

CLASSIFICATION DES SOUS-GROUPES FINIS DES RÉFLEXIONS DU PLAN ET DE L'ESPACE : ÉTUDE GÉOMÉTRIQUE DE RÉSULTATS CLASSIQUES

FLORENCE MAAS-GARIÉPY

1. Introduction	2
2. Classification des sous-groupes de $O(\mathbb{R}^2)$	3
2.1. Théorème de Cartan-Dieudonné	4
2.2. Classification des sous-groupes finis de $O(\mathbb{R}^2)$	6
3. Classification des sous-groupes finis de $SO(\mathbb{R}^3)$	10
3.1. Formule de Burnside	10
3.2. Théorèmes de Sylow	14
3.3. Polyèdres réguliers et les groupes de rotations les préservant	16
3.4. Classification des sous-groupes finis de $SO(\mathbb{R}^3)$	21
4. Note	31
5. Conclusion	32
Remerciements	32
Références	33

Table des matières

1. INTRODUCTION

La théorie des groupes forme une branche très active et prolifique des mathématiques. Puisque les groupes peuvent être difficiles à visualiser, nous avons mis à profit l'étude des groupes de réflexions, qui correspondent aux groupes des isométries du plan et de l'espace. Ces groupes permettent de visualiser concrètement la notion de groupe et ont de nombreuses applications dans plusieurs domaines, notamment en algèbre et géométrie avec les groupes de Coxeter et en chimie, avec la cristallographie. Nous nous sommes ainsi concentrés sur la classification des groupes finis des isométries du plan et de l'espace, à isomorphisme près. Cette classification est un résultat préalablement connu, mais qui demeurent intéressant et non trivial.

Nous avons conservé le plus que possible une approche géométrique au cours de ce rapport. Ainsi, lorsque possible, des figures accompagnent les énoncés afin d'augmenter la compréhension de ceux-ci.

Pour cela, nous avons majoritairement suivi le plan proposé par L.C. Grove et C.T. Benson dans [3] au chapitre 2.

Le travail réalisé dans la seconde partie du stage n'a malheureusement pas pu être intégré à ce rapport, par manque de temps, et sera expliqué rapidement dans une note précédent la conclusion.

2. CLASSIFICATION DES SOUS-GROUPES DE $O(\mathbb{R}^2)$

Nous allons tout d'abord procéder à quelques rappels de définitions et de théorèmes. Nous supposons que le lecteur possède une base en algèbre linéaire et en théorie des groupes.

Tout au long de cette section, nous considérerons (E, B) un $\mathbb{R}$ -espace vectoriel de dimension n .

Définition 2.1. L'ensemble des endomorphismes de E , noté $L(E)$, est défini par

$$L(E) = \{f : E \rightarrow E \mid f(x + \lambda y) = f(x) + \lambda f(y)\}.$$

Définition 2.2. Le groupe des automorphismes de E , noté $GL(E)$, est défini par

$$GL(E) = \{f \in L(E) \mid \exists g : E \rightarrow E \text{ tel que } f \circ g = \mathbb{1}_E\}.$$

Définition 2.3. Le groupe orthogonal de E , noté $O(E)$, correspond géométriquement au groupe des isométries de E et est défini par

$$O(E) = \{f \in GL(E) \mid B(f(v), f(u)) = B(u, v) \forall u, v \in E\}.$$

Remarque 2.4. On a que $|\det(f)| = 1$ pour tout $f \in O(E)$.

Définition 2.5. Le groupe spécial orthogonal est un sous-groupe de $O(E)$, noté $SO(E)$, correspond géométriquement au groupe des rotations de E et est défini par

$$SO(E) = \{f \in O(E) \mid \det(f) = 1\}.$$

Théorème 2.6 (Théorème du rang). *Soit $f \in L(E)$, alors*

$$\begin{aligned} n = \dim(E) &= \dim(\text{Im}(f)) + \dim(\ker(f)) \\ &= \text{rang}(f) + \dim(\ker(f)) \text{ par définition du rang.} \end{aligned}$$

Définition 2.7. Soit $s \in O(E)$ telle que

$$\text{fix}(s) = \{v \in E \mid s(v) = v\} = \ker(s - \mathbb{1}_E)$$

est un hyperplan. On dit alors que s est une réflexion.

2.1. Théorème de Cartan-Dieudonné. Ce théorème est intéressant en lui même, puisqu'il énonce que pour une isométrie f de E ($f \in O(E)$), alors f est composée d'exactlyment $\text{rang}(f - \mathbb{1})$ réflexions. Cela permet non seulement d'énoncer que toutes les isométries d'un espace sont engendrées par des réflexions de cet espace, mais également de dénombrer précisément le nombre de réflexions composant une isométrie.

Ce théorème nous sera particulièrement utile en conjonction avec le théorème du rang, car dans le cas où la dimension de E est finie, alors il sera possible de classifier de façon précise les isométries de cet espace à partir du nombre de réflexions les composant.

Théorème 2.8 (Théorème de Cartan-Dieudonné). *Soit $f \in O(E)$, alors f est composée d'exactlyment $\text{rang}(f - \mathbb{1}_E)$ réflexions.*

Preuve. Procédons par induction sur la dimension de E .

Si $n = 1$, alors E est une droite. Puisque les isométries d'une droite se limitent à celles de la forme $x \mapsto \lambda x$ pour $x \in E$ et $|\lambda| = 1$, on n'a que deux cas possibles à considérer :

Si $\lambda = 1$ alors $f = \mathbb{1}_E$. On a $\text{rang}(f - \mathbb{1}_E) = 0$ et on a effectivement que $f = \mathbb{1}_E$ est composée de $\text{rang}(f - \mathbb{1}_E)$ réflexions.

Si $\lambda = -1$, alors f est une réflexion par rapport à l'hyperplan 0 , $\dim(\text{fix}(f)) = \dim(\ker(f - \mathbb{1}_E)) = 0$. Par Théorème 2.6, on a donc que $\text{rang}(f - \mathbb{1}_E) = 1$ et f est bien composée de $\text{rang}(f - \mathbb{1}_E)$ réflexions.

Supposons que, pour (E', B') un espace vectoriel de dimension $n - 1$ et $g \in L(E')$, g est composée d'exactlyment $\text{rang}(g - \mathbb{1}_{E'})$ réflexions.

Considérons $f \in O(E)$ et $v_0 \in E$. On a soit $f(v_0) = v_0$ (et f fixe v_0), ou $f(v_0) \neq v_0$.

Cas 1 : Si $f(v_0) = v_0$, considérons l'hyperplan $H = \langle v_0 \rangle^\perp$ et $f' = f|_H$.

Puisque H est de dimension $n - 1$, alors on peut appliquer l'hypothèse de récurrence avec $E' = H$, $B' = B|_{H \times H}$ et $g = f'$. On a ainsi que $f' = s_{H'_1} \circ s_{H'_2} \circ \dots \circ s_{H'_m}$, où $m' = \text{rang}(f' - \mathbb{1}_H)$. À partir des hyperplans H'_i de H et de $\langle v_0 \rangle$, on peut construire des hyperplans $H_i = H'_i \oplus \langle v_0 \rangle$ de E , puisque H et $\langle v_0 \rangle$ sont orthogonaux. Notons pour le moment $h := s_{H_1} \circ s_{H_2} \circ \dots \circ s_{H_m}$.

On a que $v_0 \in H_i \ \forall \ 0 \leq i \leq m$, donc s_{H_i} fixe v_0 , ce qui entraîne que $h(v_0) = v_0 = f(v_0)$. De plus, $h|_H = f' = f|_H$. On ainsi que $h = f$.

Puisque f fixe $v_0 \notin H$ et que $f' = f|_H$, on a également que $\dim(\ker(f' - \mathbb{1}_H)) = \dim(\text{fix}(f')) = \dim(\text{fix}(f)) - 1 = \dim(\ker(f - \mathbb{1}_E)) - 1$. Cela nous permet d'affirmer que $\text{rang}(f - \mathbb{1}_E) = \text{rang}(f' - \mathbb{1}_H)$ et que f est composée d'exactlyement $\text{rang}(f - \mathbb{1}_E)$ réflexions.

En effet,

$$\begin{aligned} \dim(\ker(f' - \mathbb{1}_H)) &= \dim(\ker(f - \mathbb{1}_E)) - 1 \\ \Leftrightarrow \dim(H) - \text{rang}(f' - \mathbb{1}_H) &= \dim(E) - \text{rang}(f - \mathbb{1}_E) - 1 \text{ par le théorème 2.6} \\ \Leftrightarrow \text{rang}(f - \mathbb{1}_E) &= \text{rang}(f' - \mathbb{1}_H). \end{aligned}$$

Cas 2 : Si $f(v_0) \neq v_0$, considérons alors $H' = (v_0 - f(v_0))^\perp$, l'hyperplan de E médian au vecteur $v_0 - f(v_0)$, et $s_{H'} \in O(E)$.

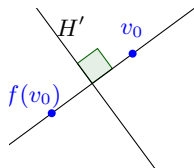


FIGURE 1. $H' = (v_0 - f(v_0))^\perp$

Remarquons que $s_{H'} \circ f(v_0) = s_{H'}(f(v_0)) = v_0$. On a donc que $s_{H'} \circ f$ fixe v_0 , on retrouve donc le cas 1, et

$s_{H'} \circ f = s_{H_1} \circ s_{H_2} \circ \dots \circ s_{H_m}$ où $m = \text{rang}(s_{H'} \circ f - \mathbb{1}_E)$, et donc $f = s_{H'} \circ s_{H_1} \circ s_{H_2} \circ \dots \circ s_{H_m}$ et f est composée de $m + 1$ réflexions.

Montrons que $m + 1 = \text{rang}(f - \mathbb{1}_E)$.

Soit $x \in E \setminus \langle v_0 \rangle$. Puisque $E = \langle v_0 \rangle \oplus H'$, alors il existe $\lambda, \gamma \in \mathbb{R}$ tels que $x = \lambda v_0 + \gamma y$ pour $y \in H' \setminus \{0\}$. Si x est fixé par $s_{H'} \circ f$, alors

$$\begin{aligned} x = \lambda v_0 + \gamma y &= (s_{H'} \circ f)(\lambda v_0 + \gamma y) \\ &= \lambda (s_{H'} \circ f)(v_0) + \gamma (s_{H'} \circ f)(y) \\ &= \lambda v_0 + \gamma (s_{H'} \circ f)(y). \end{aligned}$$

On doit donc avoir $(s_{H'} \circ f)(y) = y$, c'est-à-dire $f(y) = y$, car alors $f(y) \in H'$ et $s_{H'}(f(y)) = f(y) = y$.

On a donc que

$$\begin{aligned}\dim(\text{fix}(s_{H'} \circ f|_{E \setminus \langle v_0 \rangle})) &= \dim(\text{fix}(f)) \\ \Leftrightarrow \dim(\text{fix}(s_{H'} \circ f)) &= \dim(\text{fix}(f)) + \dim(\langle v_0 \rangle) \\ &= \dim(\text{fix}(f)) + 1,\end{aligned}$$

et ainsi

$$\begin{aligned}\dim(\ker(s_{H'} \circ f - \mathbb{1}_E)) &= \dim(\ker(f - \mathbb{1}_E)) + 1 \\ \Leftrightarrow n - \text{rang}(s_{H'} \circ f - \mathbb{1}_E) &= n - \text{rang}(f - \mathbb{1}_E) + 1 \text{ par le théorème 2.6} \\ \Leftrightarrow \text{rang}(s_{H'} \circ f - \mathbb{1}_E) + 1 &= \text{rang}(f - \mathbb{1}_E) \\ \Leftrightarrow m + 1 &= \text{rang}(f - \mathbb{1}_E).\end{aligned}$$

Alors $m + 1 = \text{rang}(f - \mathbb{1}_E)$ et f est composée d'exactly $\text{rang}(f - \mathbb{1}_E)$ réflexions. ■

2.2. Classification des sous-groupes finis de $O(\mathbb{R}^2)$. Soit (e_1, e_2) la base canonique de $\mathbb{R}^2$. Voir la figure 2.

Proposition 2.9. *Soit $s \in O(\mathbb{R}^2)$, une réflexion par rapport à la droite $\mathbb{R}\alpha$. Alors s admet comme matrice (dans la base e_1, e_2)*

$$M_s = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix},$$

où $\theta = 2\langle e_1, \alpha \rangle$.

Preuve. Soit $\beta \in (\mathbb{R}\alpha)^\perp \setminus \{0\}$, alors $B' = \left(\frac{\alpha}{|\alpha|}, \frac{\beta}{|\beta|} \right)$ est une base orthonormale de $\mathbb{R}^2$ telle que la matrice de s dans la base B' est donnée par

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

On peut voir sur la figure 2 que, dans la base (e_1, e_2) , on a

$$\frac{\alpha}{|\alpha|} = \begin{pmatrix} \cos(\gamma) \\ \sin(\gamma) \end{pmatrix} \text{ et } \frac{\beta}{|\beta|} = \begin{pmatrix} -\sin(\gamma) \\ \cos(\gamma) \end{pmatrix}.$$

On a donc le changement de base

$$P = \begin{pmatrix} \cos(\gamma) & -\sin(\gamma) \\ \sin(\gamma) & \cos(\gamma) \end{pmatrix}$$

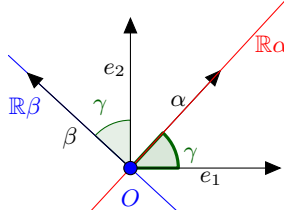


FIGURE 2. La réflexion par rapport à la droite $\mathbb{R}\alpha$ peut être définie comme une réflexion d'angle γ , où $\gamma = \langle e_1, \alpha \rangle$, puisque cet angle détermine la droite $\mathbb{R}\alpha$.

de B' à la base canonique B' , on a que

$$\begin{aligned} M_{s(e_1, e_2)} &= PM_{sB'}P^{-1} \\ &= \begin{pmatrix} \cos(2\gamma) & \sin(2\gamma) \\ \sin(2\gamma) & -\cos(2\gamma) \end{pmatrix}. \end{aligned}$$

■

Proposition 2.10. Soit $r_\theta \in O(\mathbb{R}^2)$, une rotation d'angle θ . Alors r_θ admet comme matrice (dans la base e_1, e_2)

$$M_{r_\theta} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Démonstration. On a que $r_\theta(e_1) = \begin{pmatrix} \cos(\theta) \\ \sin(\theta) \end{pmatrix}$ et $r_\theta(e_2) = \begin{pmatrix} -\sin(\theta) \\ \cos(\theta) \end{pmatrix}$.

On a donc bien que la matrice de r_θ dans la base (e_1, e_2) est celle décrite précédemment.

■

Notation 2.11. À partir de ce point, une rotation de $O(\mathbb{R}^2)$ d'angle θ sera notée r_θ et une réflexion par rapport à la droite $\mathbb{R}\alpha$, et par rapport à l'angle $\gamma = \langle e_1, \alpha \rangle$, sera notée s_γ .

Proposition 2.12. Soient $s_\theta, s_\gamma, r_\alpha, r_\beta \in O(\mathbb{R}^2)$, alors on a les résultats suivants :

$$(1) \quad s_\theta \circ s_\gamma = \begin{pmatrix} \cos(2\gamma - 2\theta) & -\sin(2\gamma - 2\theta) \\ \sin(2\gamma - 2\theta) & \cos(2\gamma - 2\theta) \end{pmatrix} = r_{2(\gamma - \theta)}$$

où $2(\gamma - \theta)$ est l'angle entre les deux droites déterminées par θ et γ ,

$$(2) \quad r_\alpha \circ r_\beta = r_{\alpha + \beta} \text{ et}$$

$$(3) \quad s_\theta \circ r_\alpha \circ s_\theta = r_{-\alpha}, \text{ ce qui revient à dire que } r_\alpha \circ s_\theta = s_\theta \circ r_{-\alpha}.$$

Preuve. Il suffit de faire le produit des matrices 2×2 pour se convaincre. ■

Remarque 2.13. Par le théorème 2.8, et puisque $\dim(\mathbb{R}^2) = 2$, alors les seules isométries de $\mathbb{R}^2$ sont les isométries composées de 0 réflexions (l'identité), 1 réflexion (les réflexions) et 2 réflexions. Par la proposition 2.12 la composition de deux réflexions est une rotation. Ainsi, les seules isométries de $\mathbb{R}^2$ sont l'identité, les réflexions et les rotations.

Notation 2.14. Le groupe cyclique d'ordre n , souvent dénoté C_n , sera noté $\mathbb{Z}/n\mathbb{Z}$. Ces deux notations sont équivalentes.

Proposition 2.15. Soit $G \leq SO((\mathbb{R}^2))$ fini tel que $|G| = n$, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Preuve. Soit $G \leq SO((\mathbb{R}^2))$ tel que $|G| = n$. Alors

$$G = \{e = r_0, r_{\theta_1}, r_{\theta_2}, \dots, r_{\theta_{n-1}}\} \text{ où } \theta_1 < \theta_2 < \dots < \theta_{n-1} \in (0, 2\pi].$$

Supposons qu'il existe $r_\gamma \in G$ tel que $\gamma \notin \mathbb{Z}\theta_1$. Il existe donc $k \in \mathbb{Z}$ tel que

$$k\theta_1 < \gamma < (k+1)\theta_1,$$

ce qui implique que $0 < \gamma - k\theta_1 < \theta_1$. Or, $r_{\gamma-k\theta_1} = r_\gamma \circ (r_{\theta_1})^{-k} \in G$, puisque G est un groupe, et on a que $\gamma - k\theta_1 < \theta_1$. On obtient donc une contradiction avec la minimalité de θ_1 . Il faut donc admettre que $\theta_i = i\theta_1, \forall 1 \leq i \leq n-1$, et on a $G = \langle r_{\theta_1} \rangle$.

Considérons le morphisme

$$\begin{aligned} f : \mathbb{Z} &\rightarrow G \\ m &\mapsto r_{\theta_1}^m. \end{aligned}$$

On a que $\ker(f) = n\mathbb{Z}$ et que f est surjective, donc par le premier théorème d'isomorphisme, on a que $G \simeq \mathbb{Z}/n\mathbb{Z}$. ■

Définition 2.16. Le groupe diédral d'ordre $2n$, noté D_n , est le groupe des isométries qui fixent un polygône régulier à n sommets. Une présentation de D_n est

$$\langle r, s \mid r^n = s^2 = (sr)^2 = e \rangle,$$

où e dénote l'identité du groupe.

Proposition 2.17. Soit $G \leq O(\mathbb{R}^2)$ fini d'ordre n . Alors soit $G \simeq \mathbb{Z}/n\mathbb{Z}$, soit $G \simeq D_{\frac{n}{2}}$.

Preuve. Considérons tout d'abord $H = G \cap SO(\mathbb{R}^2)$. Il s'agit d'un sous-groupe fini de $SO(\mathbb{R}^2)$, d'où par le théorème 2.15, $H \simeq \mathbb{Z}/m\mathbb{Z}$, avec $m = |H| \leq n$. Notons $\theta_0 = \frac{2\pi}{m}$ tel que $\langle r_{\theta_0} \rangle = H$.

Cas 1 : $m = n$. Alors $H = G$ et $G \simeq \mathbb{Z}/m\mathbb{Z}$.

Cas 2 : $m < n$. Alors il existe au moins un élément $s \in G \setminus H$. Puisque

$$\det(s(r_{\theta_0})^k) = -1 \quad \text{pour tout } k \in \{0, 1, \dots, (m-1)\},$$

alors on a que sH contient $|H| = m$ réflexions.

Supposons qu'il existe $s_\gamma \in G \setminus sH$ une autre réflexion, alors $\det(s \circ s_\gamma) = 1$ et $s \circ s_\gamma \in H$. Cela implique alors que $s_\gamma \in sH$, car $s^2 = e$.

On a donc que $G = \langle s, r_{\theta_0} \mid s^2 = (r_{\theta_0})^n = (sr_{\theta_0})^2 = e \rangle$ et donc $G \simeq D_m$ et $n = 2m$. ■

3. CLASSIFICATION DES SOUS-GROUPES FINIS DE $SO(\mathbb{R}^3)$

Tout au long de cette section, nous considérerons G un groupe fini doté d'un élément neutre e et W un ensemble.

3.1. Formule de Burnside. Rappelons tout d'abord quelques notions essentielles à la compréhension de la formule de Burnside.

Définition 3.1. On définit une action de G sur W par une application

$$\begin{aligned} G \times W &\rightarrow W \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

vérifiant les propriétés suivantes :

- 1) $e \cdot x = x \ \forall x \in W$ et
- 2) $g' \cdot (g \cdot x) = (g'g) \cdot x$ pour tout $g', g \in G$ et pour tout $x \in E$.

Définition 3.2. Soit $x \in W$. On appelle orbite de x , notée Ω_x , l'ensemble défini par

$$\Omega_x = \{g \cdot x \mid g \in G\}.$$

Remarque 3.3. Puisque $g^{-1} \in G$ et que $e \cdot x = x$, alors on a que $x \in \Omega_y, \forall y \in \Omega_x$ et $\Omega_x = \Omega_y$. Il suffit donc de choisir un élément de l'orbite comme représentant pour qu'elle soit bien identifiée.

Notation 3.4. On note Ω l'ensemble des orbites de W sous l'action de G . Il est facile de voir que Ω est une partition de W .

Définition 3.5. Soit $g \in G$. L'ensemble des points de W fixés par g sous l'action de G sur W , noté $\text{fix}(g)$, est donné par l'ensemble

$$\text{fix}(g) = \{x \in W \mid g \cdot x = x\}.$$

Définition 3.6. Soit $x \in W$. L'ensemble des éléments de G fixant x sous l'action de G sur W , noté $\text{stab}(x)$, est donné par

$$\text{stab}(x) = \{g \in G \mid g \cdot x = x\}.$$

Théorème 3.7 (Théorème de Lagrange). *Soit $H \leq G$ alors $|G| = |H||G/H|$.*

Démonstration. Soit $H \leq G$. Considérons $G/H = \{gH \mid g \in G\}$, l'ensemble des classes à gauche de H . Ces classes à gauche forment une partition de G et chaque classe a le même cardinal que H . On a donc bien que $|G| = |G/H||H|$. ■

Théorème 3.8 (Formule de Burnside). *Le nombre d'orbites de W sous l'action de G sur W , $|\Omega|$ est donnée par*

$$(4) \quad |\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|.$$

Remarque 3.9. La structure de la preuve provient de l'exercice 17 du chapitre 5 de [1].

Démonstration. 1) Considérons X, Y deux ensembles finis de W , $S \subseteq X \times Y$ et les sous-ensembles de S suivants :

$$S(a, \cdot) = \{(x, y) \in S \mid x = a\} \text{ et } S(\cdot, b) = \{(x, y) \in S \mid y = b\}.$$

Montrons que les deux ensembles suivants sont des partitions de S :

$$A = \{S(a, \cdot) \mid a \in X\} \text{ et } B = \{S(\cdot, b) \mid b \in Y\}.$$

Si on considère $(a, b) \in S$, par définition de S on a que $a \in X$ et donc

$$(a, b) \in S(a, \cdot) \subseteq A.$$

Par le même raisonnement, on a que $(a, b) \in S(\cdot, b) \subseteq B$. Ainsi,

$$S = \bigcup_{a \in X} S(a, \cdot) = \bigcup_{b \in Y} S(\cdot, b).$$

Il nous reste donc à montrer que si $a \neq b$, alors on a

$$S(a, \cdot) \cap S(b, \cdot) = \emptyset \text{ et } S(\cdot, a) \cap S(\cdot, b) = \emptyset.$$

$S(a, \cdot) = \{(a, y) \in S \mid y \in Y\}$, $S(b, \cdot) = \{(b, y) \in S \mid y \in Y\}$ et pour tous $x, y \in Y$, on a que $(a, x) \neq (b, y)$ puisque $a \neq b$. Il est donc facile de voir que $S(a, \cdot) \cap S(b, \cdot) = \emptyset$ et que A est bien une partition de S . Le même raisonnement permet de montrer que B est également une partition de S .

On peut donc en déduire que

$$|S| = \sum_{a \in X} |S(a, \cdot)| = \sum_{b \in Y} |S(\cdot, b)|.$$

2) Appliquons maintenant la partie 1) de la preuve à notre groupe G et notre ensemble E en définissant $S = \{(g, x) \in G \times W \mid g \cdot x = x\}$.

Il est facile d'établir une bijection entre $S(g, \cdot)$ et $\text{fix}(g)$. En effet, pour g fixé, on a que

$$\begin{aligned} S(g, \cdot) &= \{(g, x) \mid x \in W \text{ et } g \cdot x = x\} \\ &= \{(g, x) \mid x \in \text{fix}(g)\}. \end{aligned}$$

On a donc que $|S(g, \cdot)| = |\text{fix}(g)|$.

De même, il est facile d'établir une bijection entre $S(\cdot, x)$ et $\text{stab}(x)$, puisque pour x fixé

$$\begin{aligned} S(\cdot, x) &= \{(g, x) \mid g \in G \text{ et } g \cdot x = x\} \\ &= \{(g, x) \mid g \in \text{stab}(x)\}. \end{aligned}$$

On a donc que $|S(\cdot, x)| = |\text{stab}(x)|$.

Notons $t = |\Omega|$ le nombre d'orbites de W sous l'action de G . Pour chaque orbite i , pour $1 \leq i \leq t$, on choisit un représentant arbitraire x_i des éléments de l'orbite et cette orbite est donc notée Ω_{x_i} .

Par la partie 1), on a que

$$\sum_{g \in G} |S(g, \cdot)| = \sum_{x \in W} |S(\cdot, x)|.$$

On a donc que

$$(5) \quad \sum_{g \in G} |\text{fix}(g)| = \sum_{x \in W} |\text{stab}(x)| = \sum_{i=1}^t \sum_{x \in \Omega_{x_i}} |\text{stab}(x)|.$$

3) Montrons que $\sum_{x \in \Omega_{x_i}} |\text{stab}(x)| = |\Omega_{x_i}| |\text{stab}(x_i)|$.

Soit $x \in \Omega_{x_i}$. Alors il existe $h \in G$ tel que $x = hx_i$. On a que

$$\begin{aligned} \text{stab}(x) &= \{g \in G \mid gx = x\} \\ &= \{g \in G \mid g(hx_i) = hx_i\} \\ &= \{g \in G \mid h^{-1}ghx_i = x_i\}. \end{aligned}$$

On a ainsi une bijection

$$\begin{aligned} \text{stab}(x) &\rightarrow \text{stab}(x_i) \\ g &\mapsto h^{-1}gh \end{aligned}$$

et $|\text{stab}(x)| = |\text{stab}(x_i)|$, ce qui entraîne $\sum_{x \in \Omega_{x_i}} |\text{stab}(x)| = |\Omega_{x_i}| |\text{stab}(x_i)|$.

Notre équation (5) devient

$$(6) \quad \sum_{g \in G} |\text{fix}(g)| = \sum_{i=1}^t |\Omega_{x_i}| |\text{stab}(x_i)|.$$

4) Montrons que $|\Omega_{x_i}| |\text{stab}(x_i)| = |G| \quad \forall 1 \leq i \leq t$, c'est-à-dire que $|\Omega_{x_i}| = |G/\text{stab}(x)|$ par le Théorème de Lagrange, voir théorème 3.7.

Notons $\text{stab}(x) = G_x$ pour cette partie de la preuve.

Considérons l'application suivante :

$$\begin{aligned} \tau : G/G_x &\rightarrow \Omega_x \\ gG_x &\mapsto gx. \end{aligned}$$

Montrons tout d'abord qu'elle est bien définie. Soit $g, h \in G$.

$$\begin{aligned} gx = hx &\Leftrightarrow g^{-1}hx = x \\ &\Leftrightarrow g^{-1}h \in G_x \\ &\Leftrightarrow hG_x = gG_x \end{aligned}$$

Cela démontre aussi que τ est injective.

On a également que τ est surjective, puisque

$$\Omega_x = \{gx \mid g \in G\} = \{\tau(gG_x) \mid g \in G\} = \tau(G/G_x).$$

τ est donc une bijection, ce qui entraîne $|\Omega_{x_i}| = |G/\text{stab}(x)|$. Ainsi $|\Omega_{x_i}| |\text{stab}(x_i)| = |G| \quad \forall 1 \leq i \leq t$ et l'équation 6 devient finalement

$$\sum_{g \in G} |\text{fix}(g)| = t|G|,$$

d'où découle la formule de Burnside. ■

Exemple 3.10. L'exemple suivant permet de visualiser et mettre en pratique les résultats obtenus au cours de la preuve précédente. Voir la figure 3. Considérons $G = D_3 = \langle s, r \mid s^2 = r^3 = (sr)^2 = e \rangle$, où $s = s_0, r = r_{2\pi/3}$, le groupe diédral fixant le triangle équilatéral. L'ensemble sur lequel agit D_3 est l'ensemble des sommets du triangle équilatéral.

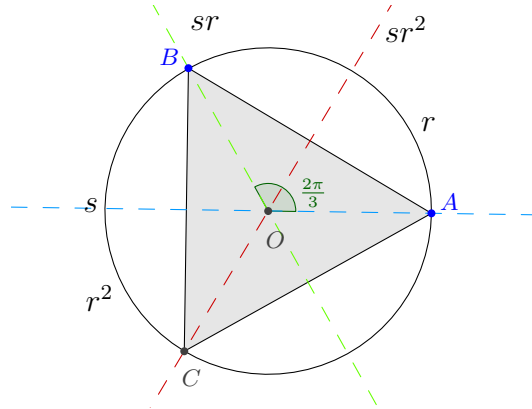


FIGURE 3. D_3 compte l'ensemble des réflexions et des rotations qui fixent le triangle équilatéral.

Les hyperplans associés aux réflexions sont indiqués par des lignes pointillées de couleurs : bleu pour s , rouge pour $s_{\frac{2\pi}{3}} = sr^2$ et vert pour $s_{\frac{4\pi}{3}} = sr$. Les rotations sont indiquées par un arc de cercle d'angle $\frac{2k\pi}{3}$ pour $0 \leq k \leq 2$.

Par la formule de Burnside, on aura

$$\begin{aligned} \frac{1}{|D_3|} \sum_{g \in D_3} |\text{fix}(g)| &= \frac{1}{6} (\text{fix}(e) + \text{fix}(r) + \text{fix}(r^2) + \text{fix}(s) + \text{fix}(sr) + \text{fix}(sr^2)) \\ &= \frac{1}{6} (3 + 0 + 0 + 1 + 1 + 1) = 1 = |\Omega|. \end{aligned}$$

De plus, vérifions dans cet exemple un résultat de la preuve, énonçant que $D_3/\text{stab}(A)$ et Ω_A sont en bijection. On a que $\text{stab}(A) = \{e, s\}$, $\Omega_A = \{A, B, C\}$ et $D_3/\text{stab}(A) = \{\{e, s\}, \{r, sr\}, \{r^2, sr^2\}\}$, où r stabilise A , sr stabilise B et sr^2 stabilise C , ce qui décrit notre bijection. On obtient donc bien que :

$$3 \cdot 2 = |\Omega_A| \cdot |\text{stab}(A)| = |D_3| = 6.$$

3.2. Théorèmes de Sylow.

Théorème 3.11 (Théorème de Sylow, première partie). *Soit p un nombre premier divisant l'ordre de G . Si $|G| = sp^n$, avec $p \nmid s$, alors il existe un sous-groupe H de G d'ordre $p^r \forall r \in \mathbb{N}$ tel que $1 \leq r \leq n$.*

Démonstration. Supposons qu'il existe $s, p, n \in \mathbb{N}$, avec p premier, tels que $|G| = sp^n$ et $p \nmid s$. Notons F l'ensemble des sous-ensembles de G qui sont de cardinalité p^r pour r fixé, $1 \leq r \leq n$.

1) Montrons tout d'abord que $|F| = \lambda p^{n-r}$ où λ est un entier non divisible par p . On a que

$$\begin{aligned} |F| &= \binom{sp^n}{p^r} = \frac{(sp^n)!}{(p^r)!(sp^n - p^r)!} \\ &= \frac{sp^n \cdot (sp^n - 1) \cdots (sp^n - (p^r - 1))}{p^r \cdot (p^r - 1) \cdots 2 \cdot 1} \\ &= sp^{n-r} \prod_{k=1}^{p^r-1} \frac{sp^n - k}{k}. \end{aligned}$$

Pour tout $1 \leq k \leq p^r - 1$, il existe $q_k, \alpha_k \in \mathbb{N}$ avec q_k non divisible par p et $0 \leq \alpha_k \leq r$ tels que k peut s'écrire $k = q_k p^{\alpha_k}$. Ainsi, pour tout k , on a

$$\begin{aligned} \frac{sp^n - k}{k} &= \frac{sp^n - q_k p^{\alpha_k}}{q_k p^{\alpha_k}} \\ &= \frac{p^{\alpha_k}(sp^{n-\alpha_k} - q_k)}{p^{\alpha_k} \cdot q_k} \\ &= \frac{sp^{n-\alpha_k} - q_k}{q_k}. \end{aligned}$$

Puisque $p \nmid q_k$, alors $p \nmid sp^{n-\alpha_k} - q_k$ et donc ni le numérateur, ni le numérateur de $\frac{sp^n - k}{k}$ est divisible par p . On a donc que

$$|F| = p^{n-r} \left(s \prod_{k=1}^{p^r-1} \frac{sp^n - k}{k} \right) = p^{n-r} \lambda,$$

où λ est un entier non divisible par p .

2) Considérons maintenant $A \in F$. On a donc que $|A| = p^r$ et $\forall g \in G, |gA| = |A|$. On a donc que G opère sur F par translation à gauche. Nous pouvons ainsi considérer $\{A_i\}_{1 \leq i \leq t}$ la famille de représentants des t orbites distinctes de F sous l'action de G .

Notons $G_{A_i} = \text{stab}(A_i) \leq G$. Puisque $|F| = \sum_{i=1}^t |\Omega_{A_i}|$ et $|\Omega_{A_i}| = |G/G_{A_i}|$, on a que $|F| = \sum_{i=1}^t |G/G_{A_i}|$.

Cela implique que

$$\lambda p^{n-r} = \sum_{i=1}^t |G/G_{A_i}|.$$

Il existe donc au moins un entier $1 \leq h \leq t$ tel que $p^{n-r+1} \nmid |G/G_{A_h}|$.

Posons $H = G_{A_h}$. Par le théorème de Lagrange en théorème 3.7, on a que $|G| = sp^n = |H||G/H|$. Puisque $p^{n-r+1} \nmid |G/H|$, alors il faut que $|G/H| = s'p^\alpha$, où $s', \alpha \in \mathbb{N}$, avec s' divise s et $0 \leq \alpha \leq n - r$.

Si on pose $s = s's''$, on a également que $|H| = s''p^{n-\alpha}$. Or, $0 \leq \alpha \leq n - r$ implique $r \leq n - \alpha \leq n$. On a donc que p^r divise $|H|$, d'où $p^r \leq |H|$.

On a également que $H = G_{A_h}$, pour $A_h \in F$. Ainsi pour tous $g, g' \in G_{A_h}$, $gA_h = g'A_h = A_h$, par la définition du stabilisateur de A_h , et que si $g \neq g'$, alors $gx \neq g'x \quad \forall x \in A_h$.

En effet, puisque G est un groupe et que $A_h \in F \subseteq G$, alors $\forall x \in A_h$,

$$gx = g'x \Leftrightarrow g = g'.$$

On doit donc avoir $|H| = |G_{A_h}| \leq |A_h| = p^r$. Il est également possible de démontrer ceci par contradiction en utilisant le dernier argument et en supposant que $|G_{A_h}| > |A_h|$.

Comme $p^r \leq |H| \leq p^r$, il faut donc que $|H| = p^r$. ■

Définition 3.12. Soit p un nombre premier divisant $|G| = sp^n$, où $p \nmid s$. Par le théorème 3.11, il existe un sous-groupe H de G d'ordre $p^r \quad \forall r \in \mathbb{N}$ tel que $1 \leq r \leq n$. Un p -sous-groupe de Sylow est un sous-groupe de G d'ordre p^n .

Théorème 3.13 (théorème de Sylow, deuxième partie). *Tous les p -Sylow de G sont conjugués entre eux.*

Démonstration. Voir la preuve dans [5]. ■

Théorème 3.14 (théorème de Sylow, troisième partie). *Soit n_p le nombre de p -sous-groupes de Sylow de G , pour $|G| = sp^n$ alors $n_p \mid s$ et $n_p \equiv 1 \pmod{p}$.*

Démonstration. Voir la preuve dans [5]. ■

3.3. Polyèdres réguliers et les groupes de rotations les préservant. Maintenant que ces théorèmes ont été énoncés et prouvés, nous pouvons nous attaquer au problème qui nous intéresse ici, qui est de classifier les sous-groupes finis de $SO(\mathbb{R}^3)$.

Nous introduirons tout d'abord les polyèdres réguliers de Platon, car ils sont centraux dans la classification des sous-groupes finis de $SO(\mathbb{R}^3)$. Connus depuis l'Antiquité, et étudiés systématiquement par Theatetus vers 380 avant J.-C., les polyèdres réguliers, aussi nommés solides de Platon ou polyèdres platoniciens, sont les polyèdres convexes

dont toutes les faces sont des polygones réguliers isométriques. Euclide fut le premier à montrer qu'il n'en existe que 5, apparaissant sur la figure 4.

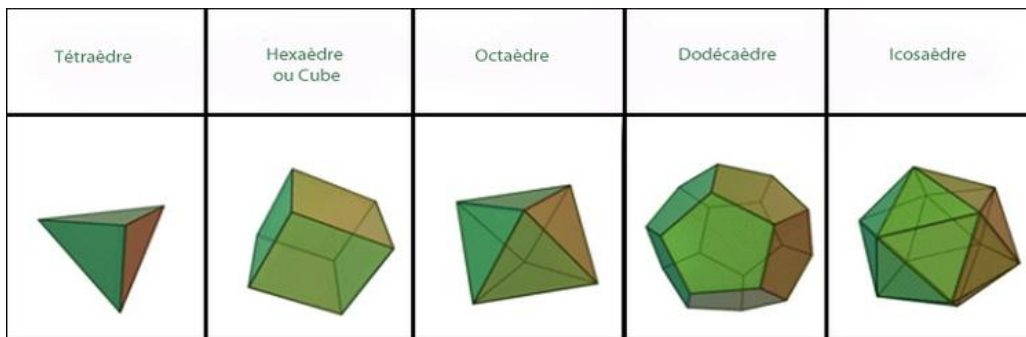


FIGURE 4. Solides de Platon [4]

Définition 3.15. Le tétraèdre est le polyèdre régulier composé de 4 faces, qui sont des triangles équilatéraux, 6 arêtes et 4 sommets.

Remarque 3.16. Le tétraèdre est auto-dual, c'est-à-dire qu'en joignant le centre des faces adjacentes on obtient à nouveau un tétraèdre.

Proposition 3.17. *Considérons le tétraèdre et T le groupe de des rotations qui préservent le tétraèdre. T consiste en les rotations d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$ dont les axes de rotation passent par le centre du tétraèdre et un des quatre sommets, en bleu sur la figure 5, les rotations d'angle π dont les axes de rotation passent par le centre des arêtes opposées, en rouge sur la figure 5, ainsi que l'identité. Ainsi*

$$|T| = 4 \cdot 2 + 3 \cdot 1 + 1 = 12.$$

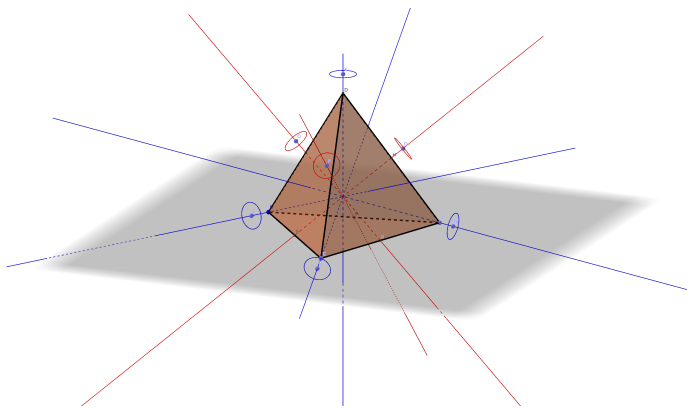


FIGURE 5. L'ensemble des rotations du tétraèdre

Définition 3.18. Le cube est le polyèdre régulier composé de 6 faces, qui sont des carrés, 12 arrêtes et 8 sommets.

Définition 3.19. L'octaèdre est le polyèdre régulier composé de 8 faces, qui sont des triangles équilatéraux, 12 arrêtes et 6 sommets.

Remarque 3.20. Le cube et l'octaèdre sont duaux, c'est-à-dire qu'il suffit de joindre le centre des faces adjacentes du cube pour obtenir l'octaèdre, et inversement. Ainsi les isométries qui préservent le cube préservent également l'octaèdre, et inversement. Voir la figure 6.

FIGURE 6. Une illustration de la dualité du cube et de l'octaèdre



Proposition 3.21. Considérons le cube et W les rotations le préservant. On a également que W préserve l'octaèdre. Voir la remarque 3.20 et la figure 6.

Les rotations du cube sont de trois types différents en plus de l'identité. Voir la figure 7 et la figure 8. Il y a les rotations d'angle $\frac{\pi}{2}$, π et $\frac{3\pi}{2}$ ayant comme axe de rotation les centres des faces opposées, en rouge sur la figure 8 (A), les rotations d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$ ayant comme axe de rotation les sommets opposés, en bleu sur la figure 8 (B), et les rotations d'angle π ayant comme axe de rotation les centres d'arrêtes opposées diagonalement, en vert sur la figure 8 (C). Alors on a que

$$|W| = 3 \cdot 3 + 4 \cdot 2 + 6 \cdot 1 + 1 = 24.$$

Définition 3.22. Le dodécaèdre est le polyèdre régulier composé de 12 faces, qui sont des pentagone réguliers, 30 arrêtes et 20 sommets.

Définition 3.23. L'icosaèdre est le polyèdre régulier composé de 20 faces, qui sont des triangles équilatéraux, 30 arrêtes et 12 sommets.

Remarque 3.24. Le dodécaèdre et l'icosaèdre sont duaux, c'est-à-dire qu'il suffit de joindre le centre des faces adjacentes du dodécaèdre pour obtenir l'icosaèdre, et inversement. Ainsi, tout comme pour le cube et l'octaèdre, les isométries qui préservent le dodécaèdre préservent également l'icosaèdre, et inversement. Voir la figure 9.

FIGURE 7. L'ensemble des réflexions du cube

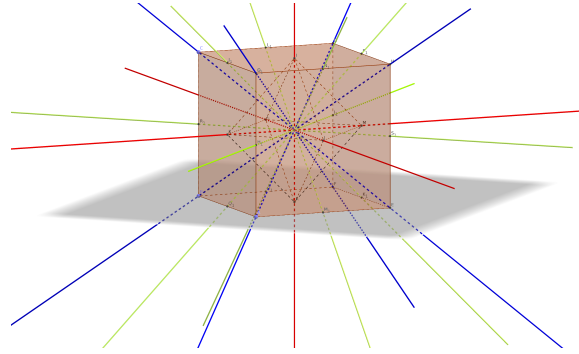


FIGURE 8. Décomposition de la figure 7 selon les types de réflexions

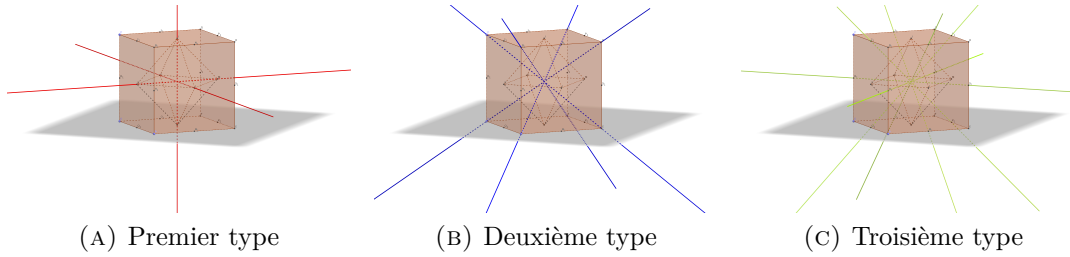
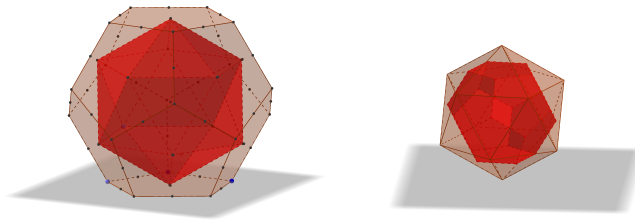


FIGURE 9. Une illustration de la dualité du dodécaèdre et de l'octaèdre



Proposition 3.25. *Considérons le dodécaèdre et D , l'ensemble des rotations préservant le dodécaèdre. On a que D préserve également l'icosaèdre, voir la remarque 3.24 et la figure 9.*

Les rotations préservant le dodécaèdre sont de trois types en plus de l'identité. Voir la figure 10 et la figure 11. Il y a les rotations d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$ dont l'axe de rotation passe par deux sommets opposés, en rouge sur la figure 11 (A), les rotations d'angle $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$ et $\frac{8\pi}{5}$ dont l'axe de rotation passe par le centre de deux faces opposées, en bleu sur la figure 11 (B) et les rotations d'angle π dont l'axe de rotation est le centre des arêtes opposées diagonalement, en vert sur la figure 11 (C). Alors on a que

$$|D| = 10 \cdot 2 + 6 \cdot 4 + 15 \cdot 1 + 1 = 60.$$

FIGURE 10. L'ensemble des réflexions du dodécaèdre

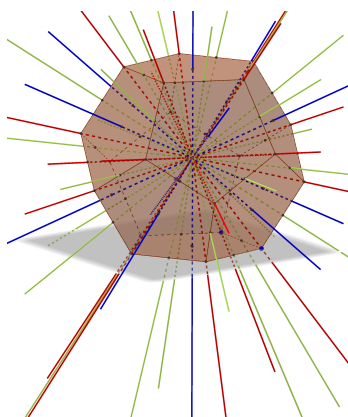
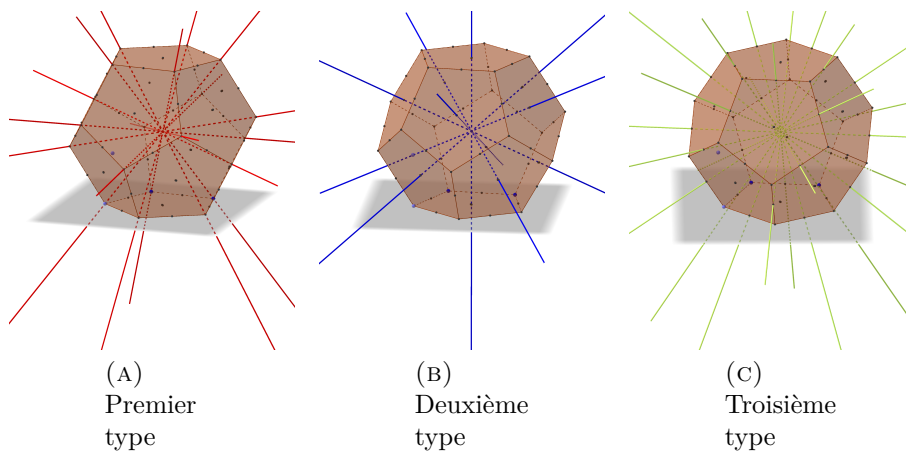


FIGURE 11. Décomposition de la figure 10 selon les types de réflexions



3.4. Classification des sous-groupes finis de $SO(\mathbb{R}^3)$. Nous allons maintenant nous concentrer sur les isométries de $\mathbb{R}^3$, et tout particulièrement sur les rotations de $\mathbb{R}^3$, dont les sous-groupes finis constituent le sujet d'étude de cette section.

Le théorème 2.8 permet d'affirmer que soit $f \in O(\mathbb{R}^3)$, alors f est soit composée de 0 réflexions (alors f est l'identité), soit de 1, 2 ou 3 réflexions. Ainsi $SO(\mathbb{R}^3)$ est le groupe des rotations dans $\mathbb{R}^3$.

Tout au long de cette section, nous considérerons $G \leq SO(\mathbb{R}^3)$ fini avec $|G| = n \geq 2$. De plus, nous nous réduirons à l'étude de l'effet des rotations de $\mathbb{R}^3$ sur S^2 , la sphère de rayon 1, puisque les rotations sont linéaires et donc centrées en zéro dans $\mathbb{R}^3$. Ainsi cette étude restreinte est suffisante pour comprendre l'effet des rotations sur $\mathbb{R}^3$.

Lemme 3.26. *Soit $g \in G$ une rotation non triviale. L'élément g fixe une droite $\mathbb{R}\alpha$, définissant ainsi deux pôles sur S^2 , $p = \frac{\alpha}{|\alpha|}$ et $-p$, et induit une rotation de $\mathbb{R}^2$ sur l'hyperplan $(\mathbb{R}\alpha)^\perp$. Soit a, b , deux vecteurs linéairement indépendants formant une base orthonormée de cet hyperplan. Dans cette base, les coordonnées de p et $-p$ sont $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$.*

Démonstration. Soit M_g la matrice de g dans la base (p, a, b) ,

$$M_g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

On a que $\det(M_g) = 1$, donc $M_g \in SO(\mathbb{R}^3)$. Il est facile de se convaincre que le comportement de g est tel que décrit en observant la matrice, et que les coordonnées de p et $-p$ sont telles que décrit.

■

Lemme 3.27. *Soit $g \in G \setminus \{e\}$ et $p, -p$ les deux pôles de g . Soit $h \in G \setminus \{g\}$, alors $h(p)$ est un pôle de hgh^{-1} . Ainsi, G agit sur l'ensemble P des pôles des éléments de $G \setminus \{e\}$ et $2 \leq |P| \leq 2(n-1)$.*

Démonstration. On voit facilement que $hgh^{-1}(h(p)) = hg(p) = h(p)$ et donc $h(p)$ est un pôle de hgh^{-1} . Ainsi P est stable sous l'action de G .

Considérons P l'ensemble des pôles des éléments de $G \setminus \{e\}$. On a démontré que chaque élément non trivial de G possède deux pôles, puisque $G \leq SO(\mathbb{R}^3)$. Ainsi $|P| = 2m$ pour $m \in \mathbb{N}$ et $1 \leq m \leq n-1$. En effet, si toutes les rotations de $G \setminus \{e\}$ préservent

des pôles distincts, alors $|P| = 2(n-1)$, et si elles préservent toutes les mêmes pôles, alors $|P| = 2$ puisque $|G| \geq 2$.

■

Définition 3.28. Le groupe symétrique d'indice n , noté Sym_n , est le groupe de permutation de l'ensemble $\{1, 2, 3, \dots, n-1, n\}$. Il est engendré par les transpositions, notées (ij) , qui consistent à échanger la position de deux éléments, ici i et j , $1 \leq i < j \leq n$. Les permutations peuvent être écrites comme la composition de transpositions ou de cycles disjoints. Le signe d'une permutation θ , notée $\text{sign}(\theta)$ est pair si elle s'écrit comme un nombre pair de transpositions, et impair sinon.

Remarque 3.29. En représentant les éléments de Sym_n comme une matrice $n \times n$ formée à partir de la matrice identité $n \times n$ en permutant ses lignes, alors il est possible, par bijection, d'identifier Sym_n à un groupe des isométries de $\mathbb{R}^n$, où une transposition de Sym_n est associée à une réflexion de $O(\mathbb{R}^n)$.

Définition 3.30. Le groupe alterné d'indice n , noté Alt_n , est un sous-groupe de Sym_n composé des permutations paires de Sym_n .

Théorème 3.31. Soit $G \leq SO(\mathbb{R}^3)$ avec $|G| = n \geq 2$. Alors soit $G \simeq \mathbb{Z}/n\mathbb{Z}$, soit $G \simeq D_{\frac{n}{2}}$, soit G est isomorphe à un des trois groupes de rotations qui préservent les polyèdres réguliers, qui correspondent à Alt_4 , Sym_4 et Alt_5 .

Remarque 3.32. Les quatre premiers cas de cette preuve représentent une version détaillée de la preuve qu'il est possible de trouver dans [2]. La preuve s'inspire également de celle trouvée au ch. 2 de [3]. Le cinquième cas est rarement inclus dans les preuves, il serait ici particulièrement détaillé et prouvé par deux approches différentes. Les principales ressources qui ont aidé à écrire la preuve du cinquième cas sont les suivantes : [6], [7], [8] et [9].

Démonstration. Considérons P , l'ensemble des pôles de $G \setminus \{e\}$. Par le lemme 3.27, G agit sur P et $2 \leq |P| \leq 2(n-1)$. Par la Formule de Burnside en théorème 3.8, on a que le nombre d'orbites de cette action, que l'on notera t , vérifie

$$(7) \quad t = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)| = \frac{1}{n} (|P| + 2(n-1)),$$

puisque e fixe l'ensemble des éléments de P et tous les autres éléments de G fixent exactement 2 pôles.

On peut ainsi établir des restrictions sur le nombre d'orbites t . En effet, par le lemme 3.27, on a que $|P| \geq 2$, alors $t \geq \frac{1}{n} (2 + 2(n-1)) = \frac{2n}{n} = 2$, et puisque $|P| \leq 2(n-1)$, alors $t \leq \frac{1}{n} (2(n-1) + 2(n-1)) = \frac{4(n-1)}{n} = 4 - \frac{1}{n} < 4$. On a donc que les seules possibilités sont $t = 2$ ou $t = 3$.

Considérons tout d'abord le cas où $t = 2$. Si $t = 2$, alors par l'équation (7), on doit donc avoir $|P| = 2$. Il s'ensuit que $P = \{\{p\}, \{-p\}\}$ et tous les éléments de $G \setminus \{e\}$ admettent les mêmes deux pôles, c'est-à-dire qu'ils admettent le même axe de rotation $\mathbb{R}\alpha$. Ainsi $\forall g \in G, g|_{(\mathbb{R}\alpha)^\perp}$ est une rotation du plan $(\mathbb{R}\alpha)^\perp$. Considérons l'isomorphisme

$$\begin{aligned} f : G &\rightarrow G|_{(\mathbb{R}\alpha)^\perp} \\ g &\mapsto g|_{(\mathbb{R}\alpha)^\perp}. \end{aligned}$$

Alors $f(G)$ est un sous-groupe d'ordre n de $SO(\mathbb{R}^2)$ et donc $G \simeq f(G) \simeq \mathbb{Z}/n\mathbb{Z}$.

Considérons maintenant le cas où $t = 3$. Notons P_1, P_2 et P_3 ces trois orbites de P sous l'action de G . Supposons $|P_1| \geq |P_2| \geq |P_3|$ et notons $m_i = \text{fix}(p_k)$ pour un pôle $p_k \in P_i$, $1 \leq i \leq 3$ et $1 \leq k \leq |P_i|$.

Par la preuve de la formule de burnside en théorème 3.8, nous avons montré que $|G| = |\Omega_p| |\text{fix}(p)|$ pour $p \in P$. Si $p \in P_i$, nous avons que $|\Omega_p| = |P_i|$, $\text{fix}(p) = m_i$ et on obtient l'équation suivante :

$$(8) \quad n = |P_i| m_i.$$

Puisque n est fixé et $|P_1| \geq |P_2| \geq |P_3|$, on a donc que $m_1 \leq m_2 \leq m_3$.

À partir de cette inéquation et de l'équation (7), nous allons établir des restreintes sur m_1, m_2 et m_3 .

Commençons par m_1 . Soit $p \in P_1$, p est stable par e et il existe au moins un $g \in G \setminus \{e\}$ tel que $g(p) = p$, puisque $p \in P$ et est donc le pôle d'un élément de G . Ainsi $m_1 \geq 2$.

Par l'équation (7), on a

$$\begin{aligned} t = 3 &= \frac{1}{n} (|P| + 2(n-1)) = \frac{1}{n} (|P_1| + |P_2| + |P_3| + 2(n-1)) \\ &= \frac{1}{n} \left(\frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3} + 2(n-1) \right) \\ &\Leftrightarrow n + 2 = \frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3} \\ (9) \quad &\Leftrightarrow 1 + \frac{2}{n} = \frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3}. \end{aligned}$$

Ainsi

$$\frac{3}{m_1} \geq \frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n} \geq 1,$$

et donc $2 \leq m_1 < 3$ et $m_1 = 2$.

De la même façon, on obtient

$$\frac{2}{m_2} \geq \frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n} > \frac{1}{2},$$

et donc $m_1 = 2 \leq m_2 < 4$. Les deux cas possibles pour m_2 sont $m_2 = 2$ et $m_2 = 3$.

Cas ($m_1 = 2 = m_2$) : Si $m_1 = m_2 = 2$, alors par l'équation (9), $m_3 = \frac{n}{2}$, et donc $|P_3| = 2$ par l'équation (7). Notons $P_3 = \{p, -p\}$. On a que $|\text{stab}(p)| = \frac{n}{2}$. En nous référant au cas $t = 2$, on a que $\text{stab}(p) \simeq \mathbb{Z}/\frac{n}{2}\mathbb{Z}$. Si $g \in G$ ne fixe pas p , alors $g(p) = -p$ et $g(-p) = p$, ce qui signifie que g est une rotation d'angle π et est donc d'ordre 2.

Considérons l'hyperplan H qui est perpendiculaire à la droite contenant p et $-p$. Dans ce plan, g simule une réflexion par rapport à l'axe de rotation de g .

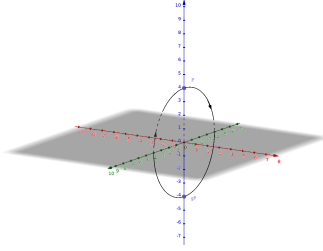


FIGURE 12. On peut observer la réflexion induite par la rotation.

On en déduit que $G \simeq G|_H \simeq D_{\frac{n}{2}} = \langle r, s \mid r^n = s^2 = (sr)^2 = e \rangle$.

Cas ($m_1 = 2, m_2 = 3$) : Si $m_1 = 2$ et $m_2 = 2$, alors par l'équation (9),

$$\frac{1}{m_3} = \frac{1}{6} + \frac{2}{n} > \frac{1}{6},$$

et donc $m_2 = 3 \leq m_3 < 6$. Ainsi $m_3 = 3, m_3 = 4$ ou $m_3 = 5$.

Cas ($m_1 = 2, m_2 = 3 = m_3$) : Par l'équation (9), on a que $n = 12$. Ainsi $|P_1| = \frac{12}{2} = 6, |P_2| = \frac{12}{3} = 4$ et $|P_3| = \frac{12}{3} = 4$ par l'équation (7).

Considérons $P_2 = \{\pm p_1, \pm p_2\}$. P_2 est stable par G , ainsi $\forall g \in G, g$ induit une permutation s_g de P_2 .

Considérons donc le morphisme

$$\begin{aligned} s : G &\rightarrow \text{Sym}_4 \\ g &\mapsto s_g. \end{aligned}$$

Montrons que s est injective. Soit $g \in \ker(s)$, alors s_g est l'identité, ce qui signifie que g envoie les quatre pôles de P_2 sur eux-même, et donc g est l'identité. Ainsi $G \simeq G/\{e\} \simeq s(G) \leq \text{Sym}_4$ et G est isomorphe à un sous-groupe de Sym_4 qui est d'ordre 12.

Montrons que Alt_4 est l'unique sous-groupe de Sym_4 qui soit d'ordre 12. Considérons $H \leq \text{Sym}_4$ tel que $|H| = 12$. Remarquons que $|G/H| = 2$, ce qui implique que H est normal. En effet, soit $g \in G$, si $g \in H$, alors $gH = H = Hg$, et si $g \notin H$, alors $gH = Hg \neq H$.

Cela implique que G/H est un groupe et $G/H \simeq \mathbb{Z}/2\mathbb{Z} \simeq \{-1, 1\}$. Soit (ij) une transposition. Puisque $(ij)^2 = e_{\text{Sym}_4}$ et on a que les transpositions engendrent Sym_4 , alors il faut que $(ij) \mapsto -1 \ \forall 1 \leq i < j \leq 4$, puisque -1 génère $\{-1, 1\}$. Ainsi les éléments pairs de Sym_4 sont envoyés sur 1 et les éléments impairs, sur -1 . Ainsi $G/H = \{\text{Alt}_4, (ij)\text{Alt}_4\}$. Puisque $e_{\text{Sym}_4} \in \text{Alt}_4$ et $e_{\text{Sym}_4} \notin (ij)\text{Alt}_4$, alors il faut $H = \text{Alt}_4$.

Il est également possible de faire la démonstration à l'aide du théorème de Sylow en exploitant le fait que H doit comporter au moins un sous-groupe d'ordre 2 et un sous-groupe d'ordre 3 ($|H| = 12 = 2^2 \cdot 3$). Il doit donc comporter au moins un élément d'ordre 3 (pair) et un élément d'ordre 2 (pair ou impair). Puisqu'un élément d'ordre 2 impair et un élément d'ordre 3 engendrent Sym_4 , il faut donc que les éléments de H d'ordre 2 soient pair, et ainsi $H = \text{Alt}_4$.

On peut donc conclure que $G \simeq \text{Alt}_4$.

Montrons maintenant que Alt_4 est isomorphe à T , le groupe des rotations préservant le tétraèdre. Voir la proposition 3.17 et la figure 5.

Associons les pôles de P_1 au milieu des arêtes du tétraèdre, les pôles de P_2 aux sommets du tétraèdre, et les pôles de P_3 aux centre des faces du tétraèdre. Ainsi le tétraèdre est invariant sous G , et donc $G \leq T$ et $|G| = |T| = 12$, ce qui implique que $T \simeq G \simeq \text{Alt}_4$.

Cas $(m_1 = 2, m_2 = 3, m_3 = 4)$: Par l'équation (9), on a que $n = 24$.

Ainsi $|P_1| = \frac{24}{2} = 12$, $|P_2| = \frac{24}{3} = 8$ et $|P_3| = \frac{24}{4} = 6$ par l'équation (7).

Si $\text{stab}(p) = 3$ pour $p \in P$, alors il faut que $p \in P_2$, puisque $m_2 = 3, m_1 \neq 3$ et $m_3 \neq 3$. De plus, $\text{stab}(-p) = 3$ également alors $p, -p \in P_2$. Ainsi $P_2 = \{\pm p_1, \pm p_2, \pm p_3, \pm p_4\}$.

Si $g \in G \setminus \{e\}$ n'admet pas un pôle dans P_2 , alors g agit comme une permutation sur les couples $(p_i, -p_i)$, puisque les paires de pôles demeurent des paires de pôles sous l'action de G . Si $g \in G \setminus \{e\}$ admet un couple de pôles $\pm p_i \in P_2, 1 \leq i \leq 4$, alors g agit comme une permutation sur les couples $(p_l, -p_l)$, pour $l \in \{1, 2, 3, 4\} \setminus \{i\}$. On a donc un morphisme semblable à celui exploité au cas précédent :

$$\begin{aligned} s : G &\rightarrow \text{Sym}_4 \\ g &\mapsto s_g. \end{aligned}$$

Montrons que s est injective.

Considérons $g \in \ker(s)$, alors g stabilise chaque couple $(p_i, -p_i)$. Si $g(p_i) = p_i \ \forall 1 \leq i \leq 4$, alors g est l'identité. Supposons qu'il existe un $g \in \ker(s) \setminus \{e\}$. Si $g(p_i) = p_i$ pour $1 \leq i \leq 4$, c'est-à-dire que g possède un couple de pôles dans P_2 , alors g permute les trois autres couples, ce qui est une contradiction avec l'hypothèse que $g \in \ker(s)$. Il faut donc $g(p_i) = -p_i \ \forall i \in \{1, 2, 3, 4\}$. Considérons (p_1, p_2, p_3) une base de $\mathbb{R}^3$. On a que

$$g \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} = \begin{pmatrix} -p_1 \\ -p_2 \\ -p_3 \end{pmatrix},$$

ce qui implique que, dans cette base,

$$M_g = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

et $\det(M_g) = -1$, ce qui entraîne que g est une réflexion, une contradiction.

Il faut donc que $\ker(s) = \{e\}$, et s est injectif.

On a ainsi que $s(G) \leq \text{Sym}_4$ et $|G| = 24 = |\text{Sym}_4|$, d'où $G \simeq \text{Sym}_4$.

Montrons maintenant que Sym_4 est isomorphe à W , le groupe des réflexions préservant le cube et l'octaèdre. Voir la proposition 3.21 et les figures 7 et 8.

Si on identifie les pôles de P_1 au milieu des arêtes du cube, les pôles de P_2 aux sommets du cube, et les pôles de P_3 aux centres des faces du cube, on a que le cube est fixé par l'action de G . On a donc que $G \leq W$ et $|G| = |W| = 24$, ainsi $W \simeq G \simeq \text{Sym}_4$.

Cas $(m_1 = 2, m_2 = 3, m_3 = 5)$: Par l'équation (9), on a que $n = 60$.

Ainsi $|P_1| = \frac{60}{2} = 30, |P_2| = \frac{60}{3} = 20$ et $|P_3| = \frac{60}{5} = 12$ par l'équation (7).

Nous allons chercher à montrer que $G \simeq \text{Alt}_5 \simeq D$, où D est le groupe de rotations préservant le dodécaèdre. Voir la proposition 3.25 et les figures 10 et 11.

Puisque Alt_5 est un groupe de 60 éléments, avec 20 éléments d'ordre 3, 24 éléments d'ordre 5, 15 éléments d'ordre 2 et l'identité, alors $D \simeq \text{Alt}_5$.

La preuve que $G \simeq \text{Alt}_5$ peut se faire de deux approches différentes. La première, plus géométrique, permet de faire la preuve en considérant les 5 cubes inscrits dans le dodécaèdre. La seconde, plus algébrique, permet de faire la preuve en utilisant le théorème ?? [Théorème de Sylow].

Première approche : Considérons P_2 . Puisque $m_1 = 2, m_2 = 3, m_3 = 5$, alors si $\text{stab}(p) = 3$ pour $p \in P_2$, alors il faut que $p, -p \in P_2$. Ainsi

$$P_2 = \{\pm p_1, \pm p_2, \pm p_3, \pm p_4, \pm p_5, \pm p_6, \pm p_7, \pm p_8, \pm p_9, \pm p_{10}\}.$$

Considérons la bijection $\gamma : P_2 \rightarrow DD$, où DD est l'ensemble des sommets du dodécaèdre. Considérons $(C_i)_{i \in \{1,2,3,4,5\}}$, la famille des cinq cubes inscrits dans DD .

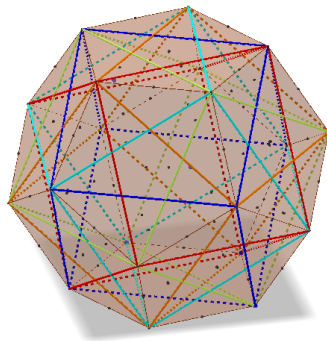
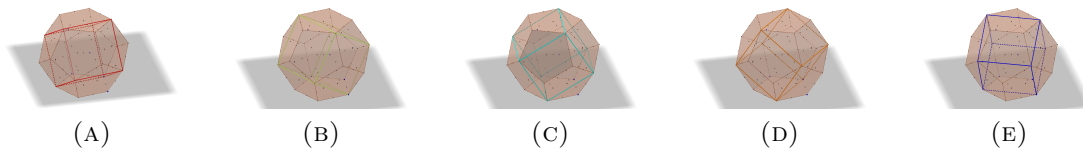


FIGURE 13. Les cinq cubes inscrits dans le dodécaèdre

FIGURE 14. Décomposition de la figure 13 en cinq figures où les différents cubes apparaissent.



Pour tout $p_l \in P_2$, $\gamma(p_l) \in C_i, \gamma(p_l) \in C_j$ pour i, j distincts, ainsi $\gamma(-p_l) \in C_i, \gamma(-p_l) \in C_j$. Puisque G agit sur les couples d'éléments, on a donc que G agit sur l'ensemble des cubes par le morphisme suivant : $\phi : G \rightarrow S_5$.

Si on considère la rotation ayant comme axe de rotation deux faces opposées du dodécaèdre, d'angle $\frac{2\pi}{5}$, on a que $\text{Im}(\phi) = \phi(G)$ contient tous les cycles d'ordre 5. En particulier, $\text{Alt}_5 \in \phi(G)$, puisque Alt_5 est engendrée par les cycles d'ordre 5, ce qu'il est facile de vérifier. On a donc que $|G| = 60 = |\text{Alt}_5| \leq |\phi(G)|$.

Il suffit donc de montrer que ϕ est injectif pour pouvoir conclure que $G \simeq \text{Alt}_5$.

Considérons $g \in \ker(\phi) \setminus \{e\}$. Alors g fixe chacun des cubes. Il faut donc que g soit une rotation d'angle π , $\frac{2\pi}{3}$ ou $\frac{4\pi}{3}$, qui préservent un cube.

Si g est une rotation d'angle π , alors son axe de rotation passe par le milieu d'une arête du dodécaèdre, et donc g ne peut pas laisser invariant chacun des cubes.

Si g est d'ordre 3 (c'est-à-dire que g est une rotation d'angle $\frac{2\pi}{3}$ ou $\frac{4\pi}{3}$), alors l'axe de rotation de g est une diagonale du dodécaèdre, et g ne peut pas stabiliser chacun des cubes.

On a donc que $\ker(\phi) = \{e\}$, et ϕ est injectif. Ainsi $G \simeq \text{Alt}_5$.

Seconde approche : Considérons P_3 . Puisque $m_1 = 2, m_2 = 3, m_3 = 5$, alors si $\text{stab}(p) = 5$ pour $p \in P$, alors il faut que $p, -p \in P_3$. Ainsi

$$P_3 = \{\pm p_1, \pm p_2, \pm p_3, \pm p_4, \pm p_5, \pm p_6\}.$$

Si $g \in G \setminus \{e\}$ n'admet pas un couple de pôles dans P_2 , alors g agit comme une permutation sur les couples, puisque les paires de pôles demeurent des paires de pôles sous l'action de G . Si $g \in G$ admet un couple de pôles $\pm p_i \in P_3, 1 \leq i \leq 6$, alors g agit comme une permutation sur les couples $(p_l, -p_l)$, pour $l \in \{1, 2, 3, 4, 5, 6\} \setminus \{i\}$.

On a donc un morphisme :

$$\begin{aligned} s : G &\rightarrow \text{Sym}_6 \\ g &\mapsto s_g. \end{aligned}$$

Par un raisonnement semblable à celui employé au cas précédent, on doit avoir que $\ker(s) = \{e\}$, et s est injectif.

On a donc que $G \subseteq \text{Sym}_6 \geq \text{Sym}_5 \supset \text{Alt}_5, |\text{Sym}_5| = 120$ et $|\text{Alt}_5| = 60$.

Définition 3.33. Un groupe F est simple si ses seuls sous-groupes normaux sont $\{e\}$ et F .

1) Montrons que $\text{Alt}_5 \triangleleft S_5$ est simple.

Considérons $H \triangleleft \text{Alt}_5$, un sous-groupe normal non trivial de Alt_5 . Soit $x \in H \setminus \{e\}$, x doit être de la forme :

- $x = (abc) = (bc)(ac)$, pour $a, b, c \in \{1, 2, 3, 4, 5\}$ distincts.
- $x = (ab)(cd)$, pour $a, b, c, d \in \{1, 2, 3, 4, 5\}$ distincts.
- $x = (aebdc) = (ab)(cd)(ae)(bc)$, pour $a, b, c, d, e \in \{1, 2, 3, 4, 5\}$ distincts.

Si x est un 2-cycles, alors H doit contenir ses conjugués. De plus, le produit de deux 2-cycles disjoints de Sym_5 est un 3-cycle. On a donc que H contient un 3-cycle.

Si x est un 5-cycle, alors H doit contenir ses conjugués. De plus, le produit de deux 5-cycles de Sym_5 est un 3-cycle. On a donc que H contient un 3-cycle.

On a ainsi que H doit contenir un 3-cycle, ainsi que ses conjugués, et contient donc l'ensemble des 3-cycles. Or, pour tout $n \in \mathbb{N}$, Alt_n est généré par les 3-cycles, c'est-à-dire que $\forall x \in \text{Alt}_n, x = \theta_1 \cdot \theta_2 \cdots \theta_k$, pour θ_i des 3-cycles.

Ainsi $H = \text{Alt}_5$ et Alt_5 est simple.

2) Montrons que Alt_5 est le seul groupe simple d'ordre 60 (à isomorphisme près).

Supposons qu'il existe un groupe simple H tel que $|H| = 60$ et $H \not\cong \text{Alt}_5$. Par le théorème de Sylow en théorème 3.11, H admet au moins un 2-sous-groupe de Sylow, c'est-à-dire un sous-groupe de cardinalité $2^2 = 4$, au moins un 3-sous-groupe de Sylow et au moins un 5-sous-groupe de Sylow.

Par le théorème 3.14, le nombre de 2-sous-groupes de Sylow est inclus dans $\{1, 3, 5, 15\}$, le nombre de 3-groupes de Sylow dans $\{1, 4, 10\}$ et le nombre de 5-groupes de Sylow, dans $\{1, 6\}$.

Lemme 3.34. *Soit F un groupe simple d'ordre tel que $|H| > 2$, alors si p est un nombre premier divisant n , alors le nombre n_p de p -sous-groupe de Sylow de F vérifie $n \leq \frac{n_p!}{2}$, avec égalité ssi $F \simeq \text{Alt}_{n_p}$.*

Démonstration. F agit sur l'ensemble de ses p -sous-groupes de Sylow par conjugaison, et cette action est transitive. Puisque F est simple, on a une injection $i : F \rightarrow S_{n_p}$. Si on considère $\gamma = \epsilon \circ i : F \rightarrow \{-1, 1\}$, ou ϵ est l'application qui envoie les éléments de S_{n_p} sur leur signe, on a que le noyau de γ est un sous-groupe normal de F , qui est soit $\{e\}$, soit F vu que F est simple. Si $\ker(\gamma) = \{e\}$, alors γ est injectif, ce qui est une contradiction, puisque $|F| > 2$ et $|\{-1, 1\}| = 2$, et $\gamma : F \rightarrow \{-1, 1\}$. Il faut donc que $\ker(\gamma) = F$ et $i : F \rightarrow \text{Alt}_{n_p}$. ■

Il faut donc que le $n_2 = 5$, $n_3 = 10$ et $n_5 = 6$.

Puisque que les 5-sous-groupes sont cycliques, alors l'intersection entre deux sous-groupes de Sylow est triviale. H contient donc 24 éléments d'ordre 5.

Puisque les 3-sous-groupes de Sylow sont engendrés par leurs éléments non-triviaux, ainsi l'intersection de deux 3-sous-groupes de Sylow distincts est triviale. H contient donc 20 éléments d'ordre 3.

Puisque le groupe H agit transitivement par conjugaison sur les cinq 2-groupes de Sylow, par le théorème 3.13, on a un morphisme de H dans Sym_5 qui est injectif (H est simple). On a donc que H est isomorphe à un groupe normal d'ordre 60 de Sym_5 , et ainsi $H \simeq \text{Alt}_5$.

3) Montrons que G est simple.

Soit H un sous-groupe normal non-trivial de G . Considérons $x \in H \setminus \{e\}$. Il faut que x soit d'ordre 2, 3 ou 5, et tous les conjugués de x sont dans H . Si x est d'ordre 2, on a que H contient au moins 16 éléments. Si x est d'ordre 3, alors H contient au moins 21 éléments, et si x est d'ordre 5, alors H contient au moins 25 éléments. De plus, il faut que $|H|$ divise $|G|$, on doit donc avoir que H contient au moins 20 éléments, ce qui signifie que H comporte au moins deux éléments d'ordre différents, et donc contient plus que 30 éléments. Il faut donc que $H = G$, et G est simple.

Puisqu'il n'existe qu'un seul groupe simple d'ordre 60 (à isomorphisme près), alors $G \simeq A_5$.

■

4. NOTE

Au cours de ce stage, nous avons beaucoup travaillé sur un volet parallèle et très intéressant qui, par manque de temps et d'espace, n'a pas trouvé sa place ici.

Nous avons exploité la théorie de la représentation ainsi que notre compréhension des groupes étudiés dans la première partie du stage pour trouver une représentation irréductible et fidèle générant des groupes de matrices isomorphes aux groupes C_n , le groupe cyclique d'ordre n , D_n , le groupe diédral d'ordre $2n$, et Sym_n , le groupe symétrique d'ordre $n!$. À l'aide de ces matrices, nous avons étudié, pour chacun des groupes mentionnés suite à leur identification à G , le polynôme $Q = \frac{1}{|G|} \sum_{g \in G} q^{\text{rang}(M_g - \mathbb{1}_G)}$.

Pour tout groupe, les monômes de Q de degré k ont comme coefficient le nombre d'élément de ce groupe qui ont la caractéristique $\text{rang}(M_g - \mathbb{1}_G) = k$. Dans le cas de Sym_n en particulier, nous avons montré que le degré k indique le nombre de transpositions composant l'élément g de S_n . Nous avons tout particulièrement cherché à prouver que ces polynômes ont des factorisations intéressantes pour chacun des groupes.

Ce sujet fera l'objet d'un second rapport réalisé sur une base volontaire qui pourra être remis à l'ISM sur demande, et sera présenté au cours de l'année lors d'une des conférences mathématiques étudiantes réalisées au baccalauréat à l'attention des étudiants au Baccalauréat en mathématiques et à la Maîtrise en mathématiques.

5. CONCLUSION

L'étude des sous-groupes finis des réflexions qui forment les symétries du plan et de l'espace, ont permis d'approfondir ma compréhension et mes connaissances en théorie des groupes. Bien que la plupart des résultats obtenus sont connus, les démonstrations réalisées sont détaillées et sont parfois abordés sous des angles nouveaux et plus géométriques.

Les polynômes étudiés au cours de la deuxième moitié du stage permettent d'aborder les groupes sous un regard nouveau à l'aide de la théorie de la représentation et ont potentiellement des applications dans d'autres domaines mathématiques. Il serait intéressant de poursuivre les recherches avec d'autres groupes, et de chercher des applications potentielles de ces résultats.

Remerciements. Je souhaiterais remercier le Laboratoire de combinatoire et d'informatique mathématique (LACIM), l'Institut des sciences mathématiques (ISM), ainsi que mes deux directeurs de stage pour l'été 2016, Nathan Williams (post-doctorat à l'UQAM) et Christophe Hohlweg (professeur à l'UQAM) pour leur soutien et leur grande disponibilité.

RÉFÉRENCES

- [1] Calais, Josette. 1984. *Éléments de théorie des groupes*. Éd. Presses universitaires de France, Paris. 368 p.
- [2] Combes, François. 1998. *Algèbre et géométrie*. Éd. Bréal, Levallois-Perret. 320 p. p.171 .
- [3] Grove, L.C. and Benson, C.T. 1985. *Finite Reflexion Groups* 2e éd. Éd. Springer-Verlag, New York. 133 p. Ch. 1-2
- [4] *Solides de platon*. In Wikipédia. [En ligne]. https://fr.wikipedia.org/wiki/Solide_de_Platon. Page consultée le 11 août 2016.
- [5] *Théorèmes de Sylow*. In Wikipédia. [En ligne]. https://fr.wikipedia.org/wiki/T%C3%A9or%C3%A8mes_de_Sylow . Page consultée le 24 août 2016.
- [6] *Sous-groupes finis de $SO(3)$* . [En ligne]. http://www.normalesup.org/~kortchem/mathclub/Sous_groupes_finis_S03.pdf. Page consultée le 24 août 2016.
- [7] *Sous-groupes finis de $SO(3)$: Cours d'Algèbre linéaire I*. [En ligne]. <http://pedestre.info/Math/le%E7on%20CAPES-Agreg/S03.pdf> Page consultée le 24 août 2016.
- [8] *A_5 est le seul groupe simple d'ordre 60*. [En ligne]. http://dyna.maths.free.fr/docs/lecons/developpement_algebre_3.pdf Page consultée le 24 août 2016.
- [9] Gelineau, Yoann. *Simplicité de A_n pour $n \geq 5$* . In Institut Camille-Jordan de l'Université de Lyon. [En ligne]. http://math.univ-lyon1.fr/~gelineau/devagreg/Simplicitete_groupe_alterne.pdf Page consultée le 24 août 2016.

UNIVERSITÉ DU QUÉBEC À MONTRÉAL