

# Autour des sous-groupes finis de $O(2)$ et $O(3)$

Vincent Pilaud

2006

## 1 Introduction

Soit  $n \in \{2, 3\}$ . On note

$$O(n) = \{M \in M_n(\mathbb{R}) \mid M^t M = \text{Id}\} \quad \text{le groupe orthogonal}$$

$$\text{et } SO(n) = \{M \in O(n) \mid \det M = 1\} \quad \text{le groupe spécial orthogonal.}$$

On suppose connue la classification des matrices de  $O(n)$  et  $SO(n)$  (pour  $n \in \{2, 3\}$ ) :

**Théorème 1.** (i) *Toute matrice de  $SO(2)$  est une rotation d'angle  $\theta \in [0, 2\pi[$ , et s'écrit sous la forme*

$$R_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}.$$

*Le groupe  $SO(2)$  est commutatif et l'application  $\mathbb{R}/2\pi\mathbb{Z} \rightarrow SO(2)$   
 $\theta \mapsto R_\theta$  est un morphisme de groupes.*

*Toute matrice de  $O(2) \setminus SO(2)$  est une symétrie et s'écrit sous la forme*

$$R_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}, \quad \text{avec } \theta \in [0, 2\pi[.$$

(ii) *Toute matrice de  $O(3)$  est semblable à une matrice de la forme*

$$\begin{pmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad \text{avec } \theta \in [0, 2\pi[ \text{ et } \varepsilon \in \{1, -1\}.$$

*Si  $\varepsilon = 1$ , c'est la matrice d'une rotation de  $SO(3)$ . Si  $\varepsilon = -1$ , c'est la matrice d'un retournement de  $O(3) \setminus SO(3)$ .*

Dans ce texte, on s'intéresse aux sous-groupes finis de  $O(2)$  et  $O(3)$ . On traite rapidement (§ 2) le cas de la dimension 2 qui est relativement simple, puis on présente (§ 3) le cas de la dimension 3. Ceci fait en particulier appel à l'étude des polyèdres réguliers de l'espace (§ 3.2) et à leurs groupes d'isométries (§ 3.3). Cette étude s'applique à divers problèmes : citons la classification des sous-groupes finis de  $GL_n(\mathbb{R})$  et de  $GA_n(\mathbb{R})$  (où  $n \in \{2, 3\}$ ), les groupes cristallographiques du plan et de l'espace et les coloriages de polygones et de polyèdres, que l'on présente dans la dernière partie (§ 4).

## 2 Sous-groupes finis de $O(2)$ et polygones réguliers

### 2.1 Groupe diedral

Soit  $m \geq 3$ . Pour  $0 \leq i \leq m-1$ , on note  $P_i = e^{2i\pi/m}$ . On appelle polygone régulier à  $m$  cotés l'enveloppe convexe des  $(P_i)_{1 \leq i \leq m-1}$ .

**Définition 1** (Groupe diedral). *On appelle groupe diedral, et on note  $\mathbb{D}_{2m}$  le groupe des isométries du plan conservant le polygone régulier à  $m$  côtés.*

**Proposition 1.** *Le groupe  $\mathbb{D}_{2m}$  est de cardinal  $2m$ .*

*Le sous-groupe  $\mathbb{D}_{2m} \cap SO(2)$  est cyclique engendré par la rotation  $\rho_m$  d'angle  $\frac{2\pi}{m}$ .*

*L'ensemble  $\mathbb{D}_{2m} \cap (O(2) \setminus SO(2))$  est constitué de  $m$  symétries*

- (i) d'axe passant par un sommet et le milieu du côté opposé lorsque  $m$  est impair,
  - (ii) d'axe passant par deux sommets opposés ou les milieux de deux côtés opposés lorsque  $m$  est pair.
- Si  $\sigma \in \mathbb{D}_{2m} \cap (O(2) \setminus SO(2))$ , alors

$$\mathbb{D}_{2m} = \langle \rho_m \rangle \rtimes \langle \sigma \rangle \simeq \mathbb{Z}/m\mathbb{Z} \rtimes_{\Phi} \mathbb{Z}/2\mathbb{Z},$$

où  $\Phi(1) : x \mapsto -x$ .

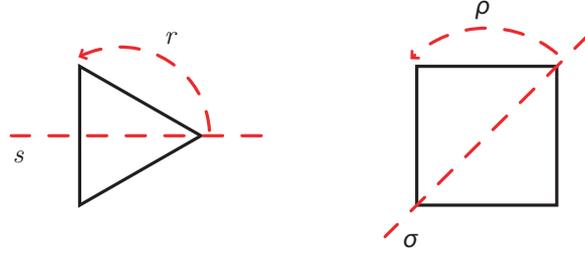


FIG. 1 –  $\mathbb{D}_6 = \{\text{Id}, \rho_3, \rho_3^2, s, s\rho_3, s\rho_3^2\}$  et  $\mathbb{D}_8 = \{\text{Id}, \rho_4, \rho_4^2, \rho_4^3, \sigma, \sigma\rho_4, \sigma\rho_4^2, \sigma\rho_4^3\}$

Pour montrer que  $\mathbb{D}_{2m}$  contient  $2m$  éléments, considérons d'abord l'ensemble  $X$  des couples  $(s, a)$ , où  $s$  est un sommet et  $a$  une arête du polygone régulier à  $m$  côtés, avec  $s \in a$ . Notons qu'une isométrie du polygone régulier à  $m$  côtés est entièrement déterminée par l'image du couple  $(P_0, [P_0, P_1])$ . Par conséquent, l'ensemble  $X$  ayant  $2m$  éléments, le groupe  $G$  admet au plus  $2m$  éléments. Or il se trouve qu'il contient clairement  $m$  rotations (d'angle  $2i\pi/m$ , avec  $0 \leq i \leq m-1$ ) et  $m$  symétries (décrites dans la proposition). La cyclicité de  $\mathbb{D}_{2m} \cap SO(2)$  découle de la structure des sous-groupes discrets de  $\mathbb{R}$  et du morphisme  $\begin{matrix} \mathbb{R}/2\pi\mathbb{Z} & \rightarrow & SO(2) \\ \theta & \mapsto & R_\theta \end{matrix}$ . Enfin pour montrer qu'il s'agit d'un produit semi-direct, on vérifie que  $\langle \rho_m \rangle$  est distingué dans  $2m$ , que  $\langle \rho_m \rangle \cap \langle \sigma \rangle = \{\text{Id}\}$  et que  $\langle \rho_m \rangle \langle \sigma \rangle = \mathbb{D}_{2m}$ .

On définit aussi  $\mathbb{D}_2 = \mathbb{Z}/2\mathbb{Z}$  et  $\mathbb{D}_2 = (\mathbb{Z}/2\mathbb{Z})^2$ .

## 2.2 Sous-groupes finis de $O(2)$

On peut maintenant énoncer le théorème de classification des sous-groupes finis de  $O(2)$  :

**Théorème 2.** Soit  $G$  un sous-groupe fini de  $O(2)$ . Alors

- (i) si  $G \subset SO(2)$ , il est cyclique,
- (ii) sinon, il est diédral.

En effet, le (i) vient de la structure des sous-groupes discrets de  $\mathbb{R}$  et du morphisme  $\begin{matrix} \mathbb{R}/2\pi\mathbb{Z} & \rightarrow & SO(2) \\ \theta & \mapsto & R_\theta \end{matrix}$ . Pour le (ii), si  $G \not\subset SO(2)$ , alors pour tout  $\sigma \in G \setminus SO(2)$ , on a  $G = (G \cap SO(2)) \rtimes \langle \sigma \rangle$ , ce qui montre qu'il est diédral.

## 3 Sous-groupes finis de $O(3)$ et polyèdres réguliers

### 3.1 Polyèdres réguliers

Commençons par définir proprement les polyèdres réguliers d'un espace euclidien  $\mathbb{R}^n$  (où  $n \in \mathbb{N}$ ) :

**Définition 2** (Polyèdres). On appelle polytope de  $\mathbb{R}^n$  toute intersection finie de demi-espaces. On appelle dimension d'un polytope  $P$ , et on note  $\dim P$ , la dimension de son enveloppe affine. Lorsqu'un polytope est borné, on parle de polyèdre.

**Définition 3** (Faces). On dit qu'un hyperplan  $H$  de  $\mathbb{R}^n$  est valide pour un polytope  $P$  si le polytope est entièrement contenu dans l'un des demi-espaces (fermés) limités par  $H$ . On appelle face de  $P$  toute intersection non vide de  $P$  par un demi-espace valide pour  $P$ .

Notons qu'une face d'un polytope est elle-même un polytope de dimension inférieure. Pour un polytope  $P$ , on considère maintenant l'ensemble  $T(P) = \{f \text{ face de } P\} \cup \{\emptyset, P\}$ . L'ensemble  $T(P)$  est un treillis (ie. un ensemble ordonné dont toute paire d'éléments admet une borne supérieure et une borne inférieure). Dans ce treillis, on s'intéresse particulièrement aux *drappeaux* :

**Définition 4** (Drapeaux). On appelle drapeau dans le polytope  $P$  toute suite complète de faces  $\emptyset = f_0 \subset f_1 \subset f_2 \subset \dots \subset f_{\dim P}$  de  $P$ .

Le groupe  $G_P$  des isométries d'un polytope  $P$  agit naturellement sur l'ensemble  $\mathcal{D}$  des drapeaux de  $P$  via :

$$\begin{aligned} G_P \times \mathcal{D} &\longrightarrow \mathcal{D} \\ (\varphi, (f_0, \dots, f_{\dim P})) &\longmapsto (\varphi(f_0), \dots, \varphi(f_{\dim P})) \end{aligned}$$

**Définition 5** (Polyèdre régulier). On dit qu'un polyèdre  $P$  est régulier si l'action de  $G_P$  sur ses drapeaux est transitive.

### 3.2 Les 5 solides platoniciens

On s'intéresse maintenant aux polyèdres réguliers de  $\mathbb{R}^3$ , et plus précisément aux classes de similitude de ces polyèdres (déplacer ou faire grossir un cube ne fournit pas une nouvelle classe de polyèdres). Nous avons la description suivante, déjà connue par Platon :

**Théorème 3** (Solides Platoniciens). Il existe exactement 5 classes de polyèdres réguliers :

	tétraèdre	cube	octaèdre	dodécaèdre	icosaèdre
sommets	4	8	6	20	12
arêtes	6	12	12	30	30
faces	4	6	8	12	20

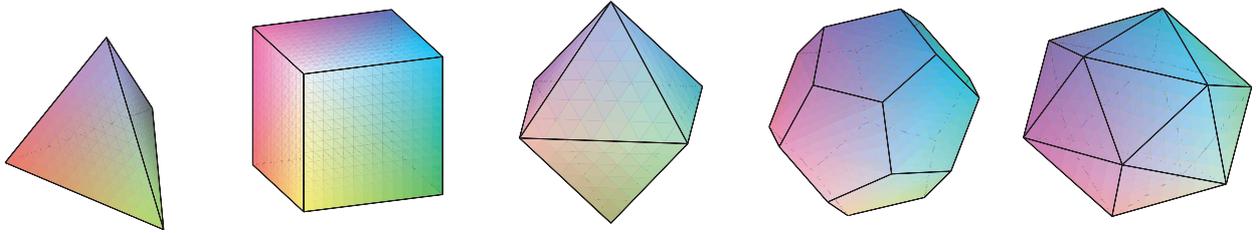


FIG. 2 – Les 5 solides de Platon

En effet, considérons un polyèdre régulier  $P$  de  $\mathbb{R}^3$  dont on note  $s$  (resp.  $a$ , resp.  $f$ ) le nombre de sommets (resp. arêtes, resp. faces). Les faces de dimension 2 de ce polyèdre sont des polygones réguliers identiques. Notons  $p$  le nombre de sommets de ces polygones. Par ailleurs, on note  $q$  le nombre de faces qui contiennent un sommet donné (ce nombre ne dépend pas du sommet considéré). Notons que l'on sait déjà que  $p \geq 3$  et  $q \geq 3$ .

En considérant la somme des angles autour d'un sommet du polyèdre, on a  $2\pi > q(\pi - 2\pi/p)$ , ce qui donne

$$p < \frac{2q}{q-2}$$

L'étude de la fonction  $x \mapsto \frac{2x}{x-2}$  permet d'affirmer que le couple  $(p, q)$  est forcément dans l'ensemble

$$\{(5, 3), (4, 3), (3, 3), (3, 4), (3, 5)\}.$$

Par ailleurs, les relations d'incidence sommets/arêtes et arêtes/faces donnent :

$$2a = \sum_{a \in A} \text{card}\{s \in S \mid s \in a\} = \text{card}\{(s, a) \in S \times A \mid s \in a\} = \sum_{s \in S} \text{card}\{a \in A \mid s \in a\} = qs,$$

$$2a = \sum_{a \in A} \text{card}\{f \in F \mid a \in f\} = \text{card}\{(a, f) \in F \times F \mid a \in f\} = \sum_{f \in F} \text{card}\{a \in A \mid a \in f\} = pf.$$

La relation d'Euler  $s - a + f = 2$  fournit donc

$$s = \frac{4p}{2p + 2q - pq}, \quad a = \frac{2pq}{2p + 2q - pq}, \quad \text{et} \quad f = \frac{4q}{2p + 2q - pq}.$$

On vérifie aisément que les trois nombres  $s, a$  et  $f$  définissent la classe de similitude d'un polyèdre, et que les 5 classes que l'on vient d'exhiber sont effectivement réalisées. Ceci termine la preuve du théorème.

### 3.3 Groupes d'isométries

Nous allons décrire ici les groupes d'isométries des polyèdres réguliers de l'espace. Commençons par remarquer deux petites choses :

- (i) le groupe d'isométries d'un polyèdre régulier à  $n$  sommets conserve l'ensemble de ses sommets (car ce sont les points extrémaux), donc s'injecte dans le groupe symétrique  $\mathfrak{S}_n$ . On peut faire la même remarque avec les faces ou les arêtes.
- (ii) on appelle *polyèdre dual* d'un polyèdre  $P$  le polyèdre dont les sommets sont les centres de gravité des faces de codimension 1 de  $P$ . Le treillis des faces du dual d'un polyèdre  $P$  est le treillis dual du treillis du polyèdre  $P$ . Cette dualité est une involution sur les classes de similitude de polyèdres. Par ailleurs, il est clair que deux polyèdres duaux ont le même groupe d'isométries. Or il se trouve que
  - le tétraèdre est autodual,
  - le cube et l'octaèdre sont duaux,
  - le dodécaèdre et l'icosaèdre sont duaux.

#### 3.3.1 Tétraèdre

**Proposition 2.** *Le groupe des isométries positives (resp. isométries) du tétraèdre est isomorphe à  $\mathfrak{A}_4$  (resp.  $\mathfrak{S}_4$ ).*

La remarque (i) assure que le groupe des isométries du tétraèdre s'injecte dans  $\mathfrak{S}_4$ . Pour montrer que l'on obtient tout le groupe symétrique, il suffit d'exhiber une famille génératrice de  $\mathfrak{S}_4$ , par exemple les transpositions. Or une transposition qui inverse deux sommets 1 et 2 et laisse stable les deux autres sommets 3 et 4 s'obtient simplement par la symétrie orthogonale par rapport au plan contenant 3, 4 et le milieu de 1 et 2 (fig. 3). Par ailleurs, il est clair qu'une transformation est directe si et seulement si la permutation associée est positive. D'où la proposition.

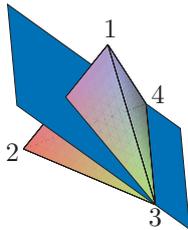


FIG. 3 – Transposition dans un tétraèdre

#### 3.3.2 Cube et octaèdre

**Proposition 3.** *Le groupe des isométries positives (resp. isométries) du cube (et de l'octaèdre) est isomorphe à  $\mathfrak{S}_4$  (resp.  $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ ).*

Remarquons d'abord que le diamètre du cube est réalisé par les quatre paires de sommets opposées (grandes diagonales du cube). Les isométries du cube conservant le diamètre, les grandes diagonales sont envoyées sur des grandes diagonales. Il est par ailleurs aisé de vérifier qu'une isométrie du cube qui stabilise les quatre diagonales appartient à  $\{\text{Id}, -\text{Id}\}$ . On en déduit que le groupe des isométries directes du cube se plonge dans le groupe symétrique  $\mathfrak{S}_4$ . Comme dans le cas du tétraèdre, on vérifie que ce plongement est surjectif en exhibant l'isométrie correspondant à une transposition de deux grandes diagonales : pour transposer deux diagonales [17] et [35], il suffit de faire une rotation d'angle  $\pi/2$  autour de la droite reliant les milieux de 1 et 5 et de 3 et 7 (fig. 4).

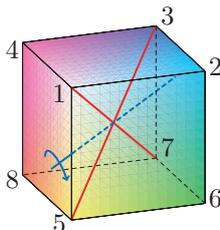


FIG. 4 – Transposition dans un cube

### 3.3.3 Icosaèdre et dodécaèdre

On a besoin ici de quelques résultats sur le groupe alterné  $\mathfrak{A}_5$  et sur les groupes simples. On va utiliser de manière récurrente le classique résultat de Sylow, que l'on suppose connu :

**Théorème 4** (Sylow). *Soient  $p$  un entier premier,  $m$  un entier premier avec  $p$  et  $\alpha$  un entier. Soit  $G$  un groupe d'ordre  $p^\alpha m$ . Alors  $G$  admet au moins un  $p$ -sous-groupe de Sylow (ie. un sous-groupe de cardinal  $p^\alpha$ ). De plus,*

- (i) *tout  $p$ -sous-groupe de  $G$  est contenu dans un  $p$ -sous-groupe de Sylow de  $G$ ,*
- (ii) *les  $p$ -sous-groupes de Sylow de  $G$  sont tous conjugués,*
- (iii) *le nombre  $n_p$  de  $p$ -sous-groupes de Sylow de  $G$  vérifie  $n_p | m$  et  $n_p \equiv 1 [p]$ .*

Commençons par établir le lemme suivant.

**Lemme 1.** *Soit  $H$  un groupe simple d'ordre  $n > 2$ . Alors*

- (i) *si  $p$  est un nombre premier divisant strictement  $n$ , le nombre  $n_p$  de  $p$ -sous-groupes de Sylow de  $H$  vérifie  $n \leq n_p!/2$  avec égalité si et seulement si  $H \simeq \mathfrak{A}_{n_p}$ .*
- (ii) *si  $K$  est un sous-groupe de  $H$  d'indice  $\ell > 1$ , alors  $n \leq \ell!/2$  avec égalité si et seulement si  $H \simeq \mathfrak{A}_\ell$ .*

Dans le cadre du (i), le groupe  $H$  agit sur l'ensemble de ses  $p$ -sous-groupes de Sylow par conjugaison, et cette action est transitive, donc non triviale. Par simplicité de  $H$ , on a donc une injection  $i : H \hookrightarrow \mathfrak{S}_n$ . Considérons l'application  $\varphi = \varepsilon \circ i : H \rightarrow \{1, -1\}$  (où  $\varepsilon : \mathfrak{S}_n \rightarrow \{1, -1\}$  désigne la signature). Le noyau de  $\varphi$  est un sous-groupe distingué de  $H$ , qui est simple. C'est donc soit  $\{1\}$  soit  $H$ . Dans le premier cas,  $\varphi$  serait une injection de  $H$  dans un groupe à 2 éléments, ce qui est impossible par hypothèse. Par conséquent, l'injection  $i$  est à image dans  $\mathfrak{A}_n$ . On en déduit immédiatement le résultat (i).

Dans le cadre du (ii), le groupe  $H$  agit sur l'ensemble des classes à droite  $H/K$  par translation à droite, et cette action est transitive. Les mêmes arguments que précédemment permettent donc d'aboutir au résultat (ii).

**Proposition 4.** (i)  $\mathfrak{A}_5$  est simple.

- (ii)  $\mathfrak{A}_5$  est le seul (à isomorphisme près) groupe simple d'ordre 60.
- (iii) Tout groupe ayant exactement 1 (resp. 15, resp. 20, resp. 24) élément(s) d'ordre 1 (resp. 2, resp. 3, resp. 5) est isomorphe à  $\mathfrak{A}_n$ .

On commence par montrer le deuxième point par l'absurde. Soit  $G$  un groupe simple d'ordre 60 non isomorphe à  $\mathfrak{A}_5$ . Le théorème de Sylow affirme que

- le nombre  $n_2$  de 2-sous-groupes de Sylow de  $G$  appartient à l'ensemble  $\{1, 3, 5, 15\}$ ,
- le nombre  $n_5$  de 5-sous-groupes de Sylow de  $G$  appartient à  $\{1, 6\}$ .

Le lemme précédent assure donc que  $n_2 = 15$  et  $n_5 = 6$ .

Les 5-sous-groupes de Sylow de  $G$  étant des sous-groupes cycliques, l'intersection de deux d'entre eux est réduite à  $\{\text{Id}\}$ . Par conséquent, le groupe  $G$  contient 24 éléments d'ordre 5.

Montrons que l'intersection de deux 2-sous-groupes de Sylow est aussi réduite à  $\{\text{Id}\}$ . Soit  $x$  un élément différent de  $\text{Id}$  d'un 2-sous-groupe de Sylow  $H$ , et  $N$  son stabilisateur. Le groupe  $H$  est d'ordre 4, donc c'est un groupe cyclique. Par conséquent,  $H \subset N$  et  $N$  est d'indice dans  $\{1, 3, 5, 15\}$ . Si cet indice est 1,  $x$  commute avec tous les éléments de  $G$ , donc le sous-groupe  $\langle x \rangle$  engendré par  $x$  est central, donc distingué. Ceci est impossible par simplicité de  $G$ . Ainsi, et grâce au résultat du lemme 1, l'indice de  $N$  est 15, donc  $N = H$  et les 2-sous-groupes de Sylow sont effectivement d'intersection réduite à  $\{\text{Id}\}$ . Le groupe  $G$  contient donc 45 éléments d'ordre 2 ou 4.

Il ne reste plus qu'à remarquer que  $1 + 24 + 45 = 70 > 60$ , donc notre hypothèse de départ est absurde.

Montrons à présent le troisième point. Pour ceci, considérons un groupe  $G$  contenant exactement 1 (resp. 15, resp. 20, resp. 24) élément(s) d'ordre 1 (resp. 2, resp. 3, resp. 5) et montrons qu'il est simple (ce qui au passage prouvera le (i)). Le deuxième point suffira alors à conclure.

Soit  $H$  un sous-groupe distingué strict de  $G$  (ie. différent de  $G$ ). Supposons d'abord que  $H$  contienne un élément d'ordre 3. Alors il contient tout le 3-Sylow qui contient cet élément, donc (par le théorème de Sylow, et par simplicité) tous les 3-sous-groupes de Sylow, et donc tous les éléments d'ordre 3. Ainsi,  $H$  contient au moins  $1 + 20 = 21$  éléments. Le théorème de Lagrange affirme alors que le cardinal de  $H$  est 30. Donc  $H$  contient un 5-sous-groupe de Sylow, donc tous les 5-sous-groupes de Sylow, et donc tous les éléments d'ordre 5. Ainsi,  $H$  contient au moins  $1 + 20 + 24 = 45$  éléments, donc  $H = G$ , ce qui est contraire à notre hypothèse. On en déduit que  $H$  ne contient aucun élément d'ordre 3. Un raisonnement identique montre que  $H$  ne contient aucun élément d'ordre 5.

Supposons maintenant que  $H$  contient un élément d'ordre 2. Alors si  $\text{card}(H) \geq 4$ ,  $H$  contient un 4-sous-groupe de Sylow de  $G$ , donc tous les 4-sous-groupes de Sylow de  $G$ , donc tous les éléments d'ordre 2. Le cardinal de  $H$  est donc

supérieur à  $1 + 15 = 16$ , donc (par le théorème de Lagrange) vaut soit 20, soit 30. Ces deux nombres étant divisible par 5,  $H$  doit alors contenir un 5-Sylow, donc un élément d'ordre 5, ce qui est exclu. Par conséquent, on peut supposer que  $\text{card}(H) = 2$ . Mais l'élément non trivial  $x$  de  $H$  commute alors avec tous les éléments de  $G$ . On obtiendrait alors un élément d'ordre 6, ce qui est exclu.

On en déduit que  $H$  est réduit à  $\{\text{Id}\}$ , et donc que  $G$  est simple, ce qui termine la preuve.

On peut maintenant facilement trouver le groupe des isométries du dodécaèdre :

**Proposition 5.** *Le groupe des isométries positives (resp. isométries) du dodécaèdre (et de l'icosaèdre) est isomorphe à  $\mathfrak{A}_5$  (resp.  $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ ).*

Le groupe  $G$  des isométries positives d'un dodécaèdre contient (fig. 5) :

- (i) l'identité,
- (ii) 15 rotations d'angle  $\pi$  autour des droites passant par les milieux de deux arêtes opposées,
- (iii) 20 rotations d'angle  $\pi/3$  et  $2\pi/3$  autour des droites passant par deux sommets opposés,
- (iv) 24 rotations d'angle  $\pi/5$ ,  $2\pi/5$ ,  $3\pi/5$  et  $4\pi/5$  autour des droites passant par les centres de deux faces opposées.

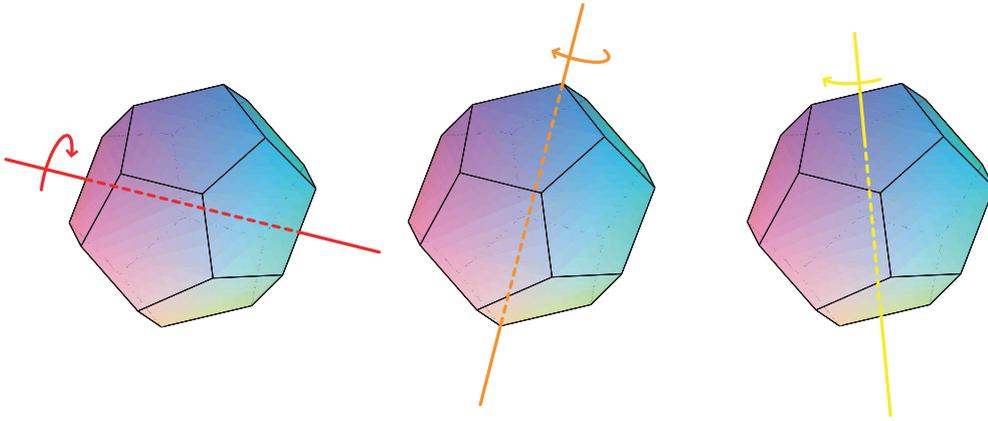


FIG. 5 – Groupe du dodécaèdre

De plus, tout élément du groupe  $G$  transforme une face en une face, donc  $G$  agit sur l'ensemble des faces. Le stabilisateur d'une face est clairement d'ordre 5, donc on a  $\text{card}(G) \leq 60$ . La proposition précédente assure que  $G$  est isomorphe à  $\mathfrak{A}_5$ . On en déduit immédiatement que le groupe des isométries d'un dodécaèdre est isomorphe à  $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ .

### 3.4 Sous-groupes finis de $O(3)$

Dans cette partie, on étudie les sous-groupes finis de  $O(3)$ . L'essentiel est de classifier les sous-groupes finis d'isométries directes. On va montrer qu'on les connaît déjà tous à ce stade.

Un sous-groupe  $G$  de  $SO(3)$  agit naturellement sur la sphère  $\mathbb{S}^2$ . Si  $g \in G \setminus \{\text{Id}\}$ , on appelle *pôle* de  $g$  tout point de  $\mathbb{S}^2$  laissé stable par  $g$ . On note  $X$  l'ensemble des pôles des éléments de  $G$ . Notons que tout élément  $g \in G \setminus \{\text{Id}\}$  admet deux pôles opposés (les deux points d'intersection de la sphère  $\mathbb{S}^2$  avec son axe de rotation). Par ailleurs, le groupe  $G$  agit naturellement sur  $X$ . Notons  $\Omega_1, \dots, \Omega_s$  l'ensemble des orbites de cette action de telle sorte que les cardinaux  $\nu_1, \dots, \nu_s$  de leurs stabilisateurs respectifs soient classés dans l'ordre décroissant. On a

$$\begin{aligned} 2(\text{card } G - 1) &= \sum_{g \in G \setminus \{\text{Id}\}} \text{card}\{x \in X \mid g(x) = x\} = \text{card}\{(g, x) \in G \setminus \{\text{Id}\} \times X \mid g(x) = x\} \\ &= \sum_{x \in X} \text{card}\{g \in G \setminus \{\text{Id}\} \mid g(x) = x\} = \sum_{i=1}^s \sum_{x \in \Omega_i} \text{card}\{g \in G \setminus \{\text{Id}\} \mid g(x) = x\} \\ &= \sum_{i=1}^s \text{card } \Omega_i (\text{card } \text{stab}(\Omega_i) - 1) = \text{card } G \sum_{i=1}^s \left(1 - \frac{1}{\nu_i}\right). \end{aligned}$$

On obtient donc l'équation suivante :

$$2 - \frac{2}{\text{card } G} = \sum_{i=1}^s \left(1 - \frac{1}{\nu_i}\right)$$

Cette égalité nous donne beaucoup d'informations sur  $s$ ,  $\text{card } G$  et les  $\nu_i$  ( $i \leq s$ ). En effet, on obtient :

(i) comme les  $\nu_i$  sont supérieurs ou égaux à 2, on a

$$2 > 2 - \frac{2}{\text{card } G} = \sum_{i=1}^s \left(1 - \frac{1}{\nu_i}\right) \geq \frac{s}{2},$$

ce qui assure que  $s \leq 3$ . Par ailleurs,  $\text{card } G \geq 2$ , donc  $2 - 2/G \geq 1$  ce qui donne  $s \geq 2$ .

(ii) supposons d'abord que  $s = 2$ . Alors

$$2 - \frac{2}{\text{card } G} = 2 - \frac{1}{\nu_1} - \frac{1}{\nu_2} \quad \text{d'où} \quad \nu_1 = \nu_2 = \text{card } G$$

Dans ce cas, il y a deux pôles opposés sur la sphère, qui sont stables par tous les éléments de  $G$ . Par conséquent,  $G$  est constitué de rotations qui ont toutes le même axe. Par projection sur le plan orthogonal à cet axe, le groupe  $G$  est isomorphe à un sous-groupe fini de  $O(2)$  donc à un groupe cyclique.

(iii) supposons maintenant que  $s = 3$ . On a alors

$$2 - \frac{2}{\text{card } G} = 3 - \frac{1}{\nu_1} - \frac{1}{\nu_2} - \frac{1}{\nu_3} \quad \text{d'où} \quad 1 + \frac{2}{\text{card } G} = \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3}$$

Mais comme on a supposé que  $\nu_1 \geq \nu_2 \geq \nu_3$ , on a

$$1 < \frac{2}{\text{card } G} \leq \frac{3}{\nu_3} \quad \text{d'où} \quad \nu_3 = 2.$$

On obtient alors

$$\frac{1}{2} < \frac{1}{2} + \frac{2}{\text{card } G} = \frac{1}{\nu_1} + \frac{1}{\nu_2} \leq \frac{2}{\nu_2} \quad \text{d'où} \quad \nu_2 \in \{2, 3\}.$$

a. si  $\nu_2 = 2$ , on obtient  $\nu_1 = \text{card } G/2$ . Comme dans le cas précédent, le stabilisateur de l'orbite  $\Omega_1$  est cyclique, isomorphe à  $\mathbb{Z}/\frac{n}{2}\mathbb{Z}$ . De plus, une isométrie  $g \in G$  qui ne stabilise pas l'orbite  $\Omega_1$  est forcément un demi-tour (une telle isométrie échange les deux points de  $\Omega_1$ ). On en déduit que le groupe  $G$  est dihédral.

b. si  $\nu_2 = 3$ , alors

$$\frac{1}{\nu_1} = \frac{1}{6} + \frac{2}{\text{card } G} \geq \frac{1}{6} \quad \text{d'où} \quad \nu_1 \in \{3, 4, 5\}.$$

- Si  $\nu_1 = 3$ , alors  $\text{card } G = 12$ . L'orbite  $\Omega_1$  est de cardinal 4. Le groupe  $G$  stabilisant cette orbite, et toute isométrie fixant 4 point de la sphère étant l'identité, le groupe  $G$  est isomorphe à un sous-groupe de  $\mathfrak{S}_4$ . Comme il est de cardinal 12,  $G$  est isomorphe à  $\mathfrak{A}_4$ .
- Si  $\nu_1 = 4$ , alors  $\text{card } G = 24$ . L'orbite  $\Omega_2$  contient tous les points d'ordre 3. Or si un point est d'ordre 3, son opposé l'est aussi. Ainsi, l'orbite  $\Omega_2$  est constituée de 4 paires de points opposés. Le groupe  $G$  agit sur ces paires de points, et une isométrie directe qui fixe 4 paires de points de la sphère est l'identité. Par conséquent,  $G$  est isomorphe à un sous-groupe de  $\mathfrak{S}_4$ . On en déduit que  $G$  est isomorphe à  $\mathfrak{S}_4$ .
- si  $\nu_1 = 5$ , alors  $\text{card } G = 60$ . Un argument similaire au cas précédent montre que  $G$  est alors isomorphe à  $\mathfrak{A}_5$ .

On a ainsi prouvé le théorème suivant :

**Théorème 5.** *Tout sous-groupe fini de  $SO(3)$  est isomorphe à l'un des groupes  $\mathbb{Z}/n\mathbb{Z}$ ,  $\mathbb{D}_{2n}$ ,  $\mathfrak{A}_4$ ,  $\mathfrak{S}_4$ ,  $\mathfrak{A}_5$ .*

## 4 Coloriages

### 4.1 Formalisation

On s'intéresse ici au nombre de coloriages des sommets d'un polyèdre. Naturellement, on ne veut compter qu'une seule fois deux coloriages qui s'obtiennent simplement par une transformation du polyèdre à colorier. Formalisons un peu ceci.

On considère un ensemble fini d'objets  $\mathbb{X}$  (ici les sommets du polyèdre à colorier), un ensemble fini de couleurs  $\mathbb{A}$  et un groupe fini  $G$  agissant sur  $\mathbb{X}$  (ici le groupe d'isométries du polyèdre régulier). On appelle *coloriage* toute application de  $\mathbb{X}$  dans  $\mathbb{A}$ . Le groupe  $G$  agit naturellement sur  $\mathbb{A}^{\mathbb{X}}$  via

$$\begin{aligned} G \times \mathbb{A}^{\mathbb{X}} &\longrightarrow \mathbb{A}^{\mathbb{X}} \\ (g, \phi) &\longmapsto g\phi : x \mapsto \phi(g^{-1}x). \end{aligned}$$

Les orbites sous cette action sont appelées *schéma de coloriage*. Le but de ce qui suit est de compter le nombre  $\mathfrak{U}$  de schémas de coloriage.

## 4.2 La formule de Burnside

**Lemme 2.** Soit  $H$  un groupe agissant sur un ensemble  $\mathbb{Y}$ . Alors le nombre d'orbites  $\gamma$  de cette action est donné par

$$\gamma = \frac{1}{\text{card } H} \sum_{h \in H} \text{card fix}(h).$$

Pour montrer ce lemme, on calcule de deux manières le cardinal de l'ensemble

$$F = \{(y, h) \in \mathbb{Y} \times H \mid h(y) = y\}.$$

On a

$$\sum_{h \in H} \text{card fix}(h) = \text{card } F = \sum_{y \in \mathbb{Y}} \text{card stab}(y) = \sum_{y \in \mathbb{Y}} \frac{\text{card } H}{\text{card } \Omega_y} = \gamma \cdot \text{card } H.$$

**Proposition 6.** Dans la situation du 4.1, on a

$$\mathfrak{U} = \frac{1}{\text{card } G} \sum_{g \in G} \text{card } \mathbb{A}^{\gamma(g)},$$

où  $\gamma(g)$  désigne le nombre d'orbites de  $\mathbb{X}$  sous l'action de  $\langle g \rangle$ , ie. le nombre de cycles de  $g$  (vu comme une permutation de  $\mathbb{X}$ ).

On applique simplement le lemme précédent. Soient  $\phi \in \mathbb{A}^{\mathbb{X}}$  et  $g \in G$ . Alors  $\phi$  est dans  $\text{fix}(g)$  si et seulement si  $\phi$  est constante sur les orbites de  $\mathbb{X}$  sous l'action de  $\langle g \rangle$ . On a donc une bijection

$$\begin{aligned} \text{fix}(g) &\longrightarrow \mathbb{A}^{\gamma(g)} \\ \phi &\longmapsto (\phi(x_i))_{i=1, \dots, \gamma(g)}, \end{aligned}$$

où  $(x_i)_{i=1, \dots, \gamma(g)}$  est un système de représentants des orbites de  $g$ . On obtient ainsi le résultat.

APPLICATION. On peut déjà appliquer ce résultat à notre problème. Considérer un polygone régulier : on veut compter le nombre de coloriages de sommets distincts modulo rotations et symétries, ou autrement dit compter le nombre de colliers de perles distincts que l'on peut réaliser avec  $p$  perles et au plus  $q$  couleurs. Le groupe est ici  $\mathbb{D}_{2p}$ . Par exemple, pour  $p = 6$ , le groupe  $\mathbb{D}_{12}$  est constitué des transformations suivantes

type	nombre	nombre de cycles
Id	1	6
(26)(35)(1)(4)	3	4
(12)(36)(45)	4	3
(135)(246)	2	2
(123456)	2	1

On obtient donc  $\frac{1}{12} (q^6 + 3q^4 + 4q^3 + 2q^2 + 2q)$  colliers à 6 perles et au plus  $q$  couleurs.

## 4.3 Théorème de Polya

Le but de ce dernier paragraphe est de généraliser le résultat précédent pour pouvoir obtenir plus de résultats. On conserve les notations introduites au 4.1. Pour garder plus d'information sur le coloriage, on introduit un anneau  $A$  et une fonction  $v : \mathbb{A} \rightarrow A$  appelée *poids*. Pour tout coloriage  $\phi \in \mathbb{A}^{\mathbb{X}}$ , on appelle *poids* de  $\phi$  la quantité

$$V(\phi) = \prod_{x \in \mathbb{X}} v(\phi(x)).$$

On a par ailleurs besoin du polynôme suivant :

**Définition 6** (Polynôme indicateur de cycles). Pour tout  $g \in G$  et  $1 \leq i \leq m = \text{card } \mathbb{X}$ , on note  $c_i(g)$  le nombre d'orbites de  $\mathbb{X}$  sous l'action de  $\langle g \rangle$  de taille  $i$ , ie. le nombre de cycles de longueur  $i$  de  $g$  (vu comme une permutation de  $\mathbb{X}$ ).

On appelle polynôme indicateur de cycles de l'action de  $G$  sur  $\mathbb{X}$  le polynôme

$$Z(X_1, \dots, X_m) = \frac{1}{\text{card } G} \sum_{g \in G} X_1^{c_1(g)} \dots X_m^{c_m(g)}.$$

En utilisant les mêmes outils que précédemment, nous allons montrer le théorème suivant :

**Théorème 6 (Polya).** *Soit  $\phi_1, \dots, \phi_{\mathfrak{U}}$  un système de représentants des orbites de  $\mathbb{X}$  sous l'action de  $G$ . Alors*

$$\sum_{i=1}^{\mathfrak{U}} V(\phi_i) = Z \left( \sum_{a \in \mathbb{A}} v(a), \sum_{a \in \mathbb{A}} v(a)^2, \dots, \sum_{a \in \mathbb{A}} v(a)^m \right).$$

Soit  $a \in A$ . La formule du lemme 2 assure que le nombre de schémas de coloriage dont le poids est  $a$  est

$$\frac{1}{\text{card } G} \sum_{g \in G} \text{card} (\text{fix}(g) \cap V^{-1}(\{a\})).$$

On a donc

$$\begin{aligned} \sum_{i=1}^{\mathfrak{U}} V(\phi_i) &= \sum_{a \in A} \left[ a \cdot \frac{1}{\text{card } G} \sum_{g \in G} \text{card} (\text{fix}(g) \cap V^{-1}(\{a\})) \right] \\ &= \frac{1}{\text{card } G} \sum_{g \in G} \left[ \sum_{a \in A} a \cdot \text{card} (\text{fix}(g) \cap V^{-1}(\{a\})) \right] \\ &= \frac{1}{\text{card } G} \sum_{g \in G} \left[ \sum_{\phi \in \text{fix}(g)} V(f) \right] \end{aligned}$$

Or il se trouve que pour tout  $g \in G$ , si on désigne par  $\mathbb{O}$  l'ensemble des orbites de  $\mathbb{X}$  sous l'action de  $\langle g \rangle$  (ie. l'ensemble des cycles de  $g$  vu comme une permutation de  $\mathbb{X}$ ), on a

$$\sum_{\phi \in \text{fix}(g)} V(f) = \sum_{\phi \in \text{fix}(g)} \prod_{x \in \mathbb{X}} v(\phi(x)) = \sum_{\psi \in \mathbb{A}^{\mathbb{O}}} \prod_{o \in \mathbb{O}} v(\psi(o))^{\text{card } o} = \prod_{o \in \mathbb{O}} \sum_{a \in \mathbb{A}} v(a)^{\text{card } o}$$

On obtient donc

$$\sum_{i=1}^{\mathfrak{U}} V(\phi_i) = \frac{1}{\text{card } G} \sum_{g \in G} \left[ \prod_{o \in \mathbb{O}} \sum_{a \in \mathbb{A}} v(a)^{\text{card } o} \right] = Z \left( \sum_{a \in \mathbb{A}} v(a), \sum_{a \in \mathbb{A}} v(a)^2, \dots, \sum_{a \in \mathbb{A}} v(a)^m \right),$$

ce qui termine la preuve.

APPLICATIONS. Donnons quelques exemples d'applications de ce résultat :

- (i) La première chose à remarquer c'est qu'on retrouve immédiatement le résultat de la proposition 6 en considérant le poids constant égal à 1. En effet, on a

$$\sum_{i=1}^{\mathfrak{U}} V(\phi_i) = \sum_{i=1}^{\mathfrak{U}} \prod_{x \in \mathbb{X}} v(\phi_i(x)) = \sum_{i=1}^{\mathfrak{U}} 1 = \mathfrak{U},$$

et 
$$Z \left( \sum_{a \in \mathbb{A}} v(a), \sum_{a \in \mathbb{A}} v(a)^2, \dots, \sum_{a \in \mathbb{A}} v(a)^m \right) = Z(\text{card } \mathbb{A}, \text{card } \mathbb{A}, \dots, \text{card } \mathbb{A}) = \frac{1}{\text{card } G} \sum_{g \in G} \text{card } \mathbb{A}^{\gamma(g)}.$$

- (ii) Par ailleurs, on peut obtenir de nombreuses informations sur les coloriages en choisissant bien l'application de poids. Soit  $q = \text{card } \mathbb{A}$  et  $a_1, \dots, a_q$  les éléments de  $\mathbb{A}$ . Posons  $A = \mathbb{R}[X_1, \dots, X_q]$  et définissons le poids par  $v(a_i) = X_i$ . Alors le nombre de coloriages de  $\mathbb{X}$  avec exactement  $n_i$  objets de couleur  $a_i$  est le coefficient de  $\prod_{i=1}^q X_i^{n_i}$  dans  $Z \left( \sum_{i=1}^q X_i, \sum_{i=1}^q X_i^2, \dots, \sum_{i=1}^q X_i^m \right)$ .

Par exemple, pour le collier à 6 perles, le polynôme indicateur de cycles est donné par

$$Z(Y_1, \dots, Y_6) = \frac{1}{12} (Y_1^6 + 3Y_1^2 Y_2^2 + 4Y_2^3 + 2Y_3^2 + 2Y_6).$$

on obtient ainsi par exemple qu'il y a 3 colliers à 6 perles ayant exactement 4 perles bleues et 2 perles rouges (à rotations et symétries près).

## 5 Questions et remarques

### 5.1 Questions

On pourra traiter les problèmes suivants :

- sur les polygones et polyèdres :
  - montrer comment l'on peut obtenir une approximation géométrique de  $\pi$  en calculant les aires de polygones réguliers inscrits et circonscrits au cercle unité. Quelle méthode utiliser pour approcher  $\pi$  ?
  - montrer que si  $F$  est une face d'un polytope  $P$ , alors  $F$  est un polytope dont les faces sont les faces de  $P$  contenues dans  $F$ .
  - montrer que les faces d'un polyèdre régulier sont des polyèdres réguliers de dimension inférieure.
  - montrer la relation d'Euler.
  - donner les détails de la preuve du théorème 3.
- sur la structure des sous-groupes finis de  $O(3)$  :
  - décrire les éléments de  $\mathfrak{S}_4$  et donner la transformation du tétraèdre correspondant (ie. par exemple, une transposition qui inverse deux sommets 1 et 2 et laisse stable les deux autres sommets 3 et 4 s'obtient simplement par la symétrie orthogonale par rapport au plan contenant 3, 4 et le milieu de 1 et 2 (fig. 3)). De la même façon, décrire géométriquement les sous-groupes de  $\mathfrak{S}_4$
  - même question sur le cube.
  - en remarquant que l'on peut inscrire deux tétraèdres opposés dans un cube (fig. 6), montrer géométriquement que l'on a la suite exacte :

$$1 \longrightarrow G_T \longrightarrow G_C \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1,$$

(où  $G_T$  et  $G_C$  désignent respectivement le groupe des isométries du tétraèdre et du cube).

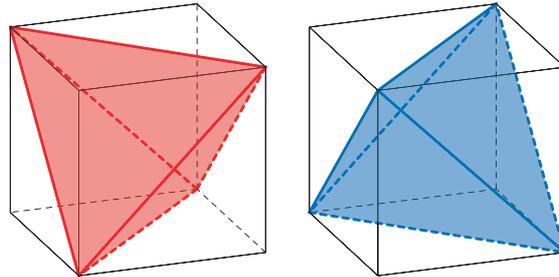


FIG. 6 – Deux tétraèdres opposés inclus dans un cube

- en remarquant que l'on peut inscrire exactement 6 cubes dans un dodécaèdre (fig. 7), et en étudiant l'action du groupe des isométries du dodécaèdre sur ces cubes, retrouver le groupe du dodécaèdre.

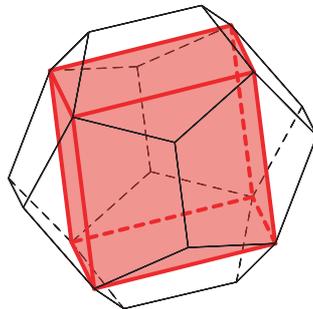


FIG. 7 – Un cube dans un dodécaèdre

- à partir des sous-groupes finis de  $SO(3)$  (théorème 5), donner une description des sous-groupes finis de  $O(3)$ .
- donner une description des sous-groupes finis du groupe linéaire  $GL_n(\mathbb{R})$  et du groupe affine  $GA_n(\mathbb{R})$  (pour  $n \in \{2, 3\}$ ).

3. sur quelques problèmes simples de théorie des groupes qui apparaissent dans ce texte :
- (a) donner des familles génératrices de  $\mathfrak{S}_n$  (resp.  $\mathfrak{A}_n$ ). Montrer que toute famille de transpositions qui engendre  $\mathfrak{S}_n$  a au moins  $n - 1$  éléments. Donner deux exemples de familles génératrices de  $\mathfrak{S}_n$  :
    - l’une constituée de  $n - 1$  transpositions,
    - l’autre de cardinal 2.
  - (b) que peut-on dire d’un groupe dont tous les éléments sont d’ordre 2 ?
  - (c) dans quel cas peut-on dire que l’ordre d’un produit de deux éléments d’un groupe est le produit des ordres de ces éléments ?
  - (d) montrer que le seul morphisme non trivial de  $\mathfrak{S}_n$  dans  $\{\pm 1\}$  est la signature. Montrer qu’un sous-groupe d’indice 2 de  $\mathfrak{S}_n$  est toujours le groupe alterné  $\mathfrak{A}_n$ .
  - (e) Soit  $G$  un groupe,  $p$  le plus petit nombre premier divisant le cardinal de  $G$  et  $H$  un sous-groupe de  $G$  d’indice  $p$ . Montrer que  $H$  est distingué.
4. sur les coloriage :
- (a) en utilisant uniquement la formule de la proposition 6, donner le nombre de colliers avec 6 perles et exactement 4 couleurs.
  - (b) donner le polynôme indicateur de cycles du groupe du cube. Donner le nombre de coloriage du cube avec 2 faces blanches et 4 faces noires.
  - (c) écrire une procédure maple qui calcule le polynôme indicateur de cycles d’un groupe.
  - (d) donner une procédure maple qui dessine les différents colliers à  $p$  perles et  $q$  couleurs.

## 5.2 Remarques et références

De nombreuses références exposent les idées présentes dans ce texte avec plus ou moins de détails :

- (i) pour ce qui est de l’étude des sous-groupes finis de  $O(2)$  et  $O(3)$ , on pourra consulter
  - *les cinq polyèdres réguliers de  $\mathbb{R}^3$  et leurs groupes*, par J.M. ARNAUDIÈS,
  - le livre de *Géométrie* (Tome 1) de M. BERGER,
  - le livre d’*Algèbre et géométrie* de F. COMBES,
  - le *cours d’algèbre* de D. PERRIN pour l’étude du groupe symétrique et les caractérisations de  $\mathfrak{A}_5$  (il me semble que la preuve de la proposition 4 est assez optimale ; je n’ai pas de référence qui la donne en détails),
- (ii) tandis que pour ce qui est du théorème de Polya, on ouvrira le livre d’*Analyse combinatoire* de L. COMTET (la preuve du théorème de Polya est donnée explicitement).

Les idées développées dans ce texte constituent de bons exemples dans les leçons d’agrégation suivantes

- SOUS-GROUPES FINIS DE  $O(2)$  ET  $O(3)$
- GROUPES OPÉRANT SUR UN ENSEMBLE  
On utilise profondément les méthodes et résultats de cette leçon. L’étude des sous-groupes fini de  $O(3)$  et le théorème de Polya sont de bons exemples d’utilisation d’actions de groupes.
- GROUPES FINIS
- GROUPE DES PERMUTATIONS D’UN ENSEMBLE FINI  
Les groupes des polyèdres réguliers sont des groupes de permutations. Il est particulièrement intéressant de comprendre les liens entre géométrie et propriétés algébriques. L’étude du groupe des isométries du dodécaèdre constitue un bon développement.
- UTILISATION DES GROUPES EN GÉOMÉTRIE
- MÉTHODES COMBINATOIRES, PROBLÈME DE DÉNOMBREMENT  
Les résultats de dénombrement issus de la théorie des groupes constituent l’un des aspects de cette leçon. Le théorème de Polya fournit un bon développement.