétraèdre régulier.	6
2.3	Groupe des isométries du cube.	7
2.4	Groupe des isométries de l'icosaèdre.	8
2.5	Classification des sous-groupes finis.	11
2.6	Application : des caractères irréductibles de \mathfrak{A}_4 , \mathfrak{S}_4 et \mathfrak{A}_5	16
3	Sous-groupes infinis engendrés par deux rotations	17
3.1	Paradoxe de Hausdorff ou paradoxe de la sphère	17

Introduction

Dans l'espace euclidien de dimension 3, il est possible de classer tous les sous-groupes finis du groupe spécial orthogonal, appelé aussi groupe des rotations, grâce à l'étude des isométries laissant invariant un polygone ou un polyèdre régulier.

Nous verrons par ailleurs que l'action du groupe des rotations sur la sphère unité donne lieu à un paradoxe dit de Hausdorff.

1 Propriétés de base du groupe SO_3

1.1 Engendrement, connexité, non commutativité

La première étape de cette étude consistera à mieux appréhender le groupe des rotations, en cherchant les éléments qui l'engendrent. On pourra alors exhiber plusieurs propriétés intéressantes.

Définition 1. Soit E un espace vectoriel de dimension n , ($n \geq 3$). On appelle un retournement une symétrie orthogonale par rapport à un sous espace vectoriel de E de dimension $n - 2$.

Définition 2. Soit E un espace vectoriel de dimension n , ($n \geq 3$). Une réflexion orthogonale est une symétrie orthogonale par rapport à un sous espace vectoriel de dimension $n - 1$ - c'est à dire par rapport à un hyperplan-.

Remarque :

En dimension 3, les retournements sont les rotations d'angle π et les réflexions sont les symétries orthogonales par rapport à des plans, de déterminant -1 .

Théorème 1. Le groupe $O_3(\mathbb{R})$ est engendré par les réflexions orthogonales et le groupe $SO_3(\mathbb{R})$ est engendré par les retournements orthogonaux.

Remarque : Ces résultats se généralisent aux groupes $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ par récurrence sur n .

Démonstration. .

Pour la première partie de l'énoncé, on prend E un espace vectoriel de dimension n et on montre par récurrence sur la dimension de E que $O(E)$ est engendré par les réflexions orthogonales.

Le groupe $O(E)$ est engendré par les réflexions en dimension 1 car on a alors $O(E) = \{Id, -Id\}$ et $-Id$ est une réflexion. On suppose que le groupe orthogonal de tout espace euclidien de dimension $n \in \mathbb{N}^*$ est engendré par les réflexions. On se donne alors un espace euclidien E de dimension $n + 1$ et $u \in O(E)$.

Si $u = Id$, u est bien un produit de réflexions.

Sinon, $\exists a \in E, u(a) \neq a$. Puisque $\|u(a)\| = \|a\|$, on peut montrer qu'il existe une réflexion s échangeant a et $u(a)$ (c'est géométriquement clair et on peut préciser que s est la réflexion par rapport à l'hyperplan $Vect(u(a) - a)^\perp$). Alors $s \circ u$ coïncide avec l'identité sur $Vect(a)$.

En particulier, $s \circ u$ stabilise $Vect(a)$. Puisque $s \circ u$ est un automorphisme orthogonal, il stabilise également $Vect(a)^\perp$. Ainsi $s \circ u$ induit un automorphisme orthogonal de $Vect(a)^\perp$. Par hypothèse de récurrence, cet automorphisme induit est un produit de réflexions de $Vect(a)^\perp$. On peut prolonger ces réflexions de $Vect(a)^\perp$ en des réflexions de E en les faisant coïncider avec l'identité sur $Vect(a)$. On vérifie alors que $s \circ u$ est le produit de ces réflexions et u est alors également un produit de réflexions puisque $s^{-1} = s$ en est une.

Tout élément de $SO_3(\mathbb{R})$ est alors la composition d'un nombre pair de réflexions (car le déterminant est 1). Il suffit donc de montrer que la composée de deux réflexions est une composée de deux retournements. Soient s et s' deux réflexions de \mathbb{R}^3 euclidien usuel. On a $s \circ s' = (-s) \circ (-s')$ et $-s$ et $-s'$ sont des retournements. ■

1.2 Simplicité et action sur la sphère unité

Définition 3. Soit E un espace euclidien de dimension n avec $n \geq 1$. On appelle sphère unité, l'hypersurface constituée des points de distance 1 à l'origine. On la notera S^{n-1} .

Théorème 2. Le groupe $SO_3(\mathbb{R})$ est simple.

Dans la suite, on munit \mathbb{R}^3 du produit scalaire usuel. Les sous-groupes $SO_3(\mathbb{R})$ et $SO(\mathbb{R}^3)$ sont alors isomorphes par l'isomorphisme $u \in SO(\mathbb{R}^3) \mapsto Mat_{B_{canonique}}(u)$

Démonstration. .

Nous admettrons le lemme suivant :

Lemme 1. Les retournements sont tous conjugués dans $SO(\mathbb{R}^3)$.

Soit $H \neq \{Id\}$ un sous-groupe distingué de $SO(\mathbb{R}^3)$. D'après les lemmes précédents, il suffit de montrer que H contient un demi-tour pour conclure qu'il les contient tous (cf Lemme 1) et que $H = SO(\mathbb{R}^3)$ (cf Théorème 1).

Comme $H \neq \{Id\}$, H contient une rotation r d'angle $\theta \neq 0$. Il n'est pas restrictif de supposer $\theta \in]0, \pi]$ (quitte à remplacer r par r^{-1}).

Montrons qu'il existe $k \in \mathbb{N}^*$ tel que r^k soit une rotation d'angle $k\theta \in]\frac{\pi}{2}, \pi]$. Ceci vient du fait que \mathbb{R} est archimédien : si $\theta \in]0, \frac{\pi}{2}]$: $\exists k \in \mathbb{N}$, $k\theta > \frac{\pi}{2}$.

Ainsi, en prenant k minimal vérifiant la propriété précédente, on a :

$$\begin{cases} (k-1)\theta \leq \frac{\pi}{2} < k\theta \\ \theta \leq \frac{\pi}{2} \end{cases} \quad \text{donc} \quad k\theta = (k-1)\theta + \theta \leq \frac{\pi}{2} + \frac{\pi}{2} = \pi.$$

$r^k \in H$ est donc une rotation d'angle $\theta' \in]\frac{\pi}{2}, \pi]$.

De la valeur de θ' on déduit que $\frac{1}{1-\cos(\theta')} \in]0, 1[$. On peut donc l'écrire $\sin^2(t)$ pour un certain $t \in]0, \pi[$.

Montrons que $\exists x \in S^2$, $\langle x, r^k(x) \rangle = 0$.

Soit x de coordonnées $(\cos(t), \sin(t), 0)$ dans B une base orthonormée dans laquelle

$$\text{Mat}_B(r^k) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta') & -\sin(\theta') \\ 0 & \sin(\theta') & \cos(\theta') \end{pmatrix}$$

Donc $r^k(x)$ a pour coordonnées $((\cos(t), \sin(t)\cos(\theta'), \sin(t)\sin(\theta'))$ et on vérifie que

$$\langle x, r^k(x) \rangle = 0.$$

Construisons maintenant un demi-tour :

Soit p_x le retournement d'axe $\langle x \rangle \in SO(\mathbb{R}^3)$.

Posons $r' = r^k$.

Alors H contient $h := p_x r' p_x^{-1} r'^{-1}$ car $H \triangleleft SO(\mathbb{R}^3)$

alors $p_x r' p_x^{-1} r'^{-1}(r'(x)) = p_x r' p_x(x) = p_x r'(x)$.

Or $r'(x) \in \langle x \rangle^\perp$, donc $p_x(r'(x)) = -r'(x)$.

Donc $h \in H$ envoie $r'(x) \in S^2$ sur $-r'(x)$.

C'est donc un retournement (les seules rotations de \mathbb{R}^3 dont -1 est valeur propre). ■

2 Sous-groupes finis de SO_3

Comme première étape dans notre travail de classifier tous les sous-groupes finis de rotations de l'espace euclidien de dimension 3, on va s'intéresser à des sous groupes particuliers de SO_3 : les groupes diédraux et le groupe des isométries laissant invariant les solides de Platon. Mais avant de commencer, il nous faut définir certains objets mathématiques.

Définition 4. On appelle "polytope" un ensemble P de points d'un espace euclidien de dimension finie qui est compact, intersection finie de demi-espaces.

Définition 5. En dimension 3, un drapeau d'un polytope est un triplet du type sommet, arête, face : (s, a, f) où $s \in a \subset f$.

Définition 6. Un polytope P est "régulier" si le groupe des isométries qui laissent P stable agit transitivement sur l'ensemble des drapeaux de P .

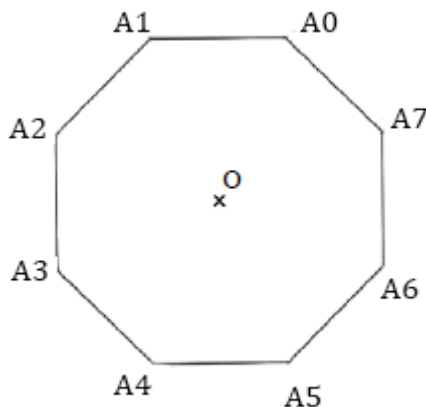
Définition 7. En géométrie, le dual d'un polytope est un polytope vérifiant :

- Le dual du polytope dual est le polytope initial.
- Les faces de l'un sont en correspondance avec les sommets de l'autre, en respectant les propriétés d'adjacence.

Pour un polyèdre régulier, on obtient un polyèdre dual en joignant les centres des faces adjacentes.

2.1 Groupe Diédral

On se place dans le plan euclidien usuel. Étant donné un polygone régulier, quelles sont les isométries qui le laissent globalement invariant ?



Définition 8. Soit $n \in \mathbb{N}$ tel que $n \geq 3$.

Dans le plan euclidien usuel, le groupe diédral d'ordre $2n$ est le groupe des isométries du plan euclidien usuel qui conservent un polygone régulier convexe à n côtés, d'isobarycentre l'origine, et dont l'un des sommets est $(1,0)$. On le note D_{2n} .

Proposition 3. D_{2n} est d'ordre $2n$ et $D_{2n} = \langle r, s \rangle$ où r est la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie par rapport à l'axe des abscisses. On a $srs = r^{-1}$.

Démonstration. Soit P_n le polygone régulier convexe à n côtés, d'isobarycentre l'origine O , et dont l'un des sommets est $(1,0)$. Soient i et j dans $\llbracket 0, n-1 \rrbracket$. Il existe une rotation r qui envoie l'arête orientée $[A_i A_{i+1}]$ sur l'arête orientée $[A_j A_{j+1}]$. On peut aussi envoyer $[A_i A_{i+1}]$ sur $[A_{j+1} A_j]$ en composant la précédente rotation par la symétrie d'axe la médiatrice de $[A_{j+1} A_j]$.

Comme $(\overrightarrow{OA_i}, \overrightarrow{OA_{i+1}})$ forme une base de \mathbb{R}^2 , les isométries précédemment considérées, qui fixent O , sont déterminées par l'image de A_i et A_{i+1} .

P_n ayant n arêtes distinctes, elle a donc $2n$ arêtes orientées distinctes. L'ordre de D_{2n} est donc $2n$.

r et s sont des éléments de D_{2n} donc $\langle r, s \rangle \subset D_{2n}$. En outre, $\langle r, s \rangle$ contient $2n$ éléments deux à deux distincts : $\{Id, r, r^2, \dots, r^{n-1}\}$ (de déterminant 1) et $\{s, rs, r^2s, \dots, r^{n-1}s\}$ (de déterminant -1).

Donc $D_{2n} = \langle r, s \rangle$.

Enfin, sr est une isométrie négative, donc une réflexion : on a $(sr)^2 = Id$, donc $srs = r^{-1}$. ■

Proposition 4. *En reprenant les mêmes notations, si l'on plonge P_n dans \mathbb{R}^3 , le groupe G des rotations de \mathbb{R}^3 qui conservent P_n est isomorphe à D_{2n} par l'application de restriction des rotations au plan du polygone.*

Démonstration. On identifie le plan euclidien \mathbb{R}^2 à $\mathbb{R}^2 \times \{0\}$, plongé dans \mathbb{R}^3 euclidien usuel, et on considère le polygone P_n de \mathbb{R}^3 introduit dans la preuve de la proposition 3.

On note G le groupe des rotations de \mathbb{R}^3 qui conservent P_n , on considère le

$$\begin{aligned} \text{morphisme : } R : G &\rightarrow O(\mathbb{R}^2) \\ g &\mapsto g|_{\mathbb{R}^2 \times \{0\}} \end{aligned}$$

R est bien défini car tout élément g de G stabilise le plan $\mathbb{R}^2 \times \{0\}$ engendré par P_n .

Alors R est injectif car si $g \in G$ est l'identité sur $\mathbb{R}^2 \times \{0\}$, la rotation g contient un plan de points fixes, c'est donc l'identité.

Il est, de plus, immédiat que $Im(R) \subset Is_{\mathbb{R}^2}(P_n) = D_{2n}$.

Il nous reste à montrer que $D_{2n} \subset Im(R)$.

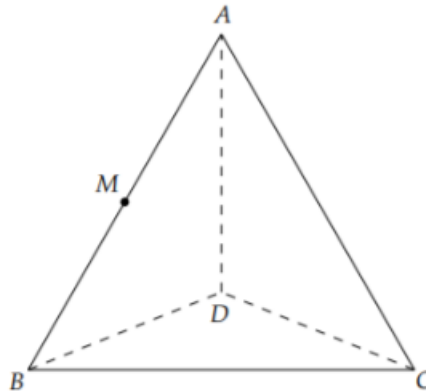
On se donne r_θ une rotation de \mathbb{R}^2 qui stabilise P_n .

r_θ est l'image par R de $\tilde{r}_\theta \in G$, la rotation d'axe e_3 et d'angle θ .

Soit alors s_D une réflexion d'axe D dans \mathbb{R}^2 qui stabilise P_n . On définit une isométrie positive \tilde{s}_D de \mathbb{R}^3 en posant $\tilde{s}_D(e_3) = -e_3$ et $\tilde{s}_D|_{\mathbb{R}^2 \times \{0\}} = s_D$: c'est un renversement d'axe D , qui vérifie $\tilde{s}_D \in G$ et $R(\tilde{s}_D) = s_D$. ■

2.2 Groupe des isométries du tétraèdre régulier.

On se place dans un espace affine réel euclidien de dimension 3.



Théorème 5 (Isométries du tétraèdre). Soit Δ un tétraèdre régulier. Le groupe des isométries préservant Δ , $Is(\Delta)$ est isomorphe à \mathfrak{S}_4 . De plus, le groupe des isométries positives préservant le tétraèdre, noté $Is_+(\Delta)$, est isomorphe au groupe alterné \mathfrak{A}_4 .

Démonstration. .

On fait agir le groupe $Is(\Delta)$ sur l'ensemble des sommets $S = \{A, B, C, D\}$, ce qui induit un morphisme de groupes donné par :

$$\begin{aligned} f : Is(\Delta) &\rightarrow \mathfrak{S}(S) \simeq \mathfrak{S}_4 \\ g &\mapsto g|S \end{aligned}$$

. On va montrer que f est bijective :

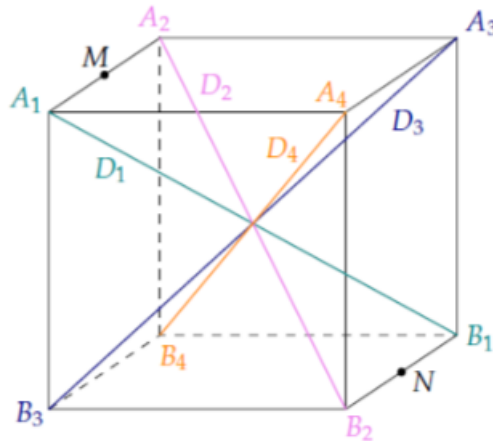
- f est injective : si $f(g) = id$, alors $g|S = id$. Or S est un repère affine de \mathbb{R}^3 , donc g ne peut être que id .
- f est surjective : soit M le milieu de $[AB]$. La réflexion par rapport au plan (MCD) réalise la transposition (AB) . De même, toutes les transpositions sont dans $f(Is(\Delta))$ et elles engendrent $\mathfrak{S}(S)$, donc $f(Is(\Delta)) = \mathfrak{S}(S)$.

Donc, f est un isomorphisme et $Is(\Delta) \simeq \mathfrak{S}_4$. Or $Is_+(\Delta)$ est d'indice 2 dans $Is(\Delta)$:

$$det : Is(\Delta) \rightarrow \{1, -1\}$$

est un morphisme surjectif, dont le noyau est Is_+ et comme \mathfrak{A}_4 est le seul sous-groupe distingué d'indice 2 de \mathfrak{S}_4 on a : $Is_+(\Delta) \simeq \mathfrak{A}_4$. ■

2.3 Groupe des isométries du cube.



Théorème 6 (Isométries du cube). Soit \square un cube. Le groupe des isométries préservant \square , que l'on notera $Is(\square)$, est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. De plus, le groupe des isométries positives préservant \square , noté $Is_+(\square)$, est isomorphe à \mathfrak{S}_4 .

Démonstration. Le cube a 4 grandes diagonales, qui relient chacune deux sommets opposés. Elles réalisent les plus grandes distances existant entre 2 points du cube, donc les isométries du cube stabilisent l'ensemble des grandes diagonales du cube. Pour $i \in \llbracket 1, 4 \rrbracket$, on note donc D_i la diagonale $(A_i B_i)$ et \mathcal{D} l'ensemble de ces grandes diagonales. Le groupe $Is_+(\square)$ agit sur \mathcal{D} , d'où le morphisme de groupes :

$$\begin{aligned} \phi : Is_+(\square) &\rightarrow \mathfrak{S}(\mathcal{D}) \simeq \mathfrak{S}_4 \\ g &\mapsto g|_{\mathcal{D}} \end{aligned}$$

On va montrer que ϕ est bijective :

— ϕ est injective :

soit g tel que $\phi(g) = Id_{\mathcal{D}}$.

Alors pour tout $i \in \llbracket 1, 4 \rrbracket$, $g(A_i) = A_i$ et $g(B_i) = B_i$ ou $g(A_i) = B_i$ et $g(B_i) = A_i$. Supposons qu'il existe $i \in \llbracket 1, 4 \rrbracket$ tel que g fixe A_i et B_i . On peut supposer sans perte de généralité $i = 1$.

Comme $A_1 A_2 \neq A_1 B_2$ et que $g \in Is(\square)$, nécessairement, $g(A_2) = A_2$. De même, $g(A_4) = A_4$ et $g(B_3) = B_3$.

g fixe donc un repère affine de l'espace, d'où $g = Id_{\mathbb{R}^3}$.

Désormais, on suppose que $\forall i \in \llbracket 1, 4 \rrbracket$, $g(A_i) = B_i$. Notons O le centre du cube, en notant s_O la symétrie par rapport à l'origine, on a :

$\forall i \in \llbracket 1, 4 \rrbracket$, $s_O \circ g(A_i) = A_i$, d'où $s_O \circ g = Id_{\mathbb{R}^3}$. Ceci contredit alors la positivité de g .

ϕ est donc injective.

— ϕ est surjective :

En effet, la transposition $(D_1 D_2)$ est l'image par ϕ du retournement d'axe (MN) où M et N sont les milieux des segments $[A_1 A_2]$ et $[B_1 B_2]$ (qui laisse stable D_3 et D_4).

Ainsi, $Is_+(\square) \simeq \mathfrak{S}_4$.

Enfin, on remarque que

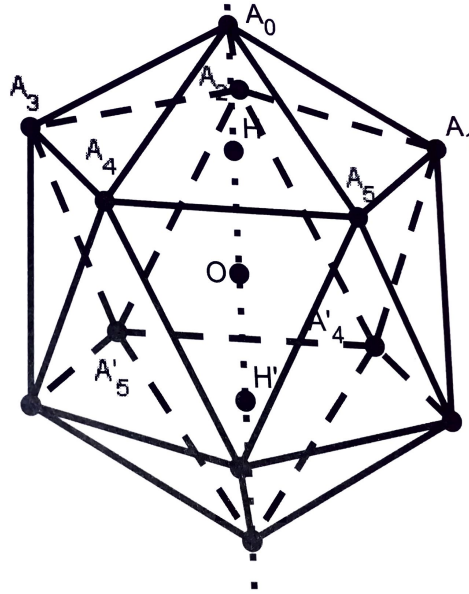
$$\begin{aligned} \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z} &\rightarrow Is(\square) \\ (\sigma, \bar{k}) &\mapsto \phi^{-1}(\sigma) \circ (-Id)^k \end{aligned}$$

est un isomorphisme, d'où le premier résultat. ■

Remarque : Les isométries conservant le cube sont les mêmes que celles conservant l'octaèdre régulier, puisque l'octaèdre est le dual du cube.

2.4 Groupe des isométries de l'icosaèdre.

Nous admettrons la construction de l'icosaèdre et son existence, et rappellerons via deux lemmes quelques propriétés fondamentales qui serviront au développement des théorèmes suivants.



Lemme 2 (Propriétés importantes de l'icosaèdre régulier). .

- L'icosaèdre régulier est un polyèdre possédant 20 faces, 30 arêtes et 12 sommets.
- Le point O est centre d'une sphère contenant les points $A_0, \dots, A_5, A'_0, \dots, A'_5$ et est isobarycentre de ces points.
- Tous les triangles formant les faces de l'icosaèdre régulier sont équilatéraux.

Lemme 3. . L'ensemble des 15 droites joignant O au milieu d'une arête peut être partitionné en cinq triplets de droites deux à deux orthogonales. Le groupe des isométries conservant l'icosaèdre agit transitivement sur l'ensemble de ces triplets de droites.

Le résultat du lemme 3 vient du fait qu'une isométrie préserve l'orthogonalité.

Théorème 7 (Rotations conservant l'icosaèdre régulier). .

Les rotations conservant l'icosaèdre sont les suivantes :

- Id
- Les rotations d'ordre 5 d'axe (OA_i) : il y en a 24.
- Les rotations d'ordre 2 (retournements) d'axe le milieu de deux arêtes opposées : il y en a 15.
- Les rotations d'ordre 3 d'axe le centre de deux faces opposées : il y en a 20.

Démonstration. L'icosaèdre possède 30 arêtes, et chaque arête peut être associée à 2 faces et 2 sommets, ce qui fait $4 \times 30 = 120$ drapeaux. L'action étant fidèle et transitive, cela correspond à $\text{card}(Is(I)) = 120$ et comme $s_O \in Is_-(I)$ on a donc $\text{card}(Is_+(I)) = 60$. En outre, on vérifie facilement que chacune de ces rotations conserve l'icosaèdre. ■

Théorème 8. *Le groupe des rotations conservant l'icosaèdre régulier est isomorphe au groupe alterné \mathfrak{A}_5 .*

Démonstration.

Nous allons voir que $Is_+(I)$ agit fidèlement sur l'ensemble des 5 triplets de droites décrits dans le lemme 3. On aura alors un morphisme injectif

$$\begin{aligned} \phi : Is_+(I) &\rightarrow \mathfrak{S}(\{t_0, t_1, t_2, t_3, t_4\}) \simeq \mathfrak{S}_5 \\ g &\mapsto \phi(g) \end{aligned}$$

où $\phi(g)(t_i) = g.t_i \quad \forall i \in \llbracket 0, 4 \rrbracket$.

En étudiant l'image de ϕ , on pourra identifier $Is_+(I)$ au groupe alterné \mathfrak{A}_5 .

Soient D_1, D_2 et D_3 les droites deux à deux orthogonales joignant O et (respectivement) les milieux des arêtes $[A_0A_4], [A_3A'_5]$ et $[A_1A_2]$. On note t_0 le triplet $\{D_1, D_2, D_3\}$ et $t_i = r_0^i(t_0)$ où r_0 est la rotation d'axe (OA_0) transformant A_1 en A_2 . Soit r une rotation conservant I et les triplets t_i . Montrons que $r = id$.

On sait par le *théorème 7* que $ord(r) \in \{1, 2, 3, 5\}$. Procédons par disjonction de cas :

- Si $ord(r) = 5$: Alors r est une rotation d'axe (OS) où S est un sommet de l'icosaèdre. Dans ce cas, un des triplets ne sera pas conservé : par exemple, si $S = A_0$ alors $r(D_1) \notin t_1$, donc $r(t_1) \neq t_1$.
- Si $ord(r) = 3$ et r conserve la face MNP .
Alors un triplet t contenant la droite D joignant O au milieu de $[MN]$ ne sera pas conservé.
En effet, $r[MN]$ est une arête de MNP donc est adjacent à $[MN]$. Or la droite joignant O au milieu de cette arête adjacente n'est pas orthogonale à D (on peut le montrer avec la réciproque du théorème de Pythagore), et r ne conserve donc pas t .
- Si $ord(r) = 2$ alors r est un retournement, par exemple, d'axe joignant O au milieu de $[A_0A_5]$. Alors $r(D_1)$ est la droite passant par O et le milieu de $[A_0A_1]$ et n'est pas dans t_1 car $r(A_4) = A_1$.

Ainsi, $r = id$, et l'action de $Is_+(I)$ sur $\{t_0, t_1, t_2, t_3, t_4\}$ est fidèle car seul l'élément neutre fixe tous les points. De là, ϕ est injective, il reste à montrer qu'elle est surjective.

Par le théorème précédent, on sait que les deux groupes ont même cardinal : 60. Ce théorème nous donne aussi la "composition" de $Is_+(I)$, donc de celle de $Im(\phi)$. Il contient au moins $(44 = 24 + 20)$ permutations paires (5 cycles et 3 cycles), relativement aux rotations d'ordre 3 et 5 de $Is_+(I)$. Enfin, $\phi(Is_+(I)) \cap \mathfrak{A}(\{t_0, t_1, t_2, t_3, t_4\}) \subseteq \mathfrak{A}(\{t_0, t_1, t_2, t_3, t_4\})$ est un sous-groupe et contient au moins $44 (\geq 31)$ éléments, donc du théorème de Lagrange, il est égal à $\mathfrak{A}(\{t_0, t_1, t_2, t_3, t_4\})$ qui est isomorphe à \mathfrak{A}_5 .

Donc $\phi(Is_+(I)) = \mathfrak{A}_5$. Ainsi on a $Is_+(I) \simeq \mathfrak{A}_5$. ■

2.5 Classification des sous-groupes finis.

Il s'agira d'associer chaque sous-groupe fini de rotations de l'espace euclidien à l'un des sous-groupes des isométries conservant les polygones et polyèdres étudiés précédemment.

Lemme 4. Soit G un groupe agissant sur un ensemble non vide X . Soit $P \in X$.

Soit $P' \in \text{Orb}(P) : \exists g \in G, P' = g(P)$
 et alors $\text{Stab}(g(P)) = g \circ \text{Stab}(P) \circ g^{-1}$.

Démonstration. On montre ce résultat par double inclusion.

- Si $f \in g \circ \text{Stab}(P) \circ g^{-1}$ alors $\exists g_1 \in \text{Stab}(P), f = g \circ g_1 \circ g^{-1}$.
 On vérifie $f(P') = f \circ g(P) = g \circ g_1 \circ g^{-1} \circ g(P) = g \circ g_1(P) = g(P) = P'$
 donc $f \in \text{Stab}(g(P))$.
- Si $f \in \text{Stab}(g(P))$ alors $f(g(P)) = g(P)$
 donc $g^{-1} \circ f \circ g(P) = P$ donc $g^{-1} \circ f \circ g \in \text{Stab}(P)$ donc $f \in \text{Stab}(g(P))$. ■

Proposition 9 (Caractérisation des polyèdres réguliers). .

Un polytope \mathcal{P} est régulier si et seulement si les trois conditions suivantes sont réalisées :

- l'ensemble $Is_-(\mathcal{P})$ est non vide.
- le groupe $Is_+(\mathcal{P})$ agit transitivement sur l'ensemble des sommets
- il existe un sommet S de \mathcal{P} tel que le groupe des rotations conservant \mathcal{P} et fixant S agit transitivement sur l'ensemble des sommets adjacents à S .

Démonstration. On admettra ce résultat, détaillé dans Szpirglas (Proposition 8.72.). ■

Théorème 10. Soit $G \subset SO_3(\mathbb{R})$ un sous-groupe d'ordre n ($n \geq 2$).

$$\text{Alors } G \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ D_n, & \exists m \geq 3, n = 2m \\ \mathfrak{A}_4 \\ \mathfrak{S}_4 \\ \mathfrak{A}_5 \end{cases}$$

Remarque : Ces groupes sont deux à deux non isomorphes. On va comme plus haut travailler dans $SO(\mathbb{R}^3)$, isomorphe à $SO_3(\mathbb{R})$.

Démonstration. Soit g une rotation non triviale d'un sous-groupe fini $G \subset SO(\mathbb{R}^3)$ d'ordre n . Alors l'axe de g intersecte la sphère unité en deux points que l'on appelle les pôles de g . Notons-les P et $-P$. Nos rotations étant des isométries vectorielles, G agit sur la sphère unité, S^2 . $\forall h \in G : hgh^{-1}h(P) = hg(P) = h(P)$ donc $h(P) \in S^2$ est un pôle de hgh^{-1} c'est à dire $h\text{Stab}(P)h^{-1} \subset \text{Stab}(h(P))$. Le lemme précédent montre en fait

qu'il y a égalité. Ainsi, G agit sur l'ensemble des pôles de ses éléments non triviaux, que l'on notera \mathcal{P} .

Remarque : faire opérer G sur \mathcal{P} est plus précis que de faire opérer G sur l'ensemble des axes des rotations car une droite conservée par une rotation n'est pas forcément l'axe de cette rotation (considérer les retournements), et un pôle conservé par une rotation non triviale caractérise l'axe de rotation.

Nous allons voir que l'application de la formule de Burnside* donne des renseignements sur le cardinal de G . Nous admettrons ce résultat.

Formule de Burnside* : Soit X un ensemble fini et G un groupe fini agissant sur X . Pour tout $g \in G$, on pose :
 $Fix(g) = \{x \in X, g.x = x\}$
 Alors le nombre k d'orbites pour l'action de G sur X est égal à $\frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

Si $P \in \mathcal{P}$: $Stab(P)$ (notons le S_P) est l'ensemble des rotations de G d'axe (OP) , qui est un groupe de rotations de même axe et fini : il est donc cyclique.

En effet, il suffit de considérer $\phi : S_P \rightarrow \phi(S_P) \subset \mathbb{C}^\times$
 $r_\theta \mapsto e^{i\theta}$ qui est un morphisme bijectif, donc $\phi(S_P)$ est un sous-groupe fini de \mathbb{C}^\times donc est isomorphe à \mathbb{U}_m où $m \geq 1$.

On définit l'ordre d'un pôle P comme $|Stab(P)|$.

Les stabilisateurs des "pôles appartenant à l'orbite de P " c'est-à-dire des pôles P' tels que $\exists g' \in G, g'(P) = P'$ sont des sous-groupes conjugués de $Stab(P)$ d'après le lemme 4, donc ils ont même cardinal. Les pôles d'une même orbite ont donc même ordre, dit l'ordre de l'orbite.

Chaque rotation non triviale ayant exactement deux pôles, on a :

$$card(\mathcal{P}) \leq 2 \times (card(G) - 1)$$

\mathcal{P} et G étant finis, on peut appliquer la formule de Burnside :

le nombre k d'orbites pour l'action de G sur \mathcal{P} est $k = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$ où $Fix(g) = \{P \in \mathcal{P}, g(P) = P\}$.

On observe que $Fix(id) = \mathcal{P}$ et $Fix(g) = \{P, -P\} \forall g \neq id$ où P est un pôle de g , donc $k = \frac{1}{|G|} \times (2(|G| - 1) + card(\mathcal{P})) \leq \frac{4(|G|-1)}{|G|} = 4 \left(1 - \frac{1}{|G|}\right) < 4$

donc $k \in \{2, 3\}$ (car $2 \leq k$ puisque $k \stackrel{2)}{=} 2 + \underbrace{\frac{card(\mathcal{P}) - 1}{|G|}}_{\geq 0}$)

Procédons par disjonction de cas :

Cas(0) : Si $k = 2$, alors toutes les rotations ont le même axe donc toutes les rotations stabilisent le plan vectoriel orthogonal à cet axe (notons le Π) et on

a l'isomorphisme $f : G \rightarrow f(G)$
 $g \mapsto g_\Pi \in SO(\mathbb{R}^2)$ où $f(G)$ est un sous-groupe fini d'ordre n de $SO(\mathbb{R}^2)$, il est unique et c'est le groupe $\langle r_{\frac{2\pi}{n}} \rangle$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Il reste à traiter les cas où $k = 3$.

Notons $\omega_1, \omega_2, \omega_3$ ces trois orbites avec pour ordres respectifs $n_1 \leq n_2 \leq n_3$. On rappelle que $n_i = |\text{Stab}(P)|$ pour $P \in w_i$. On a $\forall i \in \llbracket 1, 3 \rrbracket : |w_i| = \frac{|G|}{n_i}$ car $G/\text{Stab}(P) \simeq \text{Orb}(P)$, donc $\text{card}(\mathcal{P}) = \frac{n}{n_1} + \frac{n}{n_2} + \frac{n}{n_3}$ et d'après 2) : $3 = 2 - \frac{2}{n} + \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$
i.e $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n} > 1$.
(*)

Or $n_1 \geq 2$ car un pôle est stable en particulier par id et une rotation non triviale. Comme $2 \leq n_1 \leq n_2 \leq n_3$, au regard de (*), on a $n_1 = 2$ car sinon, $n_1 > 2$ et alors n_2 et n_3 aussi, donc $\forall i \in \llbracket 1, 3 \rrbracket n_i \geq 3$ donc $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} \leq 1$ ce qui est absurde.

De même, on trouve $n_2 \leq 3$

$$- n_2 = 2 \Rightarrow n = 2n_3$$

$$- n_2 = 3 \Rightarrow \frac{1}{n_3} = \frac{1}{6} + \frac{2}{n} \rightarrow n_3 \in \{3, 4, 5\} \text{ et } n = \frac{12 \times n_3}{6 - n_3}$$

. Ainsi, on trouve 4 configurations lorsqu'il y a 3 orbites.

Cas 1	$(n_1, n_2, n_3) = (2, 2, n_3)$	$n = 2n_3$	$ \omega_1 = n_3$	$ \omega_2 = n_3$	$ \omega_3 = 2$
Cas 2	$(n_1, n_2, n_3) = (2, 3, 3)$	$n = 12$	$ \omega_1 = 6$	$ \omega_2 = 4$	$ \omega_3 = 4$
Cas 3	$(n_1, n_2, n_3) = (2, 3, 4)$	$n = 24$	$ \omega_1 = 12$	$ \omega_2 = 8$	$ \omega_3 = 6$
Cas 4	$(n_1, n_2, n_3) = (2, 3, 5)$	$n = 60$	$ \omega_1 = 30$	$ \omega_2 = 20$	$ \omega_3 = 12$

Le but est maintenant d'identifier pour chaque cas le groupe de rotation correspondant et de montrer que les groupes correspondant à un même cas sont isomorphes. Pour cela, on remarque que les orbites sont stables par l'action de G et pour chaque cas, on va choisir une orbite qui va s'avérer être un polygone ou un polyèdre régulier.

Cas 1 :

- Supposons $n_3 = 2$: configuration $(2, 2, 2)$

On a alors $|G| = 2 \times 2 = 4$ et $|\omega_1| = |\omega_2| = |\omega_3| = 2$.

donc G contient 3 retournements, et l'identité : $G = \{id, r_1, r_2, r_3\}$ où r_1, r_2, r_3 sont des retournements d'axes orthogonaux car G est abélien.

En effet, si deux retournements distincts r et r' commutent, alors tout sous espace propre de r est stable par r' (c'est valable pour tout endomorphisme). On peut aussi l'expliquer ainsi : si r est une rotation d'axe \mathcal{D} d'angle θ , alors $r' \circ r \circ r'^{-1} = r$ (par hypothèse de commutativité) est une rotation d'axe $r'(\mathcal{D})$ d'angle θ .

Ainsi, cela nous impose $r'(\mathcal{D}) = \mathcal{D}$. Dans le cas de retournements, si r et r' sont distincts, cela nous impose que \mathcal{D} est orthogonal à \mathcal{D}' .

On a donc $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- Supposons $n_3 > 2$: configuration $(2, 2, n_3 > 2)$

Montrons que ω_1 est un polygone régulier et que G est le groupe des rotations qui le conservent.

On sait que $|\omega_1| = n_3$ et $|G| = 2n_3$

L'orbite ω_3 est la seule des trois orbites qui est d'ordre 2 (les autres étant d'ordre n_3). Il existe donc une rotation $r \in G$ d'ordre n_3 ayant

ses deux pôles dans ω_3 donc les points de ω_1 (et de ω_2) ne sont pas sur l'axe de r .

De là, si $P \in \omega_1$: pour $i \in \llbracket 0, n_3 - 1 \rrbracket$ les $r^i(P)$ sont les sommets d'un polygone régulier inscrit sur le plan vectoriel orthogonal à l'axe de la rotation r . Ils forment l'orbite ω_1 .

Or $|G| = 2n_3$ et $|G|$ conserve $\omega_3 = \{-P, P\}$: G est le groupe des rotations dans \mathbb{R}^3 qui conservent ce polygone : $G \simeq D_{2n_3}$.

(cf. *Proposition 4*)

Cas 2 :

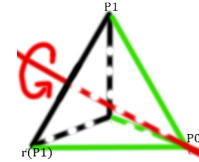
On se place dans la configuration $(n_1, n_2, n_3) = (2, 3, 3)$ avec $|w_3| = 4$.

On va montrer que ω_3 est l'ensemble des sommets d'un tétraèdre régulier, et que G est le groupe des rotations qui le préserve.

Soient $P_1, P_2 \in \omega_3$ tels que $P_1 \neq -P_2$

Comme $n_3 = 3 = |Stab(P_1)|$ (d'après le lemme 4).

Alors P_1 est pôle d'une rotation r de G d'ordre 3, conservant ω_3 . Ainsi, $\omega_3 = \{P_1, P_2, r(P_2), r^2(P_2)\}$ car les $\langle r \rangle$ -orbites ont cardinal 1 (pour P et $-P$) ou 3.



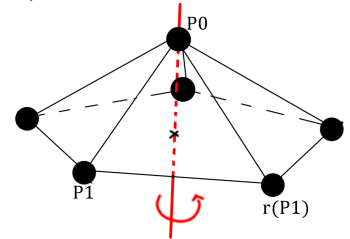
Or P_1 est équidistant des $r^i(P_2), i \in \llbracket 0, 2 \rrbracket$ et ω_3 étant une G -orbite, $\forall j \in \llbracket 0, 2 \rrbracket$: $\exists g \in G, r^j(P_2) = g(P_1)$ et g conserve les distances donc $g(P_1)$ est équidistant aux $g(r^i(P_2))$ qui sont les trois autres points de ω_3 . Ainsi, tous les points de ω_3 sont équidistants. On en conclut que ω_3 est un tétraèdre régulier.

Et comme $G \subset Is_+(\omega_3)$ et $|G| = |Is_+(\omega_3)| = 12$, alors G est le groupe des rotations conservant le tétraèdre ω_3 .

Cas 4 :

On considère la configuration $(n_1, n_2, n_3) = (2, 3, 5)$ avec $|w_3| = 12$ et $|G| = 60$. Nous allons utiliser la *proposition 9* pour montrer que ω_3 est l'ensemble des sommets d'un icosaèdre régulier dont le groupe des rotations le conservant est G . On va donc montrer que les trois conditions de la proposition 9 sont satisfaits.

- $G \subset Is_+(\omega_3)$ agit transitivement sur ω_3 par définition de l'orbite, donc $Is_+(\omega_3)$ agit transitivement sur ω_3 a fortiori.
- ω_3 est symétrique par rapport à l'origine : deux pôles d'une rotation d'ordre 5 de G sont nécessairement dans ω_3 car seule ω_3 est d'ordre 5. Par suite, l'isométrie négative $s_O (-Id)$ appartient à $Is(\omega_3)$.
- Soient P_0 et P_1 dans ω_3 tels qu'ils soient adjacents, c'est à dire que P_1 minimise la distance entre P_0 et P pour $P \in \omega_3 \setminus \{P_0\}$. Comme $|Stab(P_1)| = |\omega_3| = 5$, on peut construire 5 points adjacents à P_0 : en notant $r = r_{(OP_0), \frac{2\pi}{5}}$: $\{P_1, r(P_1), \dots, r^4(P_1)\}$



Le nombre de sommets adjacents à P_0 , noté a , est supérieur ou égal à 5.

a ne dépend pas du sommet choisi car $Is_+(\omega_3)$ agit transitivement sur ω_3 . Montrons que $a = 5$: on va admettre la formule d'Euler * pour les polyèdres :

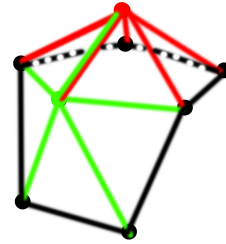
Formule d'Euler : Si un polyèdre convexe de l'espace a S sommets, A arêtes et F faces, alors $S - A + F = 2$

Dans le cas présent, ω_3 est contenue dans S^2 , on peut donc appliquer la formule d'Euler à son enveloppe convexe. Une face contient au moins 3 arêtes et chaque arête est située sur deux faces donc $2A \geq 3F$ ($3F \leq \{(\alpha, \phi), \alpha \in \phi\} \leq 2A$) donc avec la formule d'Euler :

$$3A = 3S + 3F - 6 \leq 2A + 3 \times 12 - 6$$

comme il y a 12 sommets (points de ω_3) on a $A \leq 36 - 6$.
Finalement $A \leq 30$.

Or $2A = S \times a$ (le 2 apparaît car on construit deux fois la même arête en faisant partir 5 arêtes de chaque sommet, puisque l'arête contient le nouveau sommet).



Donc $60 \geq 12 \times a$ donc $a \leq 5$. D'où $a = 5$.

Ainsi, le stabilisateur dans G d'un sommet agit transitivement sur l'ensemble de ses sommets adjacents.

La *proposition 9* montre donc que ω_3 définit un polytope régulier à 12 sommets : c'est un icosaèdre régulier.

On a $G \subset Is_+(\omega_3)$, et ces groupes ont même cardinal donc : $G = Is_+(Icosaedre)$.

Cas 3 :

On considère la configuration $(n_1, n_2, n_3) = (2, 3, 4)$ avec $|w_3| = 6$ et $|G| = 24$. Nous allons montrer que ω_3 définit un octaèdre régulier, dont le groupe des rotations le conservant est G . La preuve est, mutatis mutandis, identique à celle pour le cas 4.

Dans ce cas, une face contient au moins 3 arêtes et chaque arête appartient à deux faces, donc (Euler) $A \leq 3 \times 5 - 6 = 18 - 6 = 12$ donc $A \leq 12$.

Or $2A = 5 \times a$ donc $24 \geq 6 \times a \Rightarrow A \leq 4$. Donc $a = 4$

$G \subset Is_+(\omega_3)$, et ces groupes sont de même cardinal : $G = Is_+(Octaedre)$. ■

2.6 Application : des caractères irréductibles de \mathfrak{A}_4 , \mathfrak{S}_4 et \mathfrak{A}_5

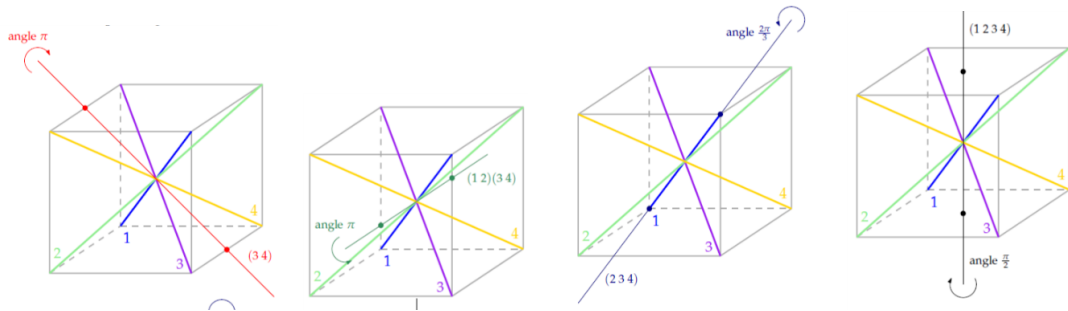
Les représentations de degré 3 de ces trois groupes issues de ce qu'ils sont les groupes d'isométries positives de polyèdres réguliers sont en fait irréductibles sur \mathbb{C} , on les trouve dans leur table des caractères :

\mathfrak{A}_4	Id	$(12)(34)$	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	$e^{\frac{2i\pi}{3}}$	$e^{\frac{4i\pi}{3}}$
χ_3	1	1	$e^{\frac{4i\pi}{3}}$	$e^{\frac{2i\pi}{3}}$
χ_4	3	-1	0	0

\mathfrak{A}_4	θ	$1 + 2\cos(\theta)$
Id	0	3
$(12)(34)$	π	-1
(123)	$\frac{2\pi}{3}$	0
(132)	$-\frac{2\pi}{3}$	0

\mathfrak{S}_4	Id	(12)	$(12)(34)$	(123)	(1234)
χ_1	1	1	1	1	1
χ_ϵ	1	-1	1	1	-1
χ_4	2	0	2	-1	0
χ_S	3	1	-1	0	-1
χ_C	3	-1	-1	0	1

\mathfrak{S}_4	θ	$1 + 2\cos(\theta)$
Id	0	3
(12)	π	-1
$(12)(34)$	π	-1
(123)	$\frac{2\pi}{3}$	0
(1234)	$\frac{\pi}{2}$	1



\mathfrak{A}_5	Id	(123)	$(12)(34)$	(12345)	(21345)
χ_1	1	1	1	1	1
χ_{std}	4	1	0	-1	-1
χ_5	5	-1	1	0	0
χ_S	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_C	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

\mathfrak{S}_4	θ	$1 + 2\cos(\theta)$
Id	0	3
(123)	$\frac{2\pi}{3}$	0
$(12)(34)$	π	-1
(12345)	$\frac{2\pi}{5}$	$\frac{1+\sqrt{5}}{2}$
(21345)	$\frac{4\pi}{5}$	$\frac{1-\sqrt{5}}{2}$

3 Sous-groupes infinis engendrés par deux rotations

Le but de cette section est de montrer le théorème de Hausdorff.

3.1 Paradoxe de Hausdorff ou paradoxe de la sphère

Définition 9. Soit G un groupe agissant sur un ensemble X . Soit $E \subset X$. On dit que E est G -paradoxal si pour des entiers naturels n et m , il existe des sous ensembles de E deux à deux disjoints $A_1, \dots, A_n, B_1, \dots, B_m$ et $g_1, \dots, g_n, h_1, \dots, h_m \in G$ tels que $E = \cup g_i(A_i)$ et $E = \cup h_j(B_j)$.

En d'autres termes, E contient deux parties disjointes qui, quitte à les réarranger via l'action de G , peuvent recouvrir E .

Dans la suite, on se placera dans l'espace euclidien \mathbb{R}^3 usuel. On considèrera l'action de $SO_3(\mathbb{R})$, identifié à $SO(\mathbb{R}^3)$ sur \mathbb{R}^3 .

Théorème 11 (Théorème de Hausdorff, (1913)). .

Soit S^2 la sphère unité de \mathbb{R}^3 . Il existe deux rotations vectorielles a et b , d'angles respectifs π et $2\pi/3$, et une partition de S^2 en quatre ensembles X, Y, Z, T tels que :

- T est dénombrable
- On a $Y = bX$, $Z = bY = b^2X$ et $X = a(Y \cup Z)$.

Remarque : Ce théorème dit que X est à la fois isométrique à Y , à Z et à $Y \cup Z$, donc à son double, puisque Y et Z sont disjoints (par définition d'une partition)...

Les rotations proposées par Hausdorff sont les suivantes :

$$a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

Proposition 12. Les endomorphismes a et b de \mathbb{R}^3 sont des rotations. La rotation a est d'axe $\mathbb{R}(e_1 + e_2)$ et d'angle π , donc d'ordre 2. La rotation b est d'axe dirigé par e_1 et d'angle $-\frac{2\pi}{3}$, donc d'ordre 3.

Démonstration. Pour b , le résultat est évident.

Il est clair que $a \times^t (e_1, e_2, e_3) =^t (e_2, e_1, -e_3)$ est une base orthonormée, donc a est une isométrie, de déterminant $-1 \times \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1$ (on développe par rapport au coefficient -1). Donc a est une rotation.

En outre, on vérifie que $a^2 = I_3$, donc a est un retournement, d'axe dirigé par $e_1 + e_2$ puisque ce vecteur non nul est fixé par a . ■

On note par la suite $G = \langle a, b \rangle$, le groupe engendré par a et b .

Proposition 13. $\forall r \in G \setminus \{Id, a\} : \exists(\epsilon_1, \epsilon_2) \in \{0, 1\}^2 : \exists k \in \mathbb{N}^* : \exists(n_1, \dots, n_k) \in \{1, 2\}^k$ tels que $r = a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2}$. Cette écriture est unique.
Autrement dit, tout élément de G s'écrit de manière unique comme un mot écrit avec l'alphabet a, b et les relations $a^2 = b^3 = Id$.

Démonstration. Comme $G = \langle a, b \rangle$ avec $a^2 = b^3 = I_3$, il en résulte que tout élément de G s'écrit comme produit fini des éléments a, b et b^2 donc G contient tous les produits finis de a, b qui apparaissent dans l'énoncé. Il reste à montrer l'existence et l'unicité de l'écriture de r . On utilisera le lemme suivant :

Lemme 5. Tout produit $c = b^{n_1} a \dots b^{n_k} a$ avec $k \geq 1$ et $n_i \in \{1, 2\}$ est de la forme : $c = \frac{1}{2^k} \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix}$ avec les $p_i, q_i \in \mathbb{Z}$ et p_i pairs et q_i impairs. Un tel c ne peut être égal à I_3 ou a .

- On montre le lemme par récurrence sur k .

Initialisation : lorsque $k = 1$, $c \in \{b^2a, ba\}$ et on a $b^2a = \frac{1}{2} \begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & \sqrt{3} \\ \sqrt{3} & 0 & 1 \end{pmatrix}$

et $ba = \frac{1}{2} \begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & -\sqrt{3} \\ -\sqrt{3} & 0 & 1 \end{pmatrix}$

Hérédité : On suppose le lemme vrai pour un certain $k \geq 1$ fixé. Il suffit alors de calculer les produits $c \times b^2a$ et $c \times ba$ pour montrer le résultat au rang $k+1$. Par hypothèse de récurrence, le premier produit, multiplié par 2^{k+1} s'écrit :

$$\begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix} \times \begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & \sqrt{3} \\ \sqrt{3} & 0 & 1 \end{pmatrix} = \begin{pmatrix} -p_2 + 3p_3 & 2p_1 & \sqrt{3}(p_2 + p_3) \\ -p_4 + 3q_2 & 2q_1 & \sqrt{3}(p_4 + q_2) \\ \sqrt{3}(q_4 - p_5) & 2q_3\sqrt{3} & 3p_5 + q_4 \end{pmatrix}$$

Or le produit de deux nombres impairs est impair. Le produit d'un nombre pair par un nombre impair est pair. La somme (resp. soustraction) d'un nombre pair et d'un nombre impair est impair. La somme (resp. soustraction) de deux nombres impairs est paire.

On vérifie alors que tous les coefficients de la matrice produit sont de la forme souhaitée.

Le second produit est de la même forme que le précédent, puisque les changements des sommes en soustractions ne modifient pas la parité.

Enfin on remarque que le coefficient $c_{3,1}$ vérifie :

$2^{k+1} \times c_{3,1} \in \{\sqrt{3}(q_4 - p_5), -\sqrt{3}(p_4 + q_2)\}$, donc $c_{3,1}$ ne peut s'annuler puisqu'une somme (resp. soustraction) d'un nombre pair et d'un nombre impair ne s'annule pas. Comparé au même coefficient au sein de a et I_3 , un tel c ne peut lui être égal.

Existence : on gardera les notations de l'énoncé.

$G = \langle a, b \rangle$ est par définition, le plus petit sous-groupe de $SO_3(\mathbb{R})$ contenant a et b .

Si on montre que l'ensemble des mots de la forme $a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2}$, avec n_i et ϵ_i comme dans l'énoncé de la *proposition 13* que l'on note F forme un groupe, alors on a $G \subset F$, d'où l'existence de l'écriture.

Pour cela, on se donne deux éléments de F : r et r' . Il nous suffit de vérifier que $r \circ r' \in F$ et que $r^{-1} \in F$.

Notons, selon les notations de la *proposition 13* :

$$\begin{cases} r = a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2} \\ r' = a^{\epsilon'_1} b^{n'_1} a b^{n'_2} \dots a b^{n'_k} a^{\epsilon'_2} \end{cases}$$

On a alors :

$$r^{-1} = a^{\epsilon_2} b^{2n_k} a b^{2n_{k-1}} a \dots a b^{2n_2} a b^{2n_1} a^{\epsilon_2} \quad \text{car } (a^{\epsilon_i})^{-1} = a^{\epsilon_i} \text{ et } (b^{n_i})^{-1} = b^{2n_i}$$

Comme $n_i \in \{1, 2\}$, $2n_i \in \{2, 4\}$. Or $b^4 = b \circ (b^3) = b$.

Ainsi, cela revient à avoir des exposants sur b dans $\{1, 2\}$.

De manière générale, pour la suite, on identifiera (pour simplifier l'écriture) les exposants de b à leur représentant dans $\{1, 2\}$ (modulo 3).

On pourra faire de même avec les exposants de a , qu'on identifiera à leur représentant dans $\{0, 1\}$ (modulo 2).

avec cette identification, r^{-1} est donc de la forme souhaitée, donc $r^{-1} \in F$.

$$rr' = a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2} \circ a^{\epsilon'_1} b^{n'_1} a b^{n'_2} \dots a b^{n'_k} a^{\epsilon'_2}$$

Si $\epsilon_2 \neq \epsilon'_1$, alors on a bien $a^{\epsilon_2} \circ a^{\epsilon'_1} = a$, donc rr' est de la forme souhaitée.

Si $\epsilon_2 = \epsilon'_1$, alors $a^{\epsilon_2} \circ a^{\epsilon'_1} = I_3$. Il peut alors y avoir des simplifications. Supposons, sans perte de généralité, que $k \leq k'$.

On distingue deux cas :

- $\exists i \in \llbracket 0, k-1 \rrbracket$, $n_{k-i} + n'_{i+1} \not\equiv 0[3]$

En prenant i maximal, on a : $rr' = a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_{k-i-1}} a b^{n_{k-i} + n'_{i+1}} a b^{n'_{i+2}} \dots a b^{n'_k} a^{\epsilon'_2}$ qui est bien un élément de F

- $\forall i \in \llbracket 0, k-1 \rrbracket$, $n_{k-i} + n'_{i+1} \equiv 0[3]$

alors $rr' = a^{\epsilon_1} b^{n'_{k+1}} a \dots b^{n'_k} a^{\epsilon'_2}$ est bien un élément de F .

On a montré que F est un groupe, donc il y a bien existence de l'écriture conformément à l'énoncé.

Unicité :

Soient r et r' , notés comme dans la partie précédente, deux écritures distinctes de $r \in G$. On suppose que $r = r'$. On suppose, sans perte de généralité $k \leq k'$ et on prend r de longueur minimale l (on définit la longueur d'un élément de G comme le nombre de monômes non triviaux qui le composent, lorsqu'il est écrit sous la forme de l'énoncé).

Si $l = 0$, alors $r = I_3$. Si $k' \geq 1$ on a alors une contradiction avec le *lemme 5*.

Si $k' = 0$, alors par convention, $\epsilon'_2 = 0$ et donc $\epsilon'_1 = 0$.

Si $l \geq 1$, l'hypothèse de minimalité impose $\epsilon_2 \neq \epsilon'_2$, donc

$$r \circ r^{-1} = a^{\epsilon_1} b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2 + \epsilon'_2} b^{2n'_k} a b^{2n'_{k-1}} a \dots a b^{2n'_1} a^{\epsilon'_1} = Id$$

En composant à gauche par a^{ϵ_1} et à droite par $a^{\epsilon'_1+1}$, on obtient :

$$b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2 + \epsilon'_2} b^{2n'_k} a b^{2n'_{k-1}} a \dots a b^{2n'_1} a = a^{\epsilon'_1 + \epsilon_1 + 1} \in \{I_3, a\}$$

ce qui contredit le *lemme 5*. On a donc l'unicité de l'écriture, conformément à l'énoncé. ■

Corollaire 1. *Le groupe G est dénombrable.*

Démonstration. Notons $2, 3, p_1 = 5, p_2 = 7 \dots$ l'ensemble des nombres premiers. On considère l'application :

$$\begin{array}{rcll} f : & G & \rightarrow & \mathbb{N} \\ & Id & \mapsto & 0 \\ & a & \mapsto & 1 \\ & a^{\epsilon_1} a b^{n_1} a b^{n_2} \dots a b^{n_k} a^{\epsilon_2} & \mapsto & 2^{\epsilon_1} 3^{\epsilon_2} p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} \end{array}$$

L'unicité de la décomposition en facteurs premiers dans \mathbb{N} montre que f est injective, donc G est dénombrable. ■

L'idée clé du théorème de Hausdorff est de découper le groupe G en trois parties disjointes X, Y, Z vérifiant $Y = bX$, $Z = bY = b^2X$ et $X = a(Y \cup Z)$. On note A_0 l'ensemble des mots commençant par a ($\epsilon_1 = 1$), B_0 l'ensemble des mots commençant par la lettre b ($\epsilon_1 = 0$ et $n_1 = 1$) et C_0 l'ensemble des mots commençant par b^2 ($\epsilon_1 = 0$ et $n_1 = 2$).

On peut écrire G sous forme d'unions disjointes : $G = A_0 \cup B_0 \cup C_0 \cup \{Id\}$.

Il est clair qu'on a les relations suivantes :

$$C_0 = bB_0, B_0 = b^2C_0, bA_0 = B_0 \setminus \{b\}, b^2A_0 = C_0 \setminus \{b^2\}, a(B_0 \cup C_0) = A_0 \setminus \{a\}.$$

On a presque les relations recherchées, mais il y a les problèmes avec les éléments a, b et c . L'idée est de les rajouter suivant le principe de "*l'hôtel de Hilbert*" qui met en évidence le fait que pour tout entier naturel $x : \mathbb{N} \setminus \{x\}$ est en bijection avec \mathbb{N} , autrement dit on peut ajouter/enlever un élément à un ensemble de cardinal infini sans modifier son cardinal.

Pour mettre cela en œuvre, il faut disposer dans G d'un ensemble qui ressemble à \mathbb{N} et il suffit pour cela de trouver un élément d'ordre infini. Le lemme 5 nous assure que $c = b^2a$ est d'ordre infini. On note N le monoïde engendré par cet élément : $N = \{Id, b^2a, (b^2a)^2, \dots\}$ On remarque que $N \setminus \{Id\} \subset C_0$, $aN \subset A_0$ et $baN \subset B_0$, ce qui prouve que ces ensembles sont disjoints.

On a $b^2aN = N \setminus \{Id\}$ donc $ab(b^2a)N = ab(N \setminus \{Id\}) = N$. On a donc ajouté Id à N . De même, on peut ajouter b par $bN = aN \cup \{b\}$ (en écrivant les deux ensembles, on voit qu'ils sont égaux), et pour ajouter b^2 on écrit $b^2N = baN \cup \{b^2\}$.

Posons $A' = A_0 \setminus aN$, $B' = B_0 \setminus baN$ et $C' = C_0 \setminus b^2aN = C_0 \setminus (N \setminus \{Id\})$

On a $bA' = B' \setminus \{b\}$, car

$$bA' = b(A_0 \setminus aN) = bA_0 \setminus baN = (B_0 \setminus \{b\}) \setminus baN = (B_0 \setminus baN) \setminus \{b\} = B' \setminus \{b\}$$

Pour rajouter le b manquant, on voudrait utiliser la formule $bN = aN \cup \{b\}$. Pour cela, il faut au préalable mettre N dans A' et aN dans B' . La même considération sur les autres ensembles nous conduit à poser :

$$A = A' \cup N, \quad B = B' \cup aN, \quad \text{et} \quad C = C' \cup baN$$

A_0, B_0 et C_0 étant disjoints, A', B' et C' aussi, et comme N, aN et baN sont eux aussi disjoints, alors A, B et C sont disjoints. Comme leur union recouvre G tout entier, ils forment donc une partition de G .

Proposition 14. *Les parties A, B et C construites ci-dessus vérifient : $B = bA, C = bB = b^2A, A = a(B \cup C)$.*

Démonstration. Il suffit d'appliquer les formules précédentes en notant que si $g \in G$ et si X et Y sont des parties de G , comme la multiplication par g est bijective, les formules $g(X - Y) = gX - gY$ et $g(X \cup Y) = gX \cup gY$ sont valides.

On a d'abord $A = (A_0 \setminus aN) \cup N$, donc

$$\begin{aligned} bA &= (bA_0 \setminus baN) \cup bN \\ &= (B_0 \setminus \{b\} \setminus baN) \cup aN \cup \{b\} \\ &= B' \cup aN = B \end{aligned}$$

On a ensuite

$$\begin{aligned} bB &= b((B_0 \setminus baN) \cup aN) \\ &= (bB_0 \setminus b^2aN) \cup baN \\ &= (C_0 \setminus b^2aN) \cup baN \\ &= C' \cup baN \\ &= C \end{aligned}$$

On a enfin

$$\begin{aligned} a(B \cup C) &= a((B_0 \setminus baN) \cup aN \cup (C_0 \setminus (N \setminus \{Id\})) \cup baN) \\ &= (aB_0 \setminus abaN) \cup N \cup aC_0 \setminus (aN \setminus \{a\}) \cup abaN \end{aligned}$$

En tenant compte de la formule donnant $a(B_0 \cup C_0)$ et des simplifications des termes $abaN$ et $\{a\}$, on trouve $a(B \cup C) = (A_0 \setminus aN) \cup N = A$.

■

Découpage de la sphère

On considère l'action de G sur la sphère $S^2 : G \times S^2 \longrightarrow S^2$.

On note T l'ensemble des pôles des éléments de G , qui est une partie de S^2 . Chaque élément de $G \setminus \{Id\}$ ayant deux pôles, on a $card(T) = 2(|G| - 1)$ et donc T est dénombrable.

Si $x \in S^2 \setminus T$, alors $\forall g \in G \setminus \{Id\} : g(x) \neq x$

On a pour un tel élément $x : Orb_G(x) \simeq G$ par l'application

$$\begin{aligned} f_x : G &\rightarrow Orb(x) \\ g &\mapsto g.x \end{aligned} \quad \text{qui est clairement surjective. Si } gx = hx \text{ avec } g \neq h$$

dans G , alors $x = gh^{-1}.x$ donc x est sur l'axe de gh^{-1} , ce qui est absurde car $x \notin T$ par hypothèse. Donc f_x est bijective.

On a donc une partition de $S \setminus T$ par \mathcal{I} , l'ensemble des orbites des points de $S^2 \setminus T$. L'axiome du choix nous permet de choisir un point dans chaque orbite, donc de choisir une application $f : \begin{array}{l} \mathcal{I} \rightarrow S^2 \\ \mathcal{O} \mapsto x \end{array}$ telle que $x \in \mathcal{O}$.

On a alors $Im(f) \subset S^2$. Notons $Im(f) = E$.

Chaque orbite est représentée par un seul point de E .

On pose :
$$\begin{cases} X = AE = \{g(x), g \in A, x \in E\} \\ Y = BE = \{g(x), g \in B, x \in E\} \\ Z = CE = \{g(x), g \in C, x \in E\} \end{cases}$$

Vérifions qu'on a les relations du théorème de Hausdorff à l'aide de la *proposition 14*.

Montrons que $Y = bX$:

Soit $x \in X$.

$\exists g \in A : \exists e \in E, x = ge$ donc $bx = bge$ et comme $bA = B$ alors $bg \in B$ et $bge \in Y$, d'où $bX \subset Y$.

Inversement, soit $y \in Y$.

Alors $\exists h \in B : \exists e \in E, y = he$. Or $B = bA$ donc $\exists g \in A, h = bg$. Ainsi, on peut écrire $y = b(ge) \in bX$.

Montrons que $Z = bY$:

On a $Z = bY \Leftrightarrow CE = bBE$ or $bB = C$ d'où l'égalité.

Les autres relations $bY = b^2X$ (qui vient de $bB = b^2A$) et $X = a(Y \cup Z)$ (qui vient de $A = a(B \cup C)$) se vérifient de la même façon.

On a alors prouvé le théorème de Hausdorff.

Ce théorème montre en particulier que la sphère est G -paradoxe, dans le sens défini dans la *définition 9*, G étant un groupe infini engendré par deux rotations bien particulières.

Références

- Wagon S., *The Banach-Tarski paradox*, Encyclopedia of Mathematics, Vol. 24, Cambridge, 1985.
- Perrin D., *Le paradoxe de Hausdorff-Banach-Tarski*, <https://www.math.u-psud.fr/~perrin/TER/HBT.pdf>
- Szpirglas A., *Mathématiques Algèbre L3*, 2009
- Caldero P. & Germoni J. , *Histoires hédonistes de groupes et de géométries, Tome premier*, 2013
- Huppert B., *Character Theory of Finite Groups*