UNIVERSITÉ
de Picardie
Jules Verne

Groupes de Réflexions

Complexes de Rang deux

MÉMOIRE DE MASTER 2

AGRÉGATION EXTERNE

Arthur GARNIER

Université de Picardie Jules Verne

Département de Mathématiques

Sous la direction de M. Ivan MARIN

2016-2017

Pour ma famille...

Table des matières

Introduction

Dans ce travail, nous étudions la structure de quelques groupes de réflexions untaires, c'est-à-dire des sous-groupes finis d'un groupe unitaire, engendrés par des réflexions. Une réflexion unitaire est une transformation géométrique d'un espace vectoriel complexe d'ordre fini qui fixe ponctuellement un hyperplan. On peut imaginer une réflexion comme une sorte de kaléidoscope, ou un arrangement de miroirs. En fait, la structure des groupes de réflexions est bien particulière, si bien que l'on peut les classifier. Aussi, ce mémoire envisage-t-il de donner une classification partielle de ces groupes.

Premièrement, nous donnons quelques rappels et propriétés élémentaires des formes hermitiennes (en se bornant au cas des formes définies positives) et des réflexions. On se propose également de fournir quelques rappels de représentations et des compléments de théorie des groupes, comme par exemple le produit central ou le produit en couronne. On en déduit en particulier la structure des sous-groupes de Sylow des groupes symétriques $\mathfrak{S}_n$. On introduit ensuite les groupes de réflexions.

Dans un second temps, pour notre étude, il nous faut distinguer deux classes de groupes de réflexions : les groupes primitifs et imprimitifs. Nous construisons ensuite les groupes $G(m, p, n)$, qui sont un type de groupes de réflexions imprimitifs. Le résultat principal de cette partie étant que ces groupes sont essentiellement les seuls groupes imprimitifs de tout rang, un théorème de Shephard et Todd, datant de 1954.

Ensuite, on introduit l'algèbre des quaternions réels et nous en étudions les premières propriétés. Nous verrons notamment son lien étroit avec la géométrie ; et plus précisément avec les groupes d'isométries $SO_3(\mathbb{R})$, $SO_4(\mathbb{R})$ et $SU_2(\mathbb{C})$. Dans cette partie, nous inspecterons aussi la structure des sous-groupes finis des unités des quaternions (via ceux de $SO_3(\mathbb{R})$), résultat qui sera fondamental pour la suite ; et qui nous donnera en particulier les sous-groupes finis de $SU_2(\mathbb{C})$.

Enfin, dans la dernière partie, nous serons en mesure de classifier des groupes de réflexions unitaires primitifs de rang 2 ; en suivant la méthode de [15]. Nous en décrirons l'ordre, l'ordre des centres et les générateurs. Puis, nous donnerons une table récapitulative de notre classification, ainsi qu'un treillis partiel des 19 groupes primitifs de rang 2.

De plus, nous donnons en Annexes quelques résultats utiles sur les groupes symétriques et alternés, les groupes de déplacements des solides de Platon, les sous-groupes finis de $SO_3(\mathbb{R})$ et enfin quelques algorithmes à implémenter sur le (génial) logiciel libre `GAP`, algorithmes permettant de construire et d'explorer les groupes que nous avons construits.

Pour conclure, je tiens à remercier M. Ivan Marin pour son aide précieuse, sa disponibilité et pour m'avoir fait découvrir ce sujet passionnant. Je remercie de plus chaleureusement toute ma famille pour son écoute et son soutien sans faille tout au long de cette année difficile...

Prérequis et notations

Dans ce travail,

1. $\mathbb{N}$ (resp. $\mathbb{Z}$) désigne l'ensemble des entiers naturels (resp. l'anneau des entiers relatifs),
2. $\mathbb{Q}$ (resp. $\mathbb{R}$, $\mathbb{C}$) désigne le corps des rationnels (resp. des réels, des complexes),
3. $\hookrightarrow$ (resp. $\twoheadrightarrow$) dénote un monomorphisme (resp. un épimorphisme),
4. $\simeq$ veut dire "est isomorphe à",
5. $\trianglelefteq$ signifie "est un sous-groupe distingué de",
6. si G est un groupe fini et si p est un nombre premier divisant l'ordre de G, on dénote par $\mathrm{Syl}_p(G)$ l'ensemble des p-sous-groupes de Sylow de G.
7. Pour un sous-groupe H d'un groupe G, on note $N_G(H)$ normalisateur de H dans G. De plus, si $g \in G$, on note $C_G(g)$ le centralisateur de g dans G, et g^G sa classe de conjugaison.
8. Le groupe symétrique (resp. alterné) sur n lettres sera noté $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$).
9. On note $\mathcal{D}_{2n}$ le groupe diédral d'ordre $2n$, présenté par
$$\mathcal{D}_{2n} := \left\langle \omega, \sigma \mid \omega^n = 1, \sigma^2 = 1, \sigma\omega\sigma = \omega^{-1} \right\rangle .$$
10. $\mathcal{Q}_8$ dénote le groupe des quaternions d'ordre 8 :
$$\mathcal{Q}_8 := \left\langle x, y \mid x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \right\rangle .$$

Première partie

Réflexions, Représentations et Produits de Groupes

1.1 Formes hermitiennes G-invariantes

Rappelons ici quelques notions de géométrie vectorielle hermitienne, indispensables à l'introduction de l'étude des réflexions.

Donnons-nous V un espace vectoriel complexe de dimension finie.

Définition 1. Une forme hermitienne sur V est une application $(-,-) : V \times V \to \mathbb{C}$ telle que pour tous $v_1, v_2, v, w \in V$ et tout $a \in \mathbb{C}$, on ait

$$(v_1 + v_2, w) = (v_1, w) + (v_2, w),$$

$$(av, w) = a(v, w),$$

$$\overline{(v, w)} = (w, v).$$

On dit de plus que la forme $(-,-)$ est définie positive si, pour tout $v \in V$, on a

$$(v, v) \geq 0, \quad \text{et} \quad (v, v) = 0 \ \Leftrightarrow \ v = 0.$$

Exemple 1. Si $(e_1, \ldots, e_n)$ est une base de V, en écrivant

$$v := a_1 e_1 + \cdots + a_n e_n \in V, \quad \text{et} \quad w := b_1 e_1 + \cdots + b_n e_n,$$

on définit une forme hermitienne définie positive par

$$(v, w) := a_1 \overline{b_1} + \cdots + a_n \overline{b_n}.$$

De plus, par réduction de Gauss, on voit que toute forme hermitienne définie positive s'écrit de cette façon dans une certaine base. Ainsi, deux formes hermitiennes définies positives $(-,-)$ et $[-,-]$ sont équivalentes, au sens où

$$\exists \varphi \in GL(V) \ ; \ \forall u, v \in V, \ (\varphi(u), \varphi(v)) = [u, v].$$

Définition 2. Si G est un sous-groupe de $GL(V)$, on dit qu'une forme hermitienne $(-,-)$ est G-invariante si

$$\forall g \in G, \ \forall u, v \in V, \ (gu, gv) = (u, v).$$

Lemme 1. *Si G est un sous-groupe fini de $GL(V)$, il existe une forme hermitienne définie positive G-invariante.*

Démonstration. Choisissons en effet une forme hermitienne définie positive $[-,-]$ et posons, pour $u, v \in V$,

$$(u, v) := \sum_{g \in G} [gu, gv].$$

Alors, $(-,-)$ est clairement une forme hermitienne définie positive sur V et on a

$$(gu, gv) = \sum_{h \in G} [hgu, hgv] = \sum_{k \in G} [ku, kv] = (u, v).$$

□

Définition 3.
- Si $(-,-)$ est une forme hermitienne définie positive sur V, on dit que $x \in GL(V)$ est unitaire (ou que c'est une isométrie) si la forme $(-,-)$ est $\langle x \rangle$-invariante, c'est-à-dire si
$$\forall u, v \in V,\ (xu, xv) = (u, v).$$
- Une base $(e_i)_i$ de V est orthogonale si
$$\forall i \neq j,\ (e_i, e_j) = 0.$$
On dit de plus que (e_i) est orthonormée si
$$\forall i, j,\ (e_i, e_j) = \delta_{i,j}.$$

Remarque 1. Soit M la matrice de $x \in GL(V)$ dans une base orthonormée. Alors x est unitaire si et seulement si M est une matrice unitaire, i.e. si $M^*M = MM^* = I$, où $M^* := {}^t\overline{M}$ est l'adjointe de M.

Définition 4. Soit $(-,-)$ une forme hermitienne définie positive sur V. Le groupe des isométries de V relativement à $(-,-)$ est noté $U(V)$ et on l'appelle le groupe unitaire de $(-,-)$. Son sous-groupe formé des isométries de déterminant 1 est noté $SU(V)$, groupe spécial unitaire. Les groupes matriciels correspondant sont notés respectivement $U_n(\mathbb{C})$ et $SU_n(\mathbb{C})$, avec $n = \dim V$.

Remarque 2.
- Comme deux formes hermitiennes définies positives sont équivalentes et comme $U(V)$ ne dépend que de la forme considérée, $U(V)$ est unique à conjugaison près dans $GL(V)$.
- Avec ces notations, le Lemme 1 nous affirme que tout sous-groupe fini de $GL(V)$ est conjugué à un sous-groupe de $U(V)$.

1.2 Réflexions

Ici, V désigne un $\mathbb{C}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $(-,-)$ est une forme hermitienne définie positive sur V.

Définition 5.
- Si U est une partie de V, l'orthogonal de U est défini par
$$U^\perp := \{v \in V \ ; \ \forall u \in U, \ (u,v) = 0\}.$$
C'est un sous-espace de V.
- Si U et W sont des sous-espaces de V, l'expression
$$V = U \perp W$$
signifie que pour tous $u \in U$, $w \in W$, on a $(u,w) = 0$ et qu'on a $V = U \oplus W$.

Remarque 3.
- On a $V = U \perp W$ si et seulement si $W = U^\perp$,
- $U^{\perp\perp} = U$,
- $\dim U + \dim U^\perp = \dim V$.

Définition 6. Notons I l'identité de $GL(V)$. Pour $g \in GL(V)$ et $H \subseteq GL(V)$, posons
1. $\operatorname{Fix} g := \ker(1-g) = \{v \in V \ ; \ gv = v\}$,
2. $V^H := \operatorname{Fix}_V(H) := \bigcap_{h \in H} \operatorname{Fix} h$,
3. $[V,g] := \operatorname{im}(1-g)$.

Lemme 2. *Pour tout $g \in U(V)$, on a $[V,g] = (\operatorname{Fix} g)^\perp$.*

Démonstration. Supposons que $u := (1-g)w \in [V,g]$ et que $v \in \operatorname{Fix} g$. Alors
$$(u,v) = (w - gw, v) = (w,v) - (gw,v) = (gw,gv) - (gw,v) = (gw, gv - v) = 0,$$
donc $[V,g] \subseteq (\operatorname{Fix} g)^\perp$ et on a égalité en comparant les dimensions. □

Définition 7.
- Une application linéaire g est une réflexion si g est d'ordre fini et si $[V,g]$ est une droite vectorielle.
- Si g est une réflexion, $\operatorname{Fix} g$ est un hyperplan, appelé hyperplan de g.
- Si $0 \neq a$ parcourt la droite $[V,g]$, pour tout $v \in V$, il existe $\varphi(v) \in \mathbb{C}$ tel que $v - gv = \varphi(v)a$. Il est alors clair que $\varphi : V \to \mathbb{C}$ est une forme linéaire telle que $\operatorname{Fix} g = \ker \varphi$.
- On dit que g est une réflexion unitaire si elle préserve la forme $(-,-)$. Dans ce cas, on a
$$V = [V,g] \perp \operatorname{Fix} g.$$

Remarque 4. Soit $g \in GL(V)$ une réflexion d'ordre m. Le sous-groupe $\langle g \rangle$ est fini et le Lemme 1 implique que g laisse invariante une forme hermitienne définie positive. Ainsi, g est une réflexion unitaire pour une certaine forme hermitienne définie positive. Si $H := \operatorname{Fix} g$, g laisse la droite $H^\perp$ invariante et donc, dans une base adaptée à la décomposition $V = H \perp H^\perp$, g est de matrice

$$\operatorname{diag}(\zeta, 1, \ldots, 1) = \begin{pmatrix} \zeta & & & (0) \\ & 1 & & \\ & & \ddots & \\ (0) & & & 1 \end{pmatrix},$$

avec ζ une racine $m^{\text{ième}}$ de l'unité.

Définition 8.
- Une racine d'une droite l de V est un vecteur non nul quelconque de l.
- Si g est une réflexion unitaire, une racine de g est une racine de $[V, g]$.
- Une racine a est courte, longue ou grande si (a, a) est égal à 1, 2 ou 3, respectivement.

Remarque 5. Toute droite de $\mathbb{C}^n$ contient des racines courtes, longues et grandes, chacune étant unique à multiplication par un élément de $\mathbb{S}^1 = \{z \in \mathbb{C} \ ; \ |z| = 1\}$ près.

Lemme 3. *Si $g, h \in GL(V)$, alors on a*

$$\operatorname{Fix}(ghg^{-1}) = g\operatorname{Fix}(h).$$

En particulier, si r est une réflexion d'hyperplan H, alors grg^{-1} est une réflexion d'hyperplan gH.

Démonstration. C'est évident. □

Définition 9. Un groupe de réflexions unitaires (ou complexes) est un sous-groupe fini de $U(V)$, engendré par des réflexions.

Remarque 6.
1. Par le Lemme 1, tout sous-groupe fini de $GL(V)$ engendré par des réflexions est un groupe de réflexions unitaires pour une certaine forme hermitienne définie positive.
2. $U(V)$ est lui-même engendré par des réflexions, par le théorème de Cartan-Dieudonné.
3. Il est important de remarquer que le concept de "groupe de réflexions unitaires" dépend autant du groupe que de sa représentation. Un groupe donné peut ou non agir comme groupe de réflexions. Par exemple, pour $\zeta := \exp\left(\frac{2i\pi}{m}\right)$, l'élément $\operatorname{diag}(\zeta, 1, \ldots, 1)$ engendre un groupe de réflexions cyclique d'ordre m et le groupe engendré par $\operatorname{diag}(\zeta, \zeta, 1, \ldots, 1)$, isomorphe au premier, n'est pas un groupe de réflexions.
4. La phrase "G est un groupe de réflexions unitaires dans V" signifie que G est un groupe fini, engendré par des réflexions dans V.

Exemple 2. Si ω est une racine cubique de l'unité, les matrices

$$r := \begin{pmatrix} \omega & 0 \\ -\omega^2 & 1 \end{pmatrix}, \quad \text{et} \quad s := \begin{pmatrix} 1 & \omega^2 \\ 0 & \omega \end{pmatrix}$$

sont des réflexions d'ordre 3 et engendrent un groupe d'ordre 24. Ce groupe sera plus tard noté G_4, conformément à la notation de Shephard-Todd.

Exemple 3. Un autre exemple de groupe de réflexions unitaires est le groupe symétrique $\mathfrak{S}_n$. En effet, pour représenter $\mathfrak{S}_n$ comme groupe de réflexions, on choisit une base orthonormée $(e_1, \ldots, e_n)$ de V, de base duale $(e_n^*, \ldots, e_n^*)$. À $\sigma \in \mathfrak{S}_n$, on associe l'endomorphisme de V qui envoie e_i sur $e_{\sigma(i)}$, de matrice la matrice de permutation associée à σ. En particulier, la transposition $(i, j) \in \mathfrak{S}_n$ correspond à la réflexion qui échange e_i et e_j et laisse fixe les autres éléments de la base. Son hyperplan est $\ker(e_i^* - e_j^*)$. $\mathfrak{S}_n$ est engendré par les transpositions, donc est bien un groupe de réflexions unitaires.

Étant donné un hyperplan H de V, soit $L_H : V \to \mathbb{C}$ une forme linéaire telle que $H = \ker(L_H)$. Alors $L_H \in V^*$ est déterminée par H, à multiplication par un scalaire non nul près.

Lemme 4. *Soient r une réflexion d'ordre m dans $GL(V)$, $H := \mathrm{Fix}\,(r)$ son hyperplan et supposons que $a \in [V, g]$ soit non nul. Alors, il existe une racine primtive $m^{\text{ième}}$ de l'unité α telle que*

$$\forall v \in V,\ rv = v - (1 - \alpha)\frac{L_H(v)}{L_H(a)}a.$$

Démonstration. Par définition, on a $rv = v - \varphi(v)a$ pour $\varphi \in V^*$ telle que $H = \ker(\varphi)$ et $a \notin H$. Ainsi, $ra = \alpha a$ pour $\alpha \in \mathbb{C}$ d'ordre m et donc $\varphi(a) = 1 - \alpha$. Finalement, on a $\varphi = \lambda L_H$ pour un $\lambda \neq 0$ et il vient alors immédiatement $\lambda = \frac{1-\alpha}{L_H(a)}$, d'où le résultat. □

Corollaire 1. *Soit r une réflexion unitaire d'ordre m dans $U(V)$ et supposons que a soit une racine de r, de longueur 1. Alors, il existe une racine primitive $m^{\text{ième}}$ de l'unité α telle que*

$$\forall v \in V,\ rv = v - (1 - \alpha)(v, a)a.$$

Démonstration. C'est le Lemme 4 appliqué au cas $L_H(v) := (v, a)$. □

Définition 10. Soient $a \in V$ non nul et $\alpha \neq 1$ une racine $m^{\text{ième}}$ de l'unité. On définit la réflexion $r_{a,\alpha}$ par

$$\forall v \in V,\ r_{a,\alpha}(v) := v - (1 - \alpha)\frac{(v, a)}{(a, a)}a. \tag{1}$$

$r_{a,\alpha}$ est une transformation unitaire d'ordre m.

Proposition 1. *On a les propriétés suivantes :*

1.
$$r_{a,\alpha}r_{a,\beta} = r_{a,\alpha\beta},$$

2.
$$\forall g \in U(V),\ gr_{a,\alpha}g^{-1} = r_{ga,\alpha},$$

3.
$$\forall \lambda \in \mathbb{C}^\times,\ r_{\lambda a,\alpha} = r_{a,\alpha}.$$

Démonstration. C'est clair. □

Proposition 2. *Si $g \in U(V)$ et si $gr_{a,\alpha}g^{-1} = r_{a,\alpha}^k$ pour un certain k, alors $k = 1$. En d'autres termes, une réflexion n'est conjuguée à aucune de ses puissances propres.*

Démonstration. Par la Proposition 1, on a $gr_{a,\alpha}g^{-1} = r_{ga,\alpha}$, d'où $r_{ga,\alpha} = r_{a,\alpha}^k$. Or, on a

$$r_{a,\alpha}^k(a) = \alpha^k a$$

et

$$r_{ga,\alpha}(a) = a - (1-\alpha)\frac{(a,ga)}{(a,a)}ga,$$

donc

$$a - (1-\alpha)\frac{(a,ga)}{(a,a)}ga = \alpha^k a \quad \Leftrightarrow \quad ga = \theta a,\ \theta := \frac{1-\alpha^k}{1-\alpha}\frac{(a,a)}{(a,ga)}.$$

Ainsi, g fixe $\mathrm{Fix}\,(r_{a,\alpha})$ et $\mathbb{C}a$. En effet, pour $\mathbb{C}a$, c'est évident et si $u \in \mathrm{Fix}\,(r_{a,\alpha})$, on a $r_{a,\alpha}(gu) = \theta r_{a,\alpha}(u) = \theta u = gu$. Donc, g commute à $r_{a,\alpha}$ car $V = \mathrm{Fix}\,(r_{a,\alpha}) \perp \mathbb{C}a$ et si $v \in V$, $v = f + \lambda a$, $f \in \mathrm{Fix}\,(r_{a,\alpha})$ pour $\lambda \in \mathbb{C}$ et alors

$$r_{a,\alpha}(gv) = r_{a,\alpha}(gf) + \lambda\theta\alpha a = gf + \lambda\theta\alpha a = g(r_{a,\alpha}(f) + \lambda r_{a,\alpha}(a)) = gr_{a,\alpha}(v).$$

Ainsi

$$gr_{a,\alpha}g^{-1} = r_{a,\alpha}$$

et donc $k = 1$. □

Proposition 3. *Les réflexions unitaires $r_{a,\alpha}$ et $r_{b,\beta}$ commutent si et seulement si $\mathbb{C}a = \mathbb{C}b$ ou $(a,b) = 0$.*

Démonstration. Un calcul direct montre que

$$r_{a,\alpha} \circ r_{b,\beta}(v) = r_{a,\alpha}\left(v - (1-\beta)\frac{(v,b)}{(b,b)}b\right)$$

$$= v - (1-\alpha)\frac{(v,a)}{(a,a)}a - (1-\beta)\frac{(v,b)}{(b,b)}b + (1-\alpha)(1-\beta)\frac{(b,a)(v,b)}{(a,a)(b,b)}a,$$

et par symétrie, on a une expression similaire pour $r_{b,\beta} \circ r_{a,\alpha}(v)$. Ainsi, si a et b sont linéairement indépendants, $r_{a,\alpha}$ commute à $r_{b,\beta}$ si et seulement si le dernier terme de chaque expression est nul, i.e. si et seulement si $(a,b) = 0$. □

Proposition 4. *Un sous-espace vectoriel W de V est invariant pour une réflexion r si et seulement si $W \subseteq \mathrm{Fix}\,(r)$ ou $[V, r] \subseteq W$.*

Démonstration. Si $W \subseteq \mathrm{Fix}\,(r)$ alors W est clairement r-invariant. Si $[V, r] \subseteq W$, l'équation (1) montre que W est aussi r-invariant. Réciproquement, supposons W r-invariant et $W \nsubseteq \mathrm{Fix}\,(r)$. Alors $[W, r] \neq 0$ et donc $[V, r] = [W, r] \subseteq W$. □

Corollaire 2. *Si r est une réflexion unitaire de racine a, un sous-espace W est r-invariant si et seulement si $a \in W \cup W^{\perp}$.*

1.3 Compléments sur les groupes et leurs représentations

1.3.1 Produit central

Nous allons définir ici un type particuler de produit de groupes, basé sur le produit direct. Cette construction se révèlera primordiale dans l'étude des groupes primitifs de rang 2, notion que nous étudierons dans la dernière partie de ce travail. La présentation adoptée ici est celle de [11], Chapter 13.

Proposition-Définition 1. *Soient H, K deux groupes, $Z \leq Z(H)$, $W \leq Z(K)$ et $\theta : Z \to W$ un isomorphisme. Posons*

$$X := \{(z, \theta(z^{-1})),\ z \in Z\}.$$

Alors X est un sous-groupe distingué de $H \times K$ et le quotient $(H \times K)\,/_X$ est appelé produit central de H et K selon θ. On le note

$$H \circ_\theta K := (H \times K)\,/_X.$$

Démonstration. Il suffit de montrer que X est distingué. Or, ceci découle directement du fait que X est central dans $H \times K$, et ce car Z et W sont centraux dans H et K respectivement. □

On dispose ensuite d'une caractérisation permettant de détecter les produits centraux ; un peu comme dans le cas du produit semi-direct. Ce résultat nous apprend essentiellement qu'un groupe G est produit central de deux de ses sous-groupes H et K s'il est produit (au sens usuel) de H et K et si tout élément de H commute à tout élément de K, ce qui s'écrit :

Proposition 5. *Soient H et K deux sous-groupes d'un groupe G donné. Sont équivalents*

i) $G \simeq H \circ K$,

ii) $G = HK$ *et* $[H, K] = 1$.

Démonstration. Montrons que $i) \Rightarrow ii)$ et supposons donc que $\theta : Z \to W$ soit un isomorphisme entre deux sous-groupes respectifs de $Z(H)$ et $Z(K)$ définissant le produit central

$$G \simeq H \circ_\theta K \stackrel{\text{def}}{=} (H \times K)\,/_X.$$

La composée

$$H \hookrightarrow H \times K \twoheadrightarrow (H \times K)\,/_X = G$$

est injective. En effet, si $h \in H$ est tel que $\overline{(h,1)} = \overline{(1,1)}$, alors $(h,1) = (z, \theta(z^{-1}))$ avec $z \in Z$ et alors $\theta(z^{-1}) = 1$, d'où $z = 1$ et $h = 1$ comme voulu. De même, on a une injection $K \hookrightarrow G$ et ceci nous permet d'identifier $h \in H$ et $k \in K$ avec $\overline{(h,1)} \in G$ et $\overline{(1,k)} \in G$, respectivement. Mais, dans ce cas, on a pour tout $g \in G$,

$$g = \overline{(h,k)} = \overline{(h,1)(1,k)} \in HK.$$

Soient ensuite $h \in H$ et $k \in K$. On calcule

$$\overline{(h,1)(1,k)(h^{-1},1)(1,k^{-1})} = \overline{(h,k)(h^{-1},k^{-1})} = \overline{(1,1)},$$

donc $[h,k] = 1$ et $[H,K] = 1$.
Réciproquement, on suppose que $G = HK$ et $[H,K] = 1$. Posons $Z := H \cap K$. Alors Z est un sous-groupe de $Z(H)$ et de $Z(K)$ par hypothèse, et soit $\theta := id_Z$, ainsi que $X := \{(z, z^{-1}),\ z \in Z\}$. Définissons encore

$$\begin{array}{rccc} \varphi & : & H \times K & \twoheadrightarrow & HK = G \\ & & (h,k) & \mapsto & hk \end{array}$$

φ est un morphisme car si $h, h' \in H$ et $k, k' \in K$, on peut écrire

$$\varphi((h,k)(h',k')) = \varphi(hh', kk') = hh'kk' = hkh'k' = \varphi(h,k)\varphi(h',k').$$

De plus, on a clairement $X \leq \ker\varphi$. Par ailleurs, si $(h,k) \in \ker\varphi$, on a $hk = 1$, donc $h = k^{-1} \in H \cap K = Z$, d'où $(h,k) = (h,h^{-1}) \in X$. Ainsi, $\ker\varphi = X$ et donc, par factorisation canonique, on obtient

$$H \circ_\theta K \stackrel{\text{def}}{=} (H \times K)\,/_X = (H \times K)\,/_{\ker\varphi} \simeq \operatorname{im}\varphi = G,$$

d'où le résultat. □

Corollaire 3. *Si $G = H \circ_\theta K$, alors H et K sont distingués dans G et $H \cap K$ est un sous-groupe du centre de G.*

Corollaire 4. *Si H et K sont des sous-groupes de G et si $G = H \circ K$, alors*

$$|G| = \frac{|H||K|}{|H \cap K|}.$$

Exemple 4. • Prenons

$$H := \mathcal{D}_8 = \langle \omega, \sigma \mid \omega^4, \sigma^2, (\sigma\omega)^2 \rangle$$

et

$$K := \mathcal{Q}_8 := \langle x, y \mid x^4, x^2y^{-2}, yxy^{-1}x \rangle,$$

Posons $z := x^2 \in \mathcal{Q}_8$,

$$Z := Z(\mathcal{D}_8) = \{1, \omega^2\} \text{ et } W := Z(\mathcal{Q}_8) = \{1, z\},$$

ainsi que

$$\begin{array}{rccc} \theta & : & Z & \to & W \\ & & \omega^2 & \mapsto & z \end{array}$$

On a alors

$$|\mathcal{D}_8 \circ_\theta \mathcal{Q}_8| = \frac{8 \times 8}{2} = 32.$$

Dans $\mathcal{D}_8 \circ \mathcal{Q}_8$,

- $*$ $(1, 1)$ est d'ordre 1,
- $*$ les carrés de $(\omega^2, 1)$ et $(1, z)$ sont dans X,
- $*$ les carrés de (ω, h), avec h d'ordre 4, sont dans X,
- $*$ les carrés de (ω^3, h), avec h d'ordre 4, sont dans X,
- $*$ les carrés de $(g, 1)$, avec g d'ordre 2, sont dans X,
- $*$ les carrés de (g, z), avec g d'ordre 2, sont dans X,
- $*$ les éléments restant sont d'ordre 4 et aucun de leurs carrés n'est dans X.

Ainsi, dans $\mathcal{D}_8 \circ \mathcal{Q}_8$, il y a 24 éléments du produit direct ; chacun ayant un ordre divisant 2 dans $\mathcal{D}_8 \circ \mathcal{Q}_8$. Il s'ensuit que ces 24 éléments forment 12 classes modulo X (y compris X lui-même). On en déduit que le produit central possède l'identité, 11 éléments d'ordre 2 et 20 éléments d'ordre 4.

- De même, on peut former le produit central $\mathcal{D}_8 \circ \mathcal{D}_8$, avec $Z = W = Z(\mathcal{D}_8) = \{1, \omega^2\}$. Ce produit a 19 éléments d'ordre 2 ; ce qui implique que

$$\mathcal{D}_8 \circ \mathcal{D}_8 \neq \mathcal{D}_8 \circ \mathcal{Q}_8.$$

1.3.2 Produit en couronne et sous-groupes de Sylow de $\mathfrak{S}_n$

Nous allons à présent construire un autre produit de groupes, basé sur le produit semi-direct. Ce nouveau produit nous sera utile pour construire et étudier les groupes imprimitifs $G(m, p, n)$. Le produit en couronne nous permettra de plus de décrire les sous-groupes de Sylow du groupe symétrique $\mathfrak{S}_n$, avec $n \geq 1$ quelconque, problème difficile à priori. Le lecteur souhaitant obtenir plus de détails sur cette construction pourra se référer à [11], Chapter 19 et [17], Chapter 7, §4.

Définition 11. • Soient G, H deux groupes et Ω un H-ensemble fini. Posons

$$K := \prod_{\omega\in\Omega} G_\omega, \quad \text{avec} \quad G_\omega \simeq G, \ \forall \omega \in \Omega.$$

Alors, H agit par automorphisme sur K via

$$h \cdot (g_\omega)_{\omega\in\Omega} := (g_{h\cdot\omega})_{\omega\in\Omega}.$$

Cette action donne un morphisme $\varphi : H \to \mathrm{Aut}\,(K)$.
On définit le produit en couronne de G par H selon Ω par

$$G \wr_\Omega H = G \wr H := K \rtimes_\varphi H.$$

Le sous-groupe $K \trianglelefteq (G \wr H)$ est appelé la base de $G \wr H$.

• Si $\Omega = H$, avec action naturelle, on parle alors de produit en couronne régulier et on note $G \wr_r H$.

Remarque 7. Si G et H sont finis, alors on a immédiatement

$$|G \wr_\Omega H| = |G|^{|\Omega|}|H| \quad \text{et} \quad |G \wr_r H| = |G|^{|H|}|H|.$$

Exemple 5. On a

$$\left(\mathbb{Z}/2\mathbb{Z}\right) \wr_r \left(\mathbb{Z}/2\mathbb{Z}\right) \simeq \mathcal{D}_4.$$

En effet, posons $G := \langle x\rangle \simeq \mathbb{Z}/2\mathbb{Z} \simeq \langle h\rangle =: H$ et remarquons que $|G \wr_r G| = 2^2 \times 2 = 8$. Soit $K := G \times G = \{(1,1),(1,x),(x,1),(x,x)\}$. Dans ce contexte, on a $\varphi(1) = id_K$ et

$$\varphi(h)(g_1, g_2) = (g_2, g_1).$$

Soient $\alpha := ((1,x),h)$ et $\beta := ((1,1),h)$. On a

$$\alpha^2 = ((1,x)\cdot\varphi(h)(1,x), h^2) = ((1,x)\cdot(x,1),1) = ((x,x),1),$$

donc α est d'ordre 4. De même, β est d'ordre 2 et on a

$$\beta\alpha\beta^{-1} = \beta\alpha\beta = ((1,1),h)((1,x),h)((1,1),h) = ((1,1),h)((1,x)\varphi(h)(1,1),h^2)$$

$$= ((1,1),h)((1,x),1) = ((1,1)\varphi(h)(1,x),h) = ((x,1),h) = ((1,x),h)^{-1} = \alpha^{-1}.$$

Ainsi, $G \wr_r G$ est de présentation

$$G \wr_r G = \left\langle \alpha, \beta \mid \alpha^4, \beta^2, (\alpha\beta)^2 \right\rangle \simeq \mathcal{D}_4.$$

Remarque 8.
1. On peut montrer (cf [17], Chapter 7, §4, p.173) que si Ω est un H-ensemble fini (resp. transitif), et si Λ est un G-ensemble (resp. transitif), alors $\Lambda \times \Omega$ est un $(G \wr H)$-ensemble (resp. transitif).
2. On peut également montrer que le produit $\wr$ est associatif, mais que $\wr_r$ ne l'est pas en général.

Nous sommes à présent en mesure de calculer les sous-groupes de Sylow de $\mathfrak{S}_n$. Par souci de lisibilité, pour un entier naturel non nul n, on note $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. Commençons par un lemme :

Lemme 5. *(Kaloujnine, 1948)*
Soit p un nombre premier. Définissons par récurrence

$$\begin{cases} Q_1 := \mathbb{Z}_p \\ Q_2 := \mathbb{Z}_p \wr_r \mathbb{Z}_p \\ Q_{n+1} := Q_n \wr_r \mathbb{Z}_p, \ \forall n \geq 1 \end{cases}$$

Alors, pour tout $k \in \mathbb{N}^*$, Q_k est un p-sous-groupe de Sylow de $\mathfrak{S}_{p^k}$.

Démonstration. (Voir [11], p.168-170)
On procède par récurrence sur k.
Si $k = 1$, la seule puissance de p divisant $p!$ est p, puisque p est premier. Si Q est un p-Sylow de $\mathfrak{S}_p$, alors $Q \simeq \mathbb{Z}_p$.
Supposons donc le résultat vrai au rang k. Pour $n \geq 1$, quelle est la plus grande puissance de p divisant $(p^n)!$? Le nombre d'entiers de $\{1, \ldots, p^n\}$ divisibles par p est $p^n - \varphi(p^n) = p^n - p^{n-1}(p-1) = p^{n-1}$. Parmi eux, exactement p^{n-2} sont divisibles par p^2, etc... Ainsi, la plus grande puissance de p divisant $(p^n)!$ est $p^{\mu(n)}$ où

$$\mu(n) := p^{n-1} + p^{n-2} + \cdots + p + 1.$$

Or, on a $|\mathbb{Z}_p \wr_r \mathbb{Z}_p| = p^p p = p^{p+1}$, $|(\mathbb{Z}_p \wr_r \mathbb{Z}_p) \wr_r \mathbb{Z}_p| = |\mathbb{Z}_p \wr_r \mathbb{Z}_p|^p p = p^{p^2+p+1}$ et par récurrence immédiate, on voit qu'alors $|Q_n| = p^{\mu(n)}$. Ainsi, le produit en couronne régulier de $(k+1)$ copies de $\mathbb{Z}_p$ est d'ordre $p^{p\mu(k)+1}$, tout comme un p-Sylow de $\mathfrak{S}_{p^{k+1}}$ puisque $p\mu(k)+1 = \mu(k+1)$. Il reste à montrer que $Q_{k+1} \leq \mathfrak{S}_{p^{k+1}}$. Dans $\mathfrak{S}_{p^{k+1}}$, définissons N comme le produit direct de p copies de $\mathfrak{S}_{p^k}$, le premier facteur étant vu comme groupe symétrique sur $\{1, \ldots, p^k\}$, le second sur $\{1 + p^k, \ldots, 2p^k\}$, etc... Ces copies de $\mathfrak{S}_{p^k}$ commutent deux à deux, car elles agissent sur des ensembles disjoints. Soit $h \in \mathfrak{S}_{p^{k+1}}$ constitué de p^k cycles d'ordre p, ceux-ci étant de la forme

$$(i, i + p^k, i + 2p^k, \ldots, i + (p-1)p^k), \ 1 \leq i \leq p^k.$$

Par hypothèse de récurrence, Q_r est un p-Sylow de $\mathfrak{S}_{p^k}$. Il est alors clair que le produit semi-direct d'un p-Sylow de N par $H := \langle h \rangle$ est isomorphe à Q_{k+1}, d'où le résultat. □

Corollaire 5. *(Findlay, 1904)*
Si p est un nombre premier et si $n \in \mathbb{N}^*$, on écrit n en base p :

$$n = a_0 + a_1 p + \cdots + a_k p^k, \ 0 \leq a_i \leq p - 1.$$

Alors, chaque p-sous-groupe de Sylow S de $\mathfrak{S}_n$ est un produit direct

$$S = (Q_1)^{a_1} \times \cdots \times (Q_k)^{a_k}.$$

Démonstration. Cherchons la plus grande puissance de p divisant $n!$. Le nombre d'entiers de $\{1,\dots,n\}$ divisibles par p est $\lfloor n/p \rfloor$, comme on le voit directement par division euclidienne. Parmis ceux-ci, $\lfloor n/p^2 \rfloor$ sont divisibles par p^2, etc... Il s'ensuit que la plus grande puissance de p divisant $n!$ est p^t, où

$$t := \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots,$$

et en utilisant l'écriture de n en base p, on obtient

$$t = (a_1 + a_2 p + \cdots + a_k p^{k-1}) + (a_2 + a_3 p + \cdots + a_k p^{k-2}) + \cdots$$

$$= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots = \sum_{j=1}^{k} a_k \mu(k),$$

de telle sorte que p^t est l'ordre de

$$(Q_1)^{a_1} \times \cdots (Q_k)^{a_k} =: S,$$

et ce d'après le Lemme précédent. Il reste à montrer que $\mathfrak{S}_n$ possède un sous-groupe isomorphe à S. Pour ceci, on partitionne l'ensemble à n éléments en sous-ensembles disjoints avec a_0 singletons, a_1 ensembles de taille p, a_2 de taille p^2,...,a_k de taille p^k et on applique le Lemme 5 à chacun des groupes symétriques sur ces sous-ensembles. □

1.3.3 Rappels sur les représentations linéaires des groupes finis

Nous supposons le lecteur familier avec le vocabulaire des représentations. Nous rappelons seulement le théorème de Maschke, le lemme de Schur et un corollaire qui nous sera utile. Pour plus d'informations sur les représentations, on pourra consulter [14] ainsi que [20] ou encore les excellents [18] et [22].

On se donne un groupe fini G.

Théorème 1. *(Maschke)*
Si G est un groupe fini et si V est une représentation linéaire (complexe) de G, alors toute sous-représentation de V en est facteur direct.

Démonstration. Soient en effet U une telle sous-représentation ainsi que $(-,-)$ une forme hermitienne définie positive G-invariante (qui existe par le Lemme 1). Alors, $U^\perp$ est G-stable et comme $V = U \oplus U^\perp$, le résultat est démontré. □

Corollaire 6. *Toute représentation de G est totalement réductible.*

Théorème 2. *(Lemme de Schur)*
Si V, W sont des représentations irréductibles de G, alors tout opérateur d'entrelacement non nul $V \to W$ est un isomorphisme. De plus, on a

$$\mathrm{End}_G(V) \simeq \mathbb{C}.$$

Démonstration. Soit $0 \neq f : V \to W$. Alors, $\ker f \leq V$ et $\operatorname{im} f \leq W$, donc $\ker f = 0$ et $\operatorname{im} f = W$, ce qui démontre la première assertion. Ensuite, si $f \in \operatorname{End}_G(V)$, avec $f \neq 0$, soit λ une valeur propre de f. Alors, $f - \lambda id_V$ n'est pas inversible, donc $f = \lambda id_V$ et l'application

$$\begin{array}{ccc} \operatorname{End}_G(V) & \to & \mathbb{C} \\ f & \mapsto & \lambda \end{array}$$

est un isomorphisme. □

Corollaire 7. *Si V est une représentation irréductible de G et si $(-,-)$, $[-,-]$ sont deux forme hermitiennes définies positives G-invariantes sur V, alors*

$$\exists \lambda \in \mathbb{R}_+^* \ ; \ (u,v) = \lambda [u,v], \ \forall u, v \in V.$$

Démonstration. Soient

$$\begin{array}{rccc} f & : & V & \to & V^* \\ & & v & \mapsto & (w \mapsto (w,v)) \end{array}$$

ainsi que

$$\begin{array}{rccc} g & : & V & \to & V^* \\ & & v & \mapsto & (w \mapsto [w,v]) \end{array}$$

Alors f et g sont des bijections et $g^{-1}f \in \operatorname{End}_G(V)$. Par le Lemme de Schur, on a $g^{-1}f = \lambda id_V$ pour $\lambda \in \mathbb{C}^*$ et donc $(u,v) = \lambda[u,v]$ pour tous $u, v \in V$. Prenant $u = v$, on voit alors que $\lambda > 0$. □

1.4 Groupes de réflexions unitaires irréductibles

Nous introduisons ici l'analogue pour les groupes de réflexions des G-modules simples pour les représentations. Ces "briques élémentaires" permettent de restreindre notre étude et notre classification aux groupes dits "irréductibles", qui seront facteurs directs de tout groupe de réflexions unitaires, comme nous allons le voir.

Définition 12. Si G est un sous-groupe de réflexions unitaire de $U(V)$, le G-module V est appelé la représentation naturelle (ou de réflexion) de G. Si la représentation de réflexion est irréductible, on dit que G est un groupe de réflexions unitaires irréductible.

Théorème 3. *Soit G un groupe fini engendré par des réflexions sur V, laissant invariante la forme hermitienne définie positive $(-,-)$. Alors, V admet une décomposition en somme directe orthogonale*

$$V = V_1 \perp \cdots \perp V_m,$$

telle que, pour tout $1 \leq i \leq m$, la restriction G_i de G à V_i soit irréductible (sur V_i) et

$$G \simeq G_1 \times \cdots \times G_m.$$

Démonstration. La preuve du Théorème de Maschke montre que V est somme directe orthogonale de sous-G-modules irréductibles $V_1, \ldots, V_m$. Par le Corollaire 2, si a est racine d'une réflexion de G, alors $a \in V_i$ pour un certain i. Soit $G_i < G$ engendré par les réflexions de G dont les racines appartiennent à V_i. Alors, pour $i \neq j$, G_i fixe tout vecteur de V_j et par la Proposition 3, les éléments de G_i commutent à ceux de G_j. Il s'ensuit que G est produit direct des (G_i) et que G_i peut être identifié à la restriction de G à V_i. Ensuite, si $W \nsubseteq \operatorname{Fix} r$ pour une réflexion r de G, alors une racine a de r est dans W. Mais il existe i tel que $a \in V_i$ et donc $W \cap V_i \neq 0$, d'où $W = V_i$ par irréductibilité. □

Remarque 9. Le Théorème et sa preuve montrent que

$$V = V^G \perp V_1 \perp \cdots \perp V_k,$$

où les V_i sont des G-modules irréductibles non triviaux.

Définition 13. Le support d'un groupe de réflexions unitaires $G \leq U(V)$ est le sous-espace M de V engendré par les racines des réflexions de G. De façon équivalente, $M := (V^G)^\perp$. Si un facteur V_i du Théorème 3 est tel que $V_i \nsubseteq M$, alors le groupe G_i est trivial.

Définition 14.

- Le rang d'un groupe de réflexions unitaire G est la dimension de son support.
- Un sous-groupe de G est un sous-groupe de réflexions s'il est engendré par des réflexions.
- Si G est engendré par les réflexions $r_1, \ldots, r_k$ avec racines $a_1, \ldots, a_k$, on définit un graphe $\Gamma := (R, E)$, que nous nommerons graphe de réflexion de G, dont les sommets sont $R := \{a_1, \ldots, a_k\}$ et on joint les sommets a_i et a_j si et seulement si $(a_i \neq a_j \text{ et } (a_i, a_j) \neq 0)$. Notons qu'avec cette définition, on peut avoir $|R| < k$.

Proposition 6. *Si G est un sous-groupe de réflexions unitaire de $U(V)$ avec V pour support et Γ pour graphe, alors la représentation V est irréductible si et seulement si Γ est connexe.*

Démonstration. Supposons G réductible. Le Théorème 3 assure que $V = V_1 \perp \cdots \perp V_k$, avec $k > 1$ et les V_i non triviaux. Alors, chaque sommet de Γ est dans un V_i. De plus, comme $V^G = 0$, chaque V_i contient au moins un sommet de $\Gamma = (R, E)$. Si $a_1 \in V_1 \cap R$ et $a_2 \in V_1 \cap R$ et si a_1 était lié par une chaîne à a_2, alors tous les sommets de la chaîne seraient dans V_1, en particulier $a_2 \in V_1 \cap V_2$, donc $a_2 = 0$, ce qui serait absurde. Γ n'est donc pas connexe.
Réciproquement, supposons Γ non connexe. Soient V_1 le sous-espace engendré par les sommets d'une composante connexe de Γ et V_2 le sous-espace engendré par les autres sommets de Γ. Alors, V_1 et V_2 sont orthogonaux et fixés par les réflexions à racines dans Γ. Mais ces réflexions engendrent G, donc V_1 et V_2 dont G-invariants et ceci montre que G est réductible. □

Corollaire 8. *Soient G un groupe de réflexions unitaire et H un sous-groupe de réflexions de G agissant de façon irréductible sur son support W. Si $r \in G$ est une réflexion de racine $a \notin W \cup W^\perp$, alors $\langle H, r \rangle$ agit de façon irréductible sur $W \oplus \mathbb{C}a$.*

Démonstration. Comme $\langle H, r\rangle$ est engendré par les réflexions à racines dans $W \oplus \mathbb{C}a$, ce premier préserve le sous-espace $W \oplus \mathbb{C}a$. Si $\Gamma = (R, E)$ est le graphe de réflexion de H, alors Γ est connexe et le graphe de sommets $R \cup \{a\}$ reste connexe puisque $a \notin W \cup W^{\perp}$. □

Corollaire 9. *Supposons que G soit un groupe de réflexions unitaire de rang n agissant de façon irréductible sur son support. Il existe alors une suite de sous-groupes*

$$1 = G_0 < G_1 < G_2 < \ldots < G_n < G_l = G,$$

avec $n \leq l$, telle que pour tout $1 \leq i \leq l$, il existe une réflexion r_i telle que $G_i = \langle G_{i-1}, r_i\rangle$ et pour tout $1 \leq i \leq n$, G_i est engendré par i réflexions, est de rang i et agit de façon irréductible sur son support.

Démonstration. On construit la suite $(G_i)_i$ par récurrence, avec $G_0 := 1$. Supposons que G_i soit un sous-groupe de réflexions de rang i, agissant de façon irréductible sur son support W. Si $i < n$, puisque G est de rang n, il existe des réflexions de G dont les racines ne sont pas dans W. Comme G est irréductible, ces racines ne sont pas toutes dans $W^{\perp}$ et il existe donc une réflexion $r \in G$ de racine $a \notin W \cup W^{\perp}$. Par le Corollaire 8, $G_{i+1} := \langle G_i, r\rangle$ agit de façon irréductible sur $W \oplus \mathbb{C}a$, son support. Par construction, G_n est de rang n et on peut ajouter successivement des réflexions engendrant G pour obtenir les groupes $G_{n+1}, \ldots, G_{l-1}, G_l = G$. □

Remarque 10. En examinant de près la preuve précédente, on remarque que l'on a montré de plus que tout groupe de réflexions unitaire irréductible de rang n contient un sous-groupe de réflexions unitaire irréductible de rang n avec n générateurs.

Théorème 4. *Si G_1 et G_2 sont des sous-groupes de réflexions unitaires irréductibles (finis) de $U(V)$, alors G_1 et G_2 sont conjugués dans $GL(V)$ si et seulement s'ils sont conjugués dans $U(V)$.*

Démonstration. On peut représenter les éléments de G_1 et G_2 par des matrices unitaires dans une base orthonormée. Supposons que pour M inversible, on ait $g' := MgM^{-1} \in G_2$, pour tout $g \in G_1$. En prenant le conjugué de la transposée de cette équation, on obtient

$$Mg^{-1}M^{-1} = (g')^{-1} = {}^t\overline{g'} = (M^{-1})^{*t}\overline{g^{-1}}M^{*} = (M^{-1})^{*}g^{-1}M^{*}$$

et ainsi, on a

$$g_1 M^{*}M = M^{*}Mg_1, \ \forall g_1 \in G_1.$$

Le Lemme de Schur (Théorème 2) assure alors l'existence de $\lambda \in \mathbb{C}$ tel que $M^{*}M = \lambda I$. Mais comme $M^{*}M$ est hermitienne, $\lambda \in \mathbb{R}$. De plus, on a

$$\lambda = (M^{*}M)_{1,1} = \sum_{k=1}^{\dim V} (M^{*})_{1,k}M_{k,1} = \sum_{k=1}^{\dim V} \overline{M_{k,1}}M_{k,1} = \sum_{k=1}^{\dim V} |M_{k,1}|^2 > 0,$$

donc $\lambda > 0$ et il existe $z \in \mathbb{C}^{\times}$ tel que $\lambda = z\overline{z}$. Maintenant, $z^{-1}M$ est une matrice unitaire qui envoie G_1 sur G_2 par conjugaison. La réciproque est évidente. □

Deuxième partie
Groupes $G(m, p, n)$

Nous allons distinguer deux classes particulières de groupes de réflexions, les groupes primitifs et les imprimitifs ; cette disjonction provenant de la structure de la représentation de réflexion des groupes considérés. Nous construirons ensuite les groupes de réflexions $G(m, p, n)$, de rang $n \geq 1$, avec $m, p \geq 1$ et p divisant m. Ces groupes se révèleront être (sous quelques hypothèses techniques) des groupes irréductibles et imprimitifs. En fait, le résultat principal de cette partie, que nous démontrerons plus loin, stipule que tout groupe de réflexions unitaires irréductible imprimitif de rang n est conjugué à un certain $G(m, p, n)$.

2.1 Primitivité et imprimitivité

On fixe un sous-groupe de réflexions G de $U(V)$.

Définition 15. Le G-module V est dit imprimitif s'il existe un entier $m > 1$ et une décomposition

$$V = V_1 \oplus \cdots \oplus V_m,$$

en sous-espaces vectoriels non triviaux de V tels que l'action de G sur V induise une action par permutation de G sur l'ensemble $\{V_1, \ldots, V_m\}$. L'ensemble $\{V_1, \ldots, V_m\}$ est alors appelé système d'imptimitivité de V. Si aucune décomposition de ce type n'est possible, on dit que V est primitif. Enfin, on dit que G est imprimitif (resp. primitif) si la représentation de réflexion de G est imprimitive (resp. primitive).

Remarque 11.
- Si V est primitif, alors il est irréductible. En effet, si $0 \neq U \leq V$ est un sous-G-module, alors $\{U, U^\perp\}$ est un système d'imprimitivité par le Théorème de Maschke.
- Si $\{V_1, \ldots, V_m\}$ est un système d'imprimitivité de V et si G est irréductible, alors les V_i sont de dimension 1. En effet, si $\dim V_i > 1$ pour un $1 \leq i \leq m$, il existe une réflexion $s \in G$ telle que $sV_i = V_j \neq V_i$, par irréductibilité de G. Mais $V_i \cap \mathrm{Fix}\,(s) \neq 0$ et si $x \in V_i \cap \mathrm{Fix}\,(s) \setminus \{0\}$, alors $x = sx \in V_j$, donc $x \in V_i \cap V_j \neq 0$, ce qui est absurde. (cf [6], §2, p.385-386).
- Si V est irréductible et imprimitif, alors G agit transitivement sur tout système d'imprimitivité. Pour le voir, choisissons un tel système $\{V_1, \ldots, V_m\}$ et soit $1 \leq j \leq m$. Alors, il existe $g_0 \in G$ tel que $g_0 V_1 = V_j$. En effet, si ce n'était pas le cas, on aurait

$$\left(\sum_{g \in G} gV_1 \right) \cap V_j = 0,$$

puisqu'en écrivant $V_1 = \mathrm{Vect}(u)$, $V_j = \mathrm{Vect}(v)$ et $x = \alpha_1 g_1 u + \cdots \alpha_k g_k u = \beta v$ où $k = |G|$, alors $x \in \sum_{1 \leq w \leq k} V_{i_w}$ avec $V_{i_w} = g_w V_1 \neq V_j$ et donc $x \in V_j \cap \sum_{i \neq j} V_i = 0$ et

donc $x = 0$. Ainsi, on a

$$0 \neq V_1 \subseteq \sum_{g \in G} gV_1 \neq V,$$

et comme $\sum_g gV_1$ est G-stable, ceci contredit l'irréductibilité de G.

- On peut montrer de plus (voir [15], Chapter 2, §1) que si G agit de façon transitive sur $\{V_1, \ldots, V_m\}$ et si $H := \mathrm{Stab}_G(V_1)$, alors V_1 est un H-module et $V \simeq \mathrm{ind}_H^G(V_1)$.

Définition 16. Si I est un G-module simple, la composante isotypique V_I de V de type d'isomorphie λ_I est la somme (directe) de tous les sous-G-modules simples de V isomorphes à I.

Rappelons que tout sous-G-module simple de V_I est isomorphe à I et que V est somme directe de ses composantes isotypiques distinctes.

Théorème 5. *Si G est un sous-groupe primitif fini de $GL(V)$ et si $A \trianglelefteq G$ est abélien, alors A est cyclique et central dans G.*

Démonstration. Comme A est abélien, ses éléments ont un vecteur propre commun, disons $w \in V$. Pour tout $a \in A$, on peut écrire $aw = \chi(a)w,\ \chi(a) \in \mathbb{C}^\times$. Alors, $\chi : A \to \mathbb{C}^\times$ est un morphisme (en fait, un caractère de A) et la composante isotypique de V de type χ est

$$V_\chi = \{v \in V\ ;\ av = \chi(a)v,\ \forall a \in A\}.$$

Pour cela, il suffit d'écrire

$$V_\chi =: \bigoplus_{1 \leq i \leq k} V_i,$$

où $V_i \simeq \mathbb{C}$ en tant que A-module. Alors

$$x \in V_\chi \ \Rightarrow\ x = v_1 + \cdots + v_k,\ v_i \in V_i \ \Rightarrow\ ax = av_1 + \cdots + av_k = \chi(a)v_1 + \cdots + \chi(a)v_k = \chi(a)x.$$

Réciproquement, si $ax = \chi(a)x$, alors $\mathrm{Vect}(x) \simeq \mathbb{C}$ en tant que A-module et alors $x \in \bigoplus_i V_i = V_\chi$.
Si $g \in G$, comme A est distingué, gV_χ est la composante isotypique de type $g\chi$, où $(g\chi)(a) := \chi(g^{-1}ag)$ car on a

$$x \in gV_\chi \ \Leftrightarrow\ g^{-1}x \in V_\chi \ \Leftrightarrow\ \forall \widetilde{a} \in A,\ \widetilde{a}g^{-1}x = \chi(\widetilde{a})g^{-1}x \ \Leftrightarrow\ \forall \widetilde{a} \in A,\ g\widetilde{a}g^{-1}x = \chi(\widetilde{a})x$$

$$\Leftrightarrow\ \forall a \in A,\ ax = \chi(g^{-1}ag)x \ \Leftrightarrow\ \forall a \in A,\ ax = (g\chi)(a)x \ \Leftrightarrow\ x \in V_{g\chi}.$$

Mais, on a

$$V = \bigoplus_{\rho \in \mathrm{Hom}\,(A, \mathbb{C}^\times)} V_\rho$$

et G permute les V_ρ. Donc, par primitivité de G, on a $V = V_\chi$, et A agit sur V par homothétie et donc $A < Z(G)$.
De plus, si $\chi(a) = 1$, alors $a = 1$, donc $\chi : A \to \mathbb{C}^\times$ est injectif et A, s'identifiant alors à un sous-groupe fini de $\mathbb{C}^\times$, est cyclique. □

Remarque 12. Pour les groupes de réflexions unitaires finis, on a une réciproque. Tout groupe de réflexions unitaires irréductible imprimitif possède un sous-groupe abélien distingué non central. Ceci est une conséquence de la structure des $G(m,p,n)$ et du théorème 7.

Théorème 6. *Si $G < U(V)$ est un groupe de réflexions unitaire primitif (fini), et si $N \trianglelefteq G$, alors soit V est un N-module irréductible, soit $N < Z(G)$.*

Démonstration. Supposons donc V réductible sur N. Alors, on peut choisir une décomposition

$$V = V_1 \oplus \cdots \oplus V_k,\ k > 1,$$

où les V_i sont des sous-N-modules irréductibles de V. Comme G est primitif, pour tout i, il existe une réflexion $r_i \in G$ de racine a_i telle que $r_i V_i \neq V_i$. Comme N est distingué, $r_i V_i$ est un N-module irréductible et donc $r_i V_i \cap V_i = 0$. D'autre part, si $a_i^\perp \cap V_i \neq 0$, alors $r_i V_i \cap V_i \neq 0$ et pour éviter une contradiction, on doit avoir $a_i^\perp \cap V_i = 0$. Mais comme $a_i^\perp$ est un hyperplan, on doit avoir $\dim V_i = 1$, pour tout i. Toute représentation irréductible de N est alors de degré 1, donc N est abélien et par le Théorème 5, on obtient que N est central dans G, d'où le résultat. □

2.2 Représentations monômiales, construction des groupes $G(m,p,n)$

Soit H un sous-groupe fini de $\mathbb{C}^\times$, disons $H = \mu_m$ pour un certain m, μ_m désignant le groupe des racines $m^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$. Soient également G un groupe agissant sur $\Omega := \{1,\dots,n\}$ et V un $\mathbb{C}$-espace vectoriel de dimension n, $(-,-)$ une forme hermitienne définie positive sur V, ainsi que $B := \prod_{1\leq i\leq n} H = \mu_m^n$. On suppose enfin que $(e_1,\dots,e_n)$ est une base orthonormée de V.

Pour $h = (h_1,\dots,h_n) \in B$, posons

$$\forall 1 \leq i \leq n,\ h \cdot e_i := h_i e_i.$$

Alors, on peut représenter matriciellement h par $\mathrm{diag}(h_1,\dots,h_n)$ avec $h_i\overline{h_i} = 1$ pour tout i ; et B s'identifie alors à un sous-groupe de $U(V)$. G agit aussi sur V en permutant les éléments de la base :

$$\forall 1 \leq i \leq n,\ g \cdot e_i := e_{g(i)}$$

et G s'identifie donc également à un sous-groupe de $U(V)$.

Les actions de B et de G sur V induisent une action de $B \rtimes G \overset{\text{def}}{=} \mu_m \wr G$ sur V :

$$(h,g) \cdot e_i = h_{g(i)} e_{g(i)},\ \forall 1 \leq i \leq n.$$

Les matrices de ces automorphismes sont des matrices ayant exactement un coefficient non nul sur chaque ligne et chaque colonne ; on les appelle des matrices monômiales. La représentation correspondante de $\mu_m \wr G$ est appelée représentation monômiale standard.

Ainsi, on identifie $\mu_m \wr G$ à un sous-groupe de $U(V)$ dont $\{\mathbb{C}e_1,\dots,\mathbb{C}e_n\}$ est un système d'imprimitivité.

On en arrive alors à la construction fondamentale suivante :

Définition 17. Avec $B := \mu_m^n$ et p un diviseur de $m \geq 1$, posons

$$A(m,p,n) := \{\theta = (\theta_1, \ldots, \theta_n) \in B \ ; \ (\theta_1 \cdots \theta_n)^{\frac{m}{p}} = 1\}.$$

Alors, $A(m,p,n)$ est clairement un sous-groupe de B, stable sous l'action naturelle de $\mathfrak{S}_n$ sur B. On définit le groupe $G(m,p,n)$ par

$$G(m,p,n) := A(m,p,n) \rtimes \mathfrak{S}_n.$$

On dispose alors de la proposition élémentaire suivante :

Proposition 7. *1. $A(m,p,n)$ est un sous-groupe d'indice p dans B.*

2. $G(m,p,n)$ est un sous-groupe distingué de $\mu_m \wr \mathfrak{S}_n$.

3. $G(m,p,n)$ est d'ordre $\frac{n!(m^n)}{p}$ et d'indice p dans $\mu_m \wr \mathfrak{S}_n$.

Démonstration. 1. Pour obtenir $\theta \in A(m,p,n)$, on a m^{n-1} choix pour $\theta_1, \ldots, \theta_{n-1}$ et θ_n doit vérifier $\theta^{m/p} = (\theta_1 \cdots \theta_{n-1})^{-m/p}$, ce qui laisse m/p choix pour θ_n, d'où

$$|A(m,p,n)| = \frac{m}{p} m^{n-1} = \frac{m^n}{p} = \frac{|B|}{p}.$$

2. Il découle d'un calcul direct et du fait que B est abélien, que

$$G(m,p,n) = A(m,p,n) \rtimes \mathfrak{S}_n \trianglelefteq B \rtimes \mathfrak{S}_n = \mu_m \wr \mathfrak{S}_n.$$

3. Finalement, on peut calculer l'ordre de $G(m,p,n)$:

$$|G(m,p,n)| = |A(m,p,n)| \times |\mathfrak{S}_n| = \frac{(m^n)n!}{p},$$

et on en déduit que

$$[\mu_m \wr \mathfrak{S}_n : G(m,p,n)] = \frac{|\mu_m \wr \mathfrak{S}_n|}{|G(m,p,n)|} = \frac{|B \rtimes \mathfrak{S}_n|}{|G(m,p,n)|} = \frac{m^n n!}{\frac{m^n n!}{p}} = p.$$

□

On peut, accessoirement, déterminer le centre de $G(m,p,n)$:

Proposition 8. *Soient $m, n \in \mathbb{N}^*$ et $p|m$. Alors, on a*

$$Z(G(m,p,n)) \simeq \{\theta \in \mu_m \ ; \ \theta^{\frac{mn}{p}} = 1\}.$$

En particulier, $Z(G(m,p,n))$ est cyclique et

$$Z(G(m,p,n)) \simeq \mathbb{Z}/_{d\mathbb{Z}} \quad \textit{avec} \quad d = \frac{mn}{p \vee n}.$$

Démonstration. Il s'agit d'un fait général sur le centre d'un produit semi-direct. Comme $G(m,p,n) = A(m,p,n) \rtimes \mathfrak{S}_n$, si $(\widetilde{\theta},\sigma) \in Z(G(m,p,n))$, alors $\sigma \in Z(\mathfrak{S}_n)$ et si $n \neq 2$, il vient $\sigma = 1$, par la proposition 1 de l'Annexe. D'autre part, $\widetilde{\theta}$ doit être invariant sous l'action de tout élément de $\mathfrak{S}_n$, donc $\widetilde{\theta} = (\theta_1, \ldots, \theta_n)$ avec $\theta_1 = \cdots = \theta_n$ et comme $\widetilde{\theta} \in A(m,p,n)$, on doit avoir $\theta_1^{\frac{mn}{p}} = 1$, ce qui donne bien le premier isomorphisme annoncé. De plus, comme le membre de droite de la première égalité est un sous-groupe de μ_m, il est cyclique et on voit que son ordre est bien égal à $\frac{mn}{\mathrm{ppcm}(p,n)}$. □

Enfin, signalons qu'afin de pouvoir manipuler ces nombreux groupes, dont l'ordre augmente manifestement très rapidement avec m et n, nous mettons à disposition du lecteur un algorithme en Annexe, permettant de construire les $G(m,p,n)$ grâce au logiciel `GAP`.

2.3 Propriétés des groupes $G(m,p,n)$

Afin de montrer que $G(m,p,n)$ est engendré par des réflexions, examinons comment une réflexion peut agir non trivialement sur un système d'imprimitivité et ensuite, appliquons ceci aux réflexions de $G(m,p,n)$. Mais commençons par deux lemmes :

Lemme 6. *Soient V un $\mathbb{C}$-espace vectoriel de dimension n, muni d'une forme hermitienne définie positive $(-,-)$ et $V_1, \ldots, V_k$ des droites vectorielles de V engendrées par une famille libre de vecteurs $(e_1, \ldots, e_k)$. Si r est une réflexion qui permute entre eux les V_i et s'il existe $i \neq j$ tels que $rV_i = V_j$, alors r est d'ordre 2 et $V_h \subseteq \mathrm{Fix}\,(r)$, pour tout $h \neq i,j$.*

Démonstration. Choisissons $\theta \in \mathbb{C}$ tel que $re_i = \theta e_j$. Si a est une racine courte de r, alors $\theta e_j = re_i = e_i - (1-\alpha)(e_i,a)a$. De plus, le même argument montre que r ne peut interchanger plus d'une paire de V_h et donc $V_h \subset \mathrm{Fix}\, r$ si $h \notin \{i,j\}$. En particulier, r agit comme la transposition (V_i, V_j) sur $\{V_1, \ldots, V_k\}$ et il existe $\theta' \in \mathbb{C}$ tel que $re_j = \theta' e_i$. Ainsi, $\theta\theta'$ est valeur propre de r^2, de multiplicité au moins 2, donc l'espace propre associé intersecte non trivialement l'hyperplan $\mathrm{Fix}\,(r^2)$ et donc $\theta\theta' = 1$. Or, pour tout $x \in V$, on a $r^2 x = x - (1-\alpha^2)(x,a)a$, d'où $\theta\theta' e_i = r^2 e_i = e_i - (1-\alpha^2)(e_i,a)a$, donc $0 = (1-\theta\theta')e_i = (1-\alpha^2)(e_i,a)a$ et $(e_i,a) \neq 0$ montre que $\alpha^2 = 1$ et donc $r^2 = 1$. □

On pense toujours à $G(m,p,n)$ comme défini à partir de la base orthonormée $(e_1, \ldots, e_n)$ fixée lors de la section précédente.

Lemme 7. *Un élément $r \in G(m,p,n)$ est une réflexion si et seulement si r vérifie l'une des propriétés suivantes :*

1. *Il existe i et une racine $(m/p)^{ième}$ de l'unité $\theta \neq 1$ tels que $r = r_{e_i,\theta}$.*
2. *Il existe $i \neq j$ et une racine $m^{ième}$ de l'unité θ tels que $r = r_{e_i - \theta e_j, -1}$.*

Dans le second cas, r est d'ordre 2, $re_i = \theta e_j$, $re_j = \theta^{-1} e_i$ et $re_k = e_k$ pour $k \neq i,j$.

Démonstration. Si $r = r_{e_i,\theta}$, soit $h \in B$ avec tout terme égal à 1 sauf le $i^{\text{ème}}$ qui vaut θ. Alors, $h \in A(m,p,n)$ et $r_{e_i,\theta} = (h,1)$. Si $r = r_{e_i-\theta e_j,-1}$, soit $h \in B$ avec tout terme égal à 1 sauf le $i^{\text{ème}}$ qui vaut θ^{-1}, le $j^{\text{ème}}$ qui vaut θ et soit $\sigma := (i,j) \in \mathfrak{S}_n$. Alors, $h \in A(m,p,n)$ et $r_{e_i-\theta e_j,-1} = (h,\sigma)$. Donc toute réflexion de la forme 1. ou 2. est dans $G(m,p,n)$.

Supposons donc que $r \in G(m,p,n)$ soit une réflexion. Si $r \in A(m,p,n)$, alors on est dans le premier cas. Sinon, il existe $i \neq j$ tels que $re_i = \theta e_j$, pour $\theta \in \mu_m$. Le Lemme 6 implique alors que r soit d'ordre 2 et il est clair que $e_i - \theta e_j \in [V,r]$. On est donc dans le second cas. □

Remarque 13. On peut montrer (voir [15], Proposition 2.9) que les groupes $G(m,m,n)$ contiennent $m\binom{n}{2}$ réflexions et que toutes sont d'ordre 2. Si de plus $n > 2$ ou si m est impair, les réflexions forment une seule classe de conjugaison. Enfin, si m est pair, $G(m,m,2)$ contient deux classes de conjugaison de réflexions.

Proposition 9. *Si $n > 1$, $G(m,p,n)$ est un groupe de réflexions unitaire imprimitif. De plus, si $m > 1$, alors $G(m,p,n)$ est irréductible sauf si $(m,p,n) = (2,2,2)$.*

Démonstration. Les réflexions $r_{e_i-e_j,-1} = (1,(i,j))$ engendrent $\mathfrak{S}_n$ et les $r_{e_i,\eta} \in A(m,p,n)$, pour $\eta \in \mu_{m/p}$, joints aux $r_{e_i-\theta e_j,-1} r_{e_i-e_j,-1} \in A(m,p,n)$, pour $\theta \in \mu_m$, engendrent $A(m,p,n)$. En effet, si $h \in A(m,p,n)$, on voit par calcul direct que l'on peut décomposer h en produit d'éléments de la forme $r_{e_i,\eta}$ et $r_{e_i-\theta e_j,-1} r_{e_i-e_j,-1}$. Ainsi, $G(m,p,n) = A(m,p,n) \rtimes \mathfrak{S}_n$ est bien engendré par des réflexions.

Il reste à montrer que si $G(m,p,n)$ est réductible, alors $m = 1$ ou bien $(m,p,n) = (2,2,2)$. Soit donc $0 \neq W \neq V$ un sous-espace $G(m,p,n)$-stable. En particulier, W est invariant sous l'action de chaque $r_{e_i-e_j,-1}$ et par le Corollaire 2, on a $e_i - e_j \in W \cup W^\perp$. Si, pour des i,j,k distincts, on a $e_i - e_j \in W$ et $e_j - e_k \in W^\perp$, alors $e_i - e_k \notin W \cup W^\perp$, ce qui est absurde.

On peut alors supposer que $e_i - e_j \in W^\perp$, pour tous i,j et alors $W^\perp$ contient la famille libre $\{e_1 - e_2, \ldots, e_1 - e_n\}$. Cette famille engendre $W^\perp$, qui est donc un hyperplan et $\dim W = 1$. De plus, pour tout $i \neq 1$, $(e_1 + \cdots + e_n, e_1 - e_i) = 0$, donc $0 \neq e_1 + \cdots + e_n \in W^{\perp\perp} = W$ et donc $W = \mathrm{Vect}(e_1 + \cdots + e_n)$.

Si $h \in A(m,p,n)$, alors $(h,1)$ préserve W et il existe donc $\lambda \in \mathbb{C}$ tel que

$$\lambda(e_1 + \cdots + e_n) = (h,1)(e_1 + \cdots + e_n) = (h,1)(e_1) + \cdots (h,1)(e_n)$$

$$= \theta_1 e_1 + \cdots + \theta_n e_n \;\Rightarrow\; \theta_1 = \theta_2 = \cdots = \theta_n = \lambda,$$

par liberté de $(e_1, \ldots, e_n)$.

Supposons alors $m > 1$. On a

$$\forall (\theta_1, \ldots, \theta_n) \in \mu_m^n,\ (\theta_1 \cdots \theta_n)^{\frac{m}{p}} = 1 \;\Rightarrow\; \theta_1 = \cdots = \theta_n.$$

Soit ω un générateur de μ_m. Si $p < m$, alors $\omega^p \neq 1$. Or, $(1, \ldots, 1, \omega^p) \in A(m,p,n)$, ce qui est faux. Donc $m = p$ et

$$\forall (\theta_1, \ldots, \theta_n) \in \mu_m^n,\ \theta_1 \cdots \theta_n = 1 \;\Rightarrow\; \theta_1 = \cdots = \theta_n.$$

Si $n > 2$, alors $(\omega, \omega^{-1}, 1, \ldots, 1) \in A(m,m,n)$, ce qui est encore faux, donc $n = 2$. Enfin, comme $(\omega, \omega^{-1}) \in A(m,m,2)$, on a $\omega = \omega^{-1}$, d'où $\omega^2 = 1$, donc $m = 2$ et donc $(m,p,n) = (2,2,2)$. □

Exemple 6. Si $m \leq 2$, les matrices de la représentation monômiale standard des éléments de $G(m,p,n)$ sont à coefficients réels et on peut alors considérer $G(m,p,n)$ comme un groupe de réflexions euclidien.

Nous allons voir quelques autres cas pour lesquels les groupes $G(m,p,n)$ nous sont familiers :

i) Le groupe $G(m,p,1)$ est cyclique d'ordre m/p.

ii) On a $G(1,1,n) = \mathfrak{S}_n$. On peut montrer de plus que l'action sur $\mathrm{Vect}(e_1 + \cdots + e_n)^\perp$ est primitive dès que $n \geq 5$.

iii) On a également $G(2,1,n) = A(2,1,n) \rtimes \mathfrak{S}_n \simeq \mu_2^n \rtimes \mathfrak{S}_n \simeq \mu_2 \wr \mathfrak{S}_n$.

iv) Le groupe $G(m,m,2) \simeq \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe dihédral $\mathcal{D}_{2m}$ d'ordre $2m$.

v) On a des isomorphismes remarquables

$$G(3,3,2) = A(3,3,2) \rtimes \mathfrak{S}_2 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathfrak{S}_3,$$

et

$$G(2,2,3) = A(2,2,3) \rtimes \mathfrak{S}_3 \simeq \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes \mathfrak{S}_3 \simeq K_4 \rtimes \mathfrak{S}_3 \simeq \mathfrak{S}_4.$$

vi) On a encore

$$G(4,4,2) = \langle (1,(1,2)), ((i,-i),1) \rangle = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\rangle \simeq \mathcal{D}_8$$

ainsi que

$$G(2,1,2) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq \mathcal{D}_8.$$

On peut montrer de plus que ces deux groupes sont conjugués dans $U_2(\mathbb{C})$.

vii) Le groupe $G(4,2,2)$ peut être décrit de quatre façons différentes comme produit central

$$G(4,2,2) = \mathcal{C}_4 \circ \mathcal{D},$$

où $\mathcal{C}_4 := \left\langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \right\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ et $|\mathcal{D}| = 8$. Le groupe $\mathcal{D}$ est ou bien le groupes $\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle \simeq \mathcal{Q}_8$ des quaternions ou un des trois groupes diédraux d'ordre 8, à savoir $\left\langle \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$, $G(4,4,2)$ ou bien $G(2,1,2)$.

Remarque 14. Les groupes de type *ii*), *iii*) et *iv*) font partie d'une classe très particulière de groupes, appelés groupes de Coxeter. En fait, un groupe de Coxeter est un groupe W ayant une présentation du type

$$W = \langle r_1, \ldots, r_n \mid (r_i r_j)^{m_{i,j}} = 1 \rangle,$$

où $m_{i,j} : \{1,\ldots,n\}^2 \to \mathbb{N} \cup \{\infty\}$ est symétrique et vérifie $m_{i,i} = 1$ et $m_{i,j} \geq 2$ pour $i \neq j$. Si $S := \{r_1, \ldots, r_n\}$, on dit aussi que (W,S) est un système de Coxeter. Par exemple, le groupe symétrique $\mathfrak{S}_n$ est un groupe de Coxeter, car on a une présentation

$$\mathfrak{S}_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i^2 = 1, (\sigma_i \sigma_{i+1})^3 = 1, \sigma_i \sigma_j = \sigma_j \sigma_i, \ \forall |i-j| \geq 2 \right\rangle.$$

Au sujet des groupes de Coxeter, le lecteur pourra consulter par exemple [12].

2.4 Classification des groupes de réflexions unitaires imprimitifs

Nous allons donner ici un théorème de Shephard et Todd qui classifie (à conjugaison près) tous les groupes de réflexions unitaires imprimitifs. La preuve donnée ici est tirée de [15]. On pourra aussi consulter [6] et [19]. Commençons par un résultat préliminaire :

Lemme 8. *Si G est un groupe de permutations transitif sur un ensemble fini Ω et si G est engendré par des transpositions, alors $G = \mathfrak{S}(\Omega)$.*

Démonstration. Soit $T \subset \mathfrak{S}(\Omega)$ un ensemble de transpositions et définissons le graphe $\Gamma_T := (\Omega, E)$ en décrétant que i et j sont liés si et seulement si (i, j) est une transposition de T. En particulier, si $\langle T \rangle = G$, Γ_T est connexe.

Le lemme est clairement vrai si $|\Omega| = 1$. Supposons donc $|\Omega| > 1$ et choisissons $i \in \Omega$ tel que le graphe de sommets $\Omega \setminus \{i\}$ reste connexe (il suffit de retirer une feuille d'un arbre couvrant). Par hypothèse de récurrence, les éléments de T qui ne font pas intervenir i engendrent $\mathfrak{S}(\Omega \setminus \{i\})$. Comme G est transitif sur Ω, le groupe $\mathfrak{S}(\Omega \setminus \{i\}) = \mathrm{Stab}_G(i)$ est d'indice $|\Omega|$ dans G et donc $|G| = |\Omega| \times |\Omega \setminus \{i\}|! = |\Omega|(|\Omega| - 1)! = |\Omega|! = |\mathfrak{S}(\Omega)|$, d'où $G = \mathfrak{S}(\Omega)$ et le résultat. □

Théorème 7. *(Shephard-Todd, 1954)*
Soient V un $\mathbb{C}$-espace vectoriel de dimension n, $(-,-)$ une forme hermitienne définie positive sur V et $G < U(V)$ un groupe de réflexions complexes, irréductible et imprimitif. Alors $n > 1$ et G est conjugué à un groupe $G(m, p, n)$, pour $m > 1$ et $p \geq 1$ divisant m.

Démonstration. Procédons par étapes :

- Soit $\Omega := \{V_1, \ldots, V_k\}$ un système d'imprimitivité de G. La Remarque 11 implique que $\dim V_i = 1$ pour tout i, ce qui entraîne $k = n$ et on peut alors supposer que $V_i = \mathbb{C}e_i$ avec $(e_i, e_i) = 1$.
- Si une réflexion r fixe tout V_i, r est de la forme $r_{e_i,\theta}$, avec θ une racine de l'unité (forme 1. du Lemme 7). D'autre part, si $rV_i = V_j$ pour $i \neq j$, le Lemme 6 montre que r est d'ordre 2 et agit sur Ω comme une transposition. Ainsi, le groupe G^Ω des permutations de Ω induit par l'action de G sur Ω est engendré par des transpositions et transitif par la Remarque 11. Le Lemme 8 entraîne alors que $G^\Omega = \mathfrak{S}(\Omega)$.
- Pour $2 \leq i \leq n$, choisissons des réflexions r_i de G telles que $r_i V_1 = V_i$ et choisissons la notation des e_i de telle sorte que $e_i = r_i e_1$. On a ainsi $\Sigma := \langle r_2, \ldots, r_n \rangle \simeq \langle (1,2), \ldots, (1,n) \rangle \simeq \mathfrak{S}_n$.
- Si $ge_i = \theta e_j$ pour un $\theta \in \mathbb{C}$, alors

$$1 = (e_i, e_i) = (ge_i, ge_i) = \theta\overline{\theta}(e_i, e_i) = \theta\overline{\theta},$$

  d'où $\theta\overline{\theta} = 1$. Ainsi, si $[-,-]$ est une autre forme hermitienne définie positive telle que $[e_i, e_j] = \delta_{i,j}$ pour tous i, j, alors $[-,-]$ est G-invariante. Par le Corollaire 7 au Lemme de Schur, $[-,-]$ est un multiple scalaire de $(-,-)$ et alors $(e_i, e_j) = 0$ pour tous $i \neq j$ et donc $(e_i, e_j) = \delta_{i,j}$; la base (e_i) est par conséquent $(-,-)$-orthonormée.

- Posons
$$\Theta := \{\theta \in \mathbb{C}\ ;\ \exists r \in G \ \text{ reflexion telle que } \ re_i = \theta e_j\}.$$
Si $\theta \in \Theta$, on peut supposer qu'il existe une réflexion $r \in G$ telle que $re_1 = \theta e_2$. En effet, soit $r_0 \in G$ une réflexion telle que $r_0 e_i = \theta e_j$. Comme Σ est 2-transitif sur $(e_1, \ldots, e_n)$, il existe $s \in \Sigma$ tel que $se_i = e_1$ et $se_j = e_2$ et $r := sr_0 s^{-1}$ convient. De plus, si s est une réflexion telle que $se_1 = \eta e_2$, alors $rr_2 s$ est une réflexion et $rr_2 se_1 = \eta rr_2 e_2 = \eta re_1 = \theta\eta e_2$, donc $\theta\eta \in \Theta$ et Θ est un sous-groupe fini de $\mathbb{C}^\times$. Θ est par conséquent cyclique et il existe $m > 0$ tel que $\Theta = \mu_m$.
- Si $r \in G$ est une réflexion telle que $re_1 = \theta e_1$, $\theta \neq 1$, alors $r^{-1}r_2 r$ est une réflexion telle que $r^{-1}r_2 re_1 = \theta e_2$, puisque $e_2 \in \mathrm{Fix}\,(r)$. Ainsi, l'ensemble
$$\Lambda := \{\theta \in \mathbb{C}\ ;\ \exists g \in G\ ;\ ge_1 = \theta e_1 \ \text{ et } \ V_1^\perp = \mathrm{Fix}\,(g)\}$$
est un sous-groupe de Θ. En effet, on vient de voir que $\Lambda \subseteq \Theta$ et si $\theta, \eta \in \Lambda$ sont associées à $g, h \in G$, alors
$$\forall x \in V_1^\perp,\ (gh(x) - x, e_1) = (gh(x), e_1) = \overline{\theta\eta}^{-1}(x, e_1) = 0,$$
et
$$\forall j \neq 1,\ (gh(x) - x, e_j) = (gh(x), gh(e_j)) - (x, e_j) = (x, e_j) - (x, e_j) = 0,$$
donc $(gh - 1)x \in V^\perp$, d'où $gh(x) = x$ et $x \in \mathrm{Fix}\,(gh)$ et comme $gh(e_1) = \theta\eta e_1$, on peut supposer que $gh \neq 1$ et $V_1^\perp = \mathrm{Fix}\,(gh)$, ce qui montre que $\theta\eta \in \Lambda$. Ainsi, il existe $q|m$ tel que $\Lambda = \mu_q$.
On a ensuite $G(q, 1, n) < G$ car si on a
$$r = r_{e_i,\theta} = ((1, \ldots, 1, \theta, 1, \ldots, 1), 1),$$
pour $\theta \in \mu_q = \Lambda$, alors $r \in G$. De même si $i > j$ et si
$$r := r_{e_i - \theta e_j, -1} r_{e_i - e_j, -1} = ((1, \ldots, 1, \theta, 1, \ldots, 1, \theta^{-1}, 1, \ldots, 1), 1),$$
on a $\theta \in \mu_m = \Theta$ et là aussi, $r \in G$. Comme $A(q, 1, n)$ est engendré par de telles réflexions, et comme tout $\pi \in \mathfrak{S}_n$ est également dans G, on obtient bien $G(q, 1, n) < G$. Par ailleurs, $m > 1$, sinon $G = \Sigma$ serait réductible car V, de dimension > 1, serait la représentation régulière de G.
- Si $\theta \in \Theta$ et $r \in G$ est une réflexion telle que $re_1 = \theta e_2$, alors $r_2 re_1 = \theta e_1$ et $r_2 re_2 = \theta^{-1} e_2$ d'où
$$r_2 r = ((1, \ldots, \theta, \ldots, \theta^{-1}, \ldots, 1), 1) \in A(m, m, n).$$
Ainsi, comme $A(m, m, n)$ est engendré par les $r_{e_i - \theta e_j, -1} r_{e_i - e_j, -1}$ avec $\theta \in \mu_m = \Theta$, $A(m, m, n)$ est un sous-groupe de G qui commute à $A(q, 1, n)$. Si l'on pose $p := m/q$, alors $A(m, p, n) = A(q, 1, n) \cdot A(m, m, n)$. En effet, le second membre est clairement un sous-groupe du premier et on a $|A(q, 1, n) \cap A(m, m, n)| = |\{\theta \in \mu_q^n\ ;\ \prod_i \theta_i = 1\}| = q^{n-1}$ et donc $|A(q, 1, n) \cdot A(m, m, n)| = \frac{m^n}{p} = |A(m, p, n)|$, d'où l'égalité. $G(m, p, n) = A(m, p, n) \rtimes \mathfrak{S}_n$ est ainsi un sous-groupe de G (voir [6], §2, p.387 pour ce dernier argument). Enfin, comme $G(m, p, n)$ contient toutes les réflexions de G, on obtient bien $G = G(m, p, n)$, ce qui achève la démonstration.

□

Remarque 15. À première vue, il semblerait que nous ayons montré qu'en fait, G et $G(m,p,n)$ sont égaux, ce qui est faux (et trop beau pour être vrai). En examinant la preuve et la définition des $G(m,p,n)$, on voit qu'on a fixé une base orthonormée (e_i) pour construire les $G(m,p,n)$ et l'irréductibilité ainsi que l'imprimitivité de G nous donnent une base orthonormée $(\widetilde{e_i})$. L'égalité vient alors du fait que l'on a supposé que $(e_i) = (\widetilde{e_i})$, donc en général, on a

$$G = G(m,p,n)^P,$$

où P est la matrice de passage de la base (e_i) à la base $(\widetilde{e_i})$ (en fait ici, P est unitaire car les bases considérées sont orthonormées). On doit conjuguer $G(m,p,n)$ par l'endomorphisme de changement de base. Par le Théorème 4, G et $G(m,p,n)$ sont conjugués dans $GL(V)$, donc aussi dans $U(V)$, comme souhaité.

Troisième partie

L'Algèbre des Quaternions réels

3.1 Construction et premières propriétés

Nous allons étudier dans cette partie une algèbre très particulière, inventée (découverte) en 1843 par William Hamilton. Cette algèbre (qui se trouve en réalité être un corps gauche), que nous noterons $\mathbb{H}$, possède beaucoup de propriétés remarquables, comme par exemple ses multiples constructions possibles, son lien étroit avec la géométrie, et plus précisément avec $SO_3(\mathbb{R})$ et $SO_4(\mathbb{R})$, $PSO_4(\mathbb{R})$ ou encore $SU_2(\mathbb{C})$, la structure des sous-groupes finis de ses unités, mais aussi le théorème de Frobenius, affirmant essentiellement que toute algèbre à division sur $\mathbb{R}$, de dimension finie, qui n'est ni $\mathbb{R}$ ni $\mathbb{C}$, est isomorphe à $\mathbb{H}$...

Commençons par construire $\mathbb{H}$ et exhibons quelques propriétés immédiates. Ces considérations se trouvent par exemple dans [16], Chapitre 7.

Proposition-Définition 2. *Il existe une $\mathbb{R}$-algèbre $\mathbb{H}$ de dimension 4, appelée algèbre des quaternions, munie d'une base $1, i, j, k$ telle que 1 soit l'élement neutre pour $\times$ et vérifiant*

$$i^2 = j^2 = k^2 = ijk = -1. \tag{2}$$

Démonstration. Il existe trois façons usuelles de construire $\mathbb{H}$:

1. On pose $\mathbb{H} := \mathbb{R}^4$, muni de la base canonique et définissons le produit sur $\mathbb{H}$ en étendant (2) par linéarité. Il suffit alors de vérifier l'associativité sur la base $1, i, j, k$, ce qui est long mais sans difficulté.
2. Supposons $\mathbb{H}$ déjà construite et définissons sur $\mathbb{H}$ l'action par translation $L_q : q' \mapsto qq'$, pour $q, q' \in \mathbb{H}$. Alors, L_q est linéaire et si $q := a + bi + cj + dk$ avec $a, b, c, d \in \mathbb{R}$, alors la matrice de L_q dans la base $1, i, j, k$ est

$$M(q) := \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} =: M(a, b, c, d).$$

Ceci étant dit, on peut définir

$$\mathbb{H} := \{M(a, b, c, d),\ a, b, c, d \in \mathbb{R}\}$$

et on vérifie alors les conditions requises. Notons que dans ce contexte, on a

$$i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

3. On peut enfin définir

$$\mathbb{H} := \left\{ M_{u,v} := \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix},\ u, v \in \mathbb{C} \right\}.$$

Alors, $\mathbb{H}$ est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{C})$ et on peut prendre

$$1 = M(1,0),\ i := M(0,1),\ j := M(\sqrt{-1},0),\ k := M(0,\sqrt{-1}).$$

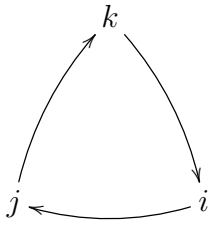
Là encore, il suffit de vérifier les formules (2).

□

Remarque 16. La relation (2) entraîne

$$ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik.$$

On peut retrouver rapidement ces formules à l'aide du diagramme



Définition 18.
- Pour un quaternion $q = a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$, on définit son conjugué :
$$\overline{q} := a - bi - cj - dk.$$
- Si $q \in \mathbb{H}$ est tel que $\overline{q} = -q$, on dit que q est un quaternion pur et on note $\mathcal{P}$ leur ensemble.

Proposition 10. *L'application*

$$\begin{array}{ccc} \mathbb{H} & \to & \mathbb{H} \\ q & \mapsto & \overline{q} \end{array}$$

est un anti-automorphisme.

Démonstration. En utilisant la représentation matricielle réelle, on voit que $M(\overline{q}) = {}^tM(q)$ et on a ${}^t(AB) = {}^tB{}^tA$. De plus, comme la conjugaison est clairement $\mathbb{R}$-linéaire, on obtient le résultat. □

Remarque 17. Pour tout $q \in \mathbb{H}$, on a $\overline{\overline{q}} = q$ (la conjugaison est une involution) et $\overline{q} = q$ si et seulement si $q \in \mathbb{R}$.

Proposition-Définition 3. *1. On définit une forme $\mathbb{R}$-linéaire sur $\mathbb{H}$, appelé trace, par*

$$\begin{array}{rccc} \mathrm{Tr}\ : & \mathbb{H} & \to & \mathbb{R} \\ & q & \mapsto & q + \overline{q} \end{array}$$

2. *On définit également la* <u>norme</u> N *comme étant la forme quadratique euclidienne sur* $\mathbb{H}$ *:*

$$\begin{array}{rccc} \mathrm{N} & : & \mathbb{H} & \to & \mathbb{R}_+ \\ & & q & \mapsto & q\overline{q} = \overline{q}q \end{array}$$

De plus, N *jouit des propriétés suivantes*

   (a) *Pour tous* $q, r \in \mathbb{H}$*, on a* $\mathrm{N}(qr) = \mathrm{N}(q)\mathrm{N}(r)$*.*

   (b) *La forme polaire de* N *est*

$$\varphi(q_1, q_2) = \frac{1}{2}(q_1\overline{q_2} + q_2\overline{q_1}),$$

   (c) *La base* $\{1, i, j, k\}$ *est* N*-orthonormale,*

   (d) *La conjugaison est une symétrie orthogonale d'espaces propres* $\mathbb{R}$ *et* $\mathcal{P}$*. En particulier, on a* $\mathbb{R} = \mathcal{P}^\perp$*.*

3. *Enfin, tout quaternion* $q \in \mathbb{H}$ *vérifie l'équation*

$$q^2 - \mathrm{Tr}(q)q + \mathrm{N}(q) = 0.$$

Démonstration. 1. Le fait que Tr soit une forme $\mathbb{R}$-linéaire est immédiat.

2. Pour $q \in \mathbb{H}$, on a $\overline{q\overline{q}} = \overline{\overline{q}q} = q\overline{q}$, donc $q\overline{q} \in \mathbb{R}$ et de même $\overline{q}q \in \mathbb{R}$. De plus, si $q = a + bi + cj + dk$, on a par calcul direct

$$q\overline{q} = a^2 + b^2 + c^2 + d^2 = \overline{q}q \in \mathbb{R}_+. \tag{3}$$

Ensuite, on a $\mathrm{N}(\lambda q) = \lambda^2\mathrm{N}(q)$ pour tout $\lambda \in \mathbb{R}$ et l'application

$$(q_1, q_2) \mapsto \frac{1}{2}(\mathrm{N}(q_1 + q_2) - \mathrm{N}(q_1) - \mathrm{N}(q_2)) = \frac{1}{2}(q_1\overline{q_2} + q_2\overline{q_1})$$

est bien $\mathbb{R}$-bilinéaire symétrique définie positive d'après (3). On vérifie alors immédiatement la multiplicativité de N et que $\{1, i, j, k\}$ est N-orthonormée. Enfin, avec la représentation matricielle réelle, on a

$$\varphi(q_1, q_2) = \frac{1}{4}\mathrm{Tr}({}^tM(q_1)M(q_2))$$

d'où

$$\varphi(\overline{q_1}, \overline{q_2}) = \frac{1}{4}\mathrm{Tr}({}^tM(\overline{q_1})M(\overline{q_2})) = \frac{1}{4}\mathrm{Tr}(M(q_1)^tM(q_2))$$

$$= \frac{1}{4}\mathrm{Tr}({}^tM(q_2)M(q_1)) = \varphi(q_2, q_1) = \varphi(q_1, q_2)$$

et ceci implique que la conjugaison soit une symétrie orthogonale.
Remarquons qu'avec la représentation complexe, on a, pour $q_l := a_l + b_li + c_lj + d_lk$ $(l = 1, 2)$,

$$\varphi(q_1, q_2) = \frac{1}{2}\mathrm{Tr}(M(a_1 + c_1i, b_1 + d_1i)M(a_2 + c_2i, b_2 + d_2i)^*)$$

et on retrouve le résultat.
Finalement, $\mathbb{R}$ et $\mathcal{P}$ sont des espaces propres pour la conjugaison et ce sont les seuls car $\mathbb{H} = \mathbb{R} \oplus^\perp \mathcal{P}$.

3. Pour $q = a + bi + cj + dk \in \mathbb{H}$, on calcule

$$q^2 - \mathrm{Tr}(q)q + \mathrm{N}(q) = a^2 - b^2 - c^2 - d^2 + 2a(bi+cj+dk) - 2a(a+bi+cj+dk) + a^2 + b^2 + c^2 + d^2 = 0,$$

d'où le résultat.

□

Théorème 8. *1. Le centre de* $\mathbb{H}$ *est* $\mathbb{R}$.

2. $\mathbb{H}$ *est une algèbre à division.*

3. $\widetilde{\mathrm{N}} := \mathrm{N}_{|\mathbb{H}^\times} : \mathbb{H}^\times \to \mathbb{R}_+^*$ *est un morphisme de groupes surjectif et on note*

$$\mathbb{S}^3 := \ker(\widetilde{\mathrm{N}}) \trianglelefteq \mathbb{H}^\times,$$

le groupe des quaternions de norme 1.

Démonstration. 1. Comme $\mathbb{H}$ est une $\mathbb{R}$ algèbre, on a clairement $\mathbb{R} \subset Z(\mathbb{H})$. Réciproquement, si $q := a + bi + cj + dk \in Z(\mathbb{H})$, on a $jq = qj$, d'où $b = d = 0$ et $qi = iq$ d'où $c = 0$ et donc $q = a \in \mathbb{R}$.

2. On a

$$\forall q \in \mathbb{H},\ \mathrm{N}(q) = 0 \ \Leftrightarrow\ q = 0.$$

De plus, $\mathrm{N}(q) \in \mathbb{R}$ donc $\mathrm{N}(q)$ et q commutent et si $q \neq 0$, on a

$$(\mathrm{N}(q)^{-1}\overline{q})q = 1 = q(\mathrm{N}(q)^{-1}\overline{q}),$$

donc q est inversible et

$$q^{-1} = \frac{\overline{q}}{\mathrm{N}(q)}.$$

3. $\widetilde{\mathrm{N}}$ est bien un morphisme d'après la Proposition-Définition 3 et si $a \in \mathbb{R}_+^*$, alors $\widetilde{\mathrm{N}}(\sqrt{a}) = a$ et donc $\widetilde{\mathrm{N}}$ est bien surjectif.

□

Remarque 18. Pour tout $q \in \mathbb{H}^\times$, on a $q \in \mathbb{S}^3$ si et seulement si $q^{-1} = \overline{q}$.
En identifiant $\mathbb{H}$ avec l'espace vectoriel euclidien $\mathbb{R}^4$, on a

$$\mathbb{S}^3 = \{(a,b,c,d) \in \mathbb{R}^4\ ;\ a^2 + b^2 + c^2 + d^2 = 1\},$$

donc $\mathbb{S}^3$ est homéomorphe à la sphère unité de $\mathbb{R}^4$, ce qui justifie notre notation. En particulier, $\mathbb{S}^3$ est connexe et compact (pour la métrique induite par N).
Enfin, pour $q \in \mathbb{H}$, on a

$$q \in \mathbb{R} \ \Leftrightarrow\ q^2 \in \mathbb{R}_+ \ \text{ et } \ q \in \mathcal{P} \ \Leftrightarrow\ q^2 \in \mathbb{R}_-.$$

3.2 Opération de $\mathbb{H}$ sur $\mathbb{R}^3$: Structure de $SO_3(\mathbb{R})$

Nous allons chercher ici à paramétrer $SO_3(\mathbb{R})$ par un sous-groupe de $\mathbb{H}^\times$, un peu comme on paramètre $SO_2(\mathbb{R})$ par le sous-groupe $\mathbb{U}$ de $\mathbb{C}^\times$, formé des complexes de module 1.

Pour ceci, on va faire agir $\mathbb{H}^\times$ sur $\mathbb{H}$ par automorphisme intérieur ; action non triviale puisque $\mathbb{H}$ n'est pas commutatif. Mais, si $q \in \mathbb{H}^\times$, on écrit $q = \sqrt{\mathrm{N}(q)}q'$ avec $q' \in \mathbb{S}^3$ et comme $\sqrt{\mathrm{N}(q)} \in \mathbb{R}^*$ est central, il n'influe pas sur l'action. Notons qu'au passage, on a une suite exacte courte scindée

$$1 \longrightarrow \mathbb{S}^3 \longrightarrow \mathbb{H}^\times \longrightarrow \mathbb{R}_+^* \longrightarrow 1$$

et il en découle un isomorphisme

$$\mathbb{H}^\times \simeq \mathbb{S}^3 \rtimes \mathbb{R}_+^*.$$

Il suffit donc de faire agir $\mathbb{S}^3$ sur $\mathbb{H}$ par

$$\forall q \in \mathbb{S}^3,\ \forall q' \in \mathbb{H},\ S_q(q') := qq'q^{-1} = qq'\overline{q}.$$

On pose de plus

$$s_q := S_{q|\mathcal{P}}.$$

On a alors le résultat suivant :

Théorème 9. *L'application $s : \mathbb{S}^3 \to \mathrm{Aut}\,(\mathbb{H})$ se factorise en un isomorphisme*

$$\overline{s}\ :\ \mathbb{S}^3 \Big/ \{\pm 1\} \xrightarrow{\sim} SO_3(\mathbb{R})\ .$$

Démonstration. 1. Pour $q \in \mathbb{S}^3$, l'application $S_q : \mathbb{H} \to \mathbb{H}$ est $\mathbb{R}$-linéaire et bijective puisque $(S_q)^{-1} = S_{\overline{q}}$, d'où une application

$$S : \mathbb{S}^3 \to GL_4(\mathbb{R}).$$

C'est de plus un morphisme car

$$\forall q_1, q_2 \in \mathbb{S}^3,\ \forall q' \in \mathbb{H},\ (S_{q_1} \circ S_{q_2})(q') = S_{q_1}(q_2q'q_2^{-1})$$

$$= q_1q_2q'\overline{q_2}\ \overline{q_1} = (q_1q_2)q'(\overline{q_1q_2}) = S_{q_1q_2}(q')$$

et on a

$$\ker S = \{q \in \mathbb{S}^3\ ;\ \forall q' \in \mathbb{H},\ qq'q^{-1} = q'\} = Z(\mathbb{H}) \cap \mathbb{S}^3 = \mathbb{R} \cap \mathbb{S}^3 = \{\pm 1\}.$$

2. Par ailleurs, on a

$$\forall q \in \mathbb{S}^3,\ \forall q' \in \mathbb{H},\ \mathrm{N}(S_q(q')) = \mathrm{N}(q)\mathrm{N}(q')\mathrm{N}(\overline{q}) = \mathrm{N}(q')\ \Rightarrow\ S_q \in O(\mathrm{N}) \simeq O_4(\mathbb{R})$$

et comme pour $a \in \mathbb{R}$, $S_q(a) = a$, il vient $S_{q|\mathbb{R}} = id_{\mathbb{R}}$. Ainsi, $\mathcal{P}$ est S_q-stable puisque $\mathcal{P} = \mathbb{R}^\perp$ et donc $s_q = S_{q|\mathcal{P}} \in O(\mathrm{N}_{|\mathcal{P}}) \simeq O_3(\mathbb{R})$. On obtient donc un morphisme

$$s : \mathbb{S}^3 \to O_3(\mathbb{R}).$$

3. Considérons sur $\mathbb{S}^3$ la topologie induite par l'espace vectoriel normé $(\mathbb{H}, \sqrt{\mathrm{N}})$ et sur $O_3(\mathbb{R})$, celle induite par $\mathcal{M}_3(\mathbb{R}) \simeq \mathbb{R}^9$. L'application s est alors continue. En effet, si $q = a + bi + cj + dk \in \mathbb{S}^3$, la matrice de s_q dans la base $\{i, j, k\}$ de $\mathcal{P}$ est donnée par

$$\mathrm{Mat}_{(i,j,k)}(s_q) = \begin{pmatrix} a^2+b^2-c^2-d^2 & 2(cb-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix},$$

et chaque coefficient de cette matrice est un polynôme homogène de degré 2 en les coefficients de q, donc est continu. Mais, l'application $\det : O_3(\mathbb{R}) \twoheadrightarrow \{\pm 1\}$ étant polynômiale en les coefficients de son argument, elle est aussi continue. Ainsi, la composée

$$\det \circ s : \mathbb{S}^3 \to \{\pm 1\}$$

est continue et comme $\mathbb{S}^3$ est connexe, $\det(s(\mathbb{S}^3))$ est connexe et puisque $s(1) = id$, on a $\det(s(\mathbb{S}^3)) = \{1\}$ et donc $s(\mathbb{S}^3) \subset SO_3(\mathbb{R})$.

4. Il reste à montrer que $s(\mathbb{S}^3) = SO_3(\mathbb{R})$. Puisque les renversements engendrent $SO_3(\mathbb{R})$ (cf Annexe, théorème 3), il suffit de montrer que tout renversement est atteint. Soit donc $\sigma \in SO_3(\mathbb{R})$ un renversement d'axe Vect $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$. Comme a, b, c sont non tous nuls, on peut supposer que $a^2 + b^2 + c^2 = 1$ et soit alors $q := ai + bj + ck \in \mathcal{P} \cap \mathbb{S}^3$. On a $s_q(q) = qq\overline{q} = q$ donc $s_q \in SO_3(\mathbb{R})$ fixe q et donc s_q est une rotation d'axe $\langle q \rangle$. Comme $q \in \mathcal{P} \cap \mathbb{S}^3$, on a $q^2 = -q\overline{q} = -1$ d'où $(s_q)^2 = s_{q^2} = s_{-1} = id$ et s_q est une involution, donc s_q est le renversement d'axe $\langle q \rangle$ et donc $s_q = \sigma$. On en déduit, par factorisation canonique, un diagramme

$$\begin{array}{ccc} \mathbb{S}^3 & \xrightarrow{\ s\ } & SO_3(\mathbb{R}) \\ {\scriptstyle \pi}\downarrow & \overset{\sim}{\nearrow}_{\overline{s}} & \\ \mathbb{S}^3 \big/ \{\pm 1\} & & \end{array}$$

et le résultat.

□

Remarque 19. On peut alors se demander si l'extension associée

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{S}^3 \xrightarrow{\ s\ } SO_3(\mathbb{R}) \longrightarrow 1$$

est scindée. Ce n'est pas le cas. En effet, sinon, il existerait $H < \mathbb{S}^3$ d'indice 2 tel que $s_{|H}$ soit un isomorphisme entre H et $SO_3(\mathbb{R})$. Mais, dans ce cas, si $g \in \mathbb{S}^3$, on a $g \in H$ ou $-g \in H$, et si $q \in \mathcal{P} \cap \mathbb{S}^3$, on aurait $q^2 = -q\overline{q} = -\mathrm{N}(q) = -1$, d'où $-1 \in H$, ce qui est absurde.

On peut donner en première application le résultat suivant :

Théorème 10. *Tout automorphisme de $\mathbb{H}$ est intérieur.*

Démonstration. Soit donc $u \in \mathrm{Aut}(\mathbb{H})$. u conserve $Z(\mathbb{H}) = \mathbb{R}$, donc $u_{|\mathbb{R}} \in \mathrm{Aut}(\mathbb{R})$ et donc $u_{|\mathbb{R}} = id_{\mathbb{R}}$. Ensuite, par la remarque 18, $q \in \mathcal{P}$ si et seulement si $q^2 \in \mathbb{R}_-$, donc, si $q \in \mathcal{P}$, on a $u(q)^2 = u(q^2) = q^2 \in \mathbb{R}_-$, donc $u(q) \in \mathcal{P}$ et $\mathcal{P}$ est u-stable. De plus, pour $q \in \mathcal{P}$, on a $\mathrm{N}(q) = -q^2$ et donc $\mathrm{N}(u(q)) = -u(q)^2 = -u(q^2) = -q^2 = \mathrm{N}(q)$, d'où $u_{|\mathcal{P}} \in O(\mathrm{N}_{|\mathcal{P}}) \simeq O_3(\mathbb{R})$. Or, $\{i, j, k\}$ est une base N-orthonormée de $\mathcal{P}$, donc $i' := u(i)$, $j' := u(j)$ et $k' := u(k)$ constituent également une base orthonormée. Il existe donc $\epsilon \in \{\pm 1\}$ tel que les bases $\{i, j, k\}$ et $\{i', j', \epsilon k'\}$ soient de même orientation. Par le Théorème 9, il existe alors $q \in \mathbb{S}^3$ tel que $i' = s_q(i)$, $j' = s_q(j)$ et $\epsilon k' = s_q(k)$. Mais, u et S_q sont dans $\mathrm{Aut}(\mathbb{H})$, donc il vient

$$i'j' = u(i)u(j) = u(ij) = u(k) = k' \quad \text{et} \quad i'j' = s_q(i)s_q(j) = s_q(ij) = s_q(k) = \epsilon k',$$

d'où $\epsilon = 1$ et donc $u_{|\mathcal{P}} = s_q = S_{q|\mathcal{P}}$ et comme $u_{|\mathbb{R}} = id_{\mathbb{R}} = S_{q|\mathbb{R}}$, on en déduit que $u = S_q$ est bien un automorphisme intérieur. □

3.3 Action sur $SO_4(\mathbb{R})$, relation avec $SU_2(\mathbb{C})$ et théorème de Frobenius

On dispose d'une autre action de $\mathbb{S}^3$ sur $\mathbb{H}$, définie par la translation à gauche

$$L_q(q') := qq',\ q \in \mathbb{S}^3,\ q' \in \mathbb{H}.$$

Nous allons effectuer le même travail que dans la section précédente, afin de paramétrer $SO_4(\mathbb{R})$. Pour cela, on va faire agir le produit direct $\mathbb{S}^3 \times \mathbb{S}^3$ sur $\mathbb{H}$. Soient $q_1, q_2 \in \mathbb{S}^3$ et posons

$$S_{q_1,q_2} := L_{q_1\overline{q_2}} \circ S_{q_2},$$

c'est-à-dire que, pour $q \in \mathbb{H}$, on pose

$$S_{q_1,q_2}(q) := q_1 q \overline{q_2}.$$

On a alors le résultat :

Théorème 11. *L'application $S_{\bullet,\bullet}$ induit un isomorphisme*

$$\overline{S} \ : \ (\mathbb{S}^3 \times \mathbb{S}^3) \Big/ \{\pm(1,1)\} \xrightarrow{\sim} SO_4(\mathbb{R})\ .$$

Démonstration.

1. Pour $q_1, q_2 \in \mathbb{S}^3$, l'application $S_{q_1,q_2} : \mathbb{H} \to \mathbb{H}$ est $\mathbb{R}$-linéaire et bijective (d'inverse $S_{\overline{q_1},\overline{q_2}}$) et l'application

$$\begin{array}{rccc} S & : & \mathbb{S}^3 \times \mathbb{S}^3 & \to & GL_4(\mathbb{R}) \\ & & (q_1, q_2) & \mapsto & S_{q_1,q_2} \end{array}$$

est un morphisme de groupes.

2. Calculons le noyau de S. Si $(q_1, q_2) \in \ker S$, (i.e. $S_{q_1,q_2} = id$), alors on a, pour tout $q \in \mathbb{H}$, $q_1 q \overline{q_2} = q$. Pour $q = 1$, on obtient $q_1 = q_2$ et q_1 est alors central, donc $q_1 \in \{\pm 1\}$, d'où $\ker S = \{(1,1), (-1,-1)\}$.

3. Montrons que $\operatorname{im} S = SO_4(\mathbb{R})$. Comme S est continue, par composition et comme $\mathbb{S}^3 \times \mathbb{S}^3$ est connexe, le même argument que dans la preuve du Théorème 9 montre que $S(\mathbb{S}^3 \times \mathbb{S}^3) \subset SO(\mathrm{N}) \simeq SO_4(\mathbb{R})$. Pour l'inclusion réciproque, soit $g \in SO(\mathrm{N})$. Si $g(1) = 1$, comme $\mathcal{P} = 1^\perp$, on a $g(\mathcal{P}) = \mathcal{P}$, d'où $g_{|\mathcal{P}} \in SO_3(\mathbb{R})$ et par le Théorème 9, il existe $q \in \mathbb{S}^3$ tel que $g_{|\mathcal{P}} = s_q$ et alors $g = S_{q,q}$. Si $g(1) = r \neq 1$, on a $\mathrm{N}(r) = \mathrm{N}(1) = 1$ d'où $r \in \mathbb{S}^3$. Alors, on a $S_{\overline{r},1} \circ g(1) = S_{\overline{r},1}(r) = \overline{r}r1 = 1$. Par le premier cas, il existe $q \in \mathbb{S}^3$ tel que $S_{\overline{r},1} \circ g = S_{q,q}$ et donc $g = S_{rq,q}$, comme voulu.
4. Le théorème s'obtient maintenant par factorisation canonique

$$\begin{array}{ccc} \mathbb{S}^3 \times \mathbb{S}^3 & \xrightarrow{\quad S \quad} & SO_4(\mathbb{R}) \\ {\scriptstyle \pi}\downarrow & \overset{\sim}{\nearrow}_{\overline{S}} & \\ (\mathbb{S}^3 \times \mathbb{S}^3) \Big/ \{\pm(1,1)\} & & \end{array}$$

□

Rappelons la définition du groupe projectif orthogonal (voir [16], Chapitre 6, §2) :

$$PO_n(\mathbb{R}) := O_n(\mathbb{R}) \Big/ Z(O_n(\mathbb{R})) = O_n(\mathbb{R}) \Big/ \{\pm id\}$$

et du groupe projectif spécial orthogonal :

$$PSO_n(\mathbb{R}) := SO_n(\mathbb{R}) \Big/ Z(SO_n(\mathbb{R}))$$

$$= SO_n(\mathbb{R}) \Big/ (\{\pm id\} \cap SO_n(\mathbb{R})) = \begin{cases} SO_n(\mathbb{R}) & \text{si } n \text{ est impair} \\ SO_n(\mathbb{R}) \Big/ \{\pm id\} & \text{si } n \text{ est pair} \end{cases}$$

Notons V le sous-groupe de $\mathbb{S}^3 \times \mathbb{S}^3$ défini par

$$V := \{(1,1), (-1,1), (1,-1), (-1,-1)\}.$$

Corollaire 10. *On a un isomorphisme*

$$\widehat{S} \ : \ (\mathbb{S}^3 \times \mathbb{S}^3) \,/_V \xrightarrow{\sim} PSO_4(\mathbb{R}) \, .$$

Démonstration. Par le Théorème 11, on a déjà un morphisme surjectif

$$S \ : \ \mathbb{S}^3 \times \mathbb{S}^3 \xrightarrow{\pi} (\mathbb{S}^3 \times \mathbb{S}^3) \Big/ \{\pm(1,1)\} \xrightarrow[\sim]{\overline{S}} SO_4(\mathbb{R}) \, ,$$

ce qui donne, par passage au quotient, un épimorphisme

$$\check{S} \ : \ \mathbb{S}^3 \times \mathbb{S}^3 \xrightarrow{S} SO_4(\mathbb{R}) \longrightarrow PSO_4(\mathbb{R}) \, .$$

Il reste à en calculer le noyau. Soient donc $q_1, q_2 \in \mathbb{S}^3$. Si $S_{q_1,q_2} = id$, on a vu que $(q_1, q_2) \in \{(1,1), (-1,-1)\}$. Si $S_{q_1,q_2} = -id$, i.e. si pour tout $q \in \mathbb{H}$, $q_1 q \overline{q_2} = -q$, en faisant $q = 1$, on trouve $q_1 = -q_2$ et q_1 est alors central, donc $q_1 = \pm 1$ et donc $(q_1, q_2) \in \{(1,-1), (-1,1)\}$. On en déduit que $\ker \check{S} = V$, d'où le résultat, par factorisation canonique. □

Corollaire 11. *On a encore un isomorphisme*

$$PSO_4(\mathbb{R}) \simeq SO_3(\mathbb{R}) \times SO_3(\mathbb{R}).$$

En particulier, $PSO_4(\mathbb{R})$ n'est pas simple, contrairement aux autres $PSO_n(\mathbb{R})$ pour $n \geq 3$ (cf [16], Chapitre 6, §7).

Démonstration. On a un épimorphisme

$$\begin{array}{rccc} \varphi & : & \mathbb{S}^3 \times \mathbb{S}^3 & \to & \mathbb{S}^3 \Big/ \{\pm 1\} \times \mathbb{S}^3 / \pm 1\} \\ & & (q_1, q_2) & \mapsto & (\pi(q_1), \pi(q_2)) \end{array}$$

où $\pi : \mathbb{S}^3 \twoheadrightarrow \mathbb{S}^3 \Big/ \{\pm 1\}$ est la projection canonique. On voit alors que $\ker \varphi = V$, d'où un isomorphisme

$$PSO_4(\mathbb{R}) \simeq \left(\mathbb{S}^3 \times \mathbb{S}^3\right) / V \xrightarrow[\sim]{\overline{\varphi}} \left(\mathbb{S}^3 \Big/ \{\pm 1\} \times \mathbb{S}^3 \Big/ \{\pm 1\}\right) \simeq SO_3(\mathbb{R}) \times SO_3(\mathbb{R}).$$

□

Étudions à présent la relation entre $\mathbb{H}$ et $SU_2(\mathbb{C})$. Commençons par deux résultats :

Lemme 9. *Définissons*

$$\begin{array}{rccc} \psi & : & \mathbb{S}^1 \times \mathbb{S}^3 & \to & U_2(\mathbb{C}) \\ & & (\alpha, q) & \mapsto & L(\alpha)R(q) = S_{\alpha,q} \end{array}$$

Alors, ψ est surjectif et $\ker \psi = \{\pm(1,1)\}$.

Démonstration. (Voir [15], Proposition 5.11)
Le corps $\mathbb{C}$ se plonge dans $\mathbb{H}$ et $\mathbb{H}$ est alors un $\mathbb{C}$-espace vectoriel pour la loi externe

$$\begin{array}{ccc} \mathbb{C} \times \mathbb{H} & \to & \mathbb{H} \\ (\lambda, q) & \mapsto & \lambda q \end{array}$$

De plus, une base de $\mathbb{H}$ sur $\mathbb{C}$ est donnée par $(1, j)$. En effet, si $q \in \mathbb{H}$, que l'on écrit $q = a + bi + cj + dk$, alors $q = (a + bi) + (c + di)j = \lambda \cdot 1 + \mu \cdot j$ où $\lambda, \mu \in \mathbb{C}$.
Si $q := a + bj \in \mathbb{S}^3$, on a

$$\mathrm{Mat}_{(1,j)}(R(q)) = \begin{pmatrix} \overline{a} & \overline{b} \\ -b & a \end{pmatrix}.$$

De plus, on voit que $\alpha \in \mathbb{S}^1$ si et seulement si $L(\alpha)$ est $\mathbb{C}$-linéaire et orthogonale pour la forme

$$(q, r) = \frac{q\overline{r} - iq\overline{r}i}{2}$$

dont la forme quadratique associée est $(q, q) = \mathrm{N}(q)$. Ainsi, si $(\alpha, q) \in \mathbb{S}^1 \times \mathbb{S}^3$, alors $S_{\alpha,q} \in U_2(\mathbb{C})$. Si $T \in U_2(\mathbb{C})$, soit $q := T(1)$. Alors, $R(q)T$ fixe 1, donc laisse stable $1^\perp = \mathbb{C}j$. Ainsi, $R(q)T(j) = \alpha j$ pour un certain $\alpha \in \mathbb{C}$ et ainsi, $T = L(\alpha)R(q^{-1}) = S_{\alpha,\overline{q}}$. En fait, comme $R(q)T$ est orthogonale, $\alpha \in \mathbb{S}^1$. De plus, si $\psi(\alpha, q) = id_{\mathbb{C}^2}$, on a $1 = L(\alpha)R(q)(1) = \alpha\overline{q}$ donc $\alpha = q$ et $j = L(\alpha)R(\alpha)(j) = \alpha j \alpha^{-1}$ donc $\alpha \in \mathbb{R}$ et comme $|\alpha| = 1$, on obtient $\alpha \in \{\pm 1\}$. □

Corollaire 12. *On a*

$$U_2(\mathbb{C}) \simeq L(\mathbb{S}^1) \circ R(\mathbb{S}^3).$$

Démonstration. On a $Z(L(\mathbb{S}^1)) = L(\mathbb{S}^1)$ et $Z(R(\mathbb{S}^3)) = \{\pm 1\} =: Z$. La première égalité est évidente et pour la seconde, si $R(q) \in Z(R(\mathbb{S}^3))$, alors pour tout $r \in \mathbb{S}^3$, on a

$$R(q)R(r) = R(r)R(q) \;\Leftrightarrow\; R(qrq^{-1}r^{-1}) = 1 \;\Leftrightarrow\; qr = rq.$$

En prenant $r = i$, on obtient $q \in \mathbb{C}$ et avec $r = j$, il vient $q \in \mathbb{R}$ et comme $q \in \mathbb{S}^3$, ceci implique $q = \pm 1$ et donc $R(q) = \pm 1$.
Soit aussi

$$W := \{1, L(i)\} = \{\pm 1\} \leq L(\mathbb{S}^1) = Z(L(\mathbb{S}^1))$$

ainsi que

$$\theta : Z \to W$$

l'isomorphisme naturel. En écrivant

$$K := \{(z, \theta(z^{-1})),\ z \in Z\} = \{\pm(1,1)\} = \ker \psi,$$

il vient alors

$$L(\mathbb{S}^1) \circ R(\mathbb{S}^3) \overset{\text{def}}{=} (L(\mathbb{S}^1) \times R(\mathbb{S}^3)) \,/_K \simeq (\mathbb{S}^1 \times \mathbb{S}^3) \Big/ \{\pm(1,1)\} = (\mathbb{S}^1 \times \mathbb{S}^3) \,/_{\ker \psi} \simeq U_2(\mathbb{C}).$$

□

On en arrive au théorème :

Théorème 12. *On a un isomorphisme*

$$R \;:\; \mathbb{S}^3 \xrightarrow{\sim} SU_2(\mathbb{C})\ .$$

Démonstration. Considérons l'opération par translation R de $\mathbb{S}^3$ sur $\mathbb{H}$. Pour $g \in \mathbb{S}^3$, $R(q)$ est $\mathbb{C}$-linéaire car

$$\forall q' \in \mathbb{H},\ \forall \lambda \in \mathbb{C},\ R(q)(\lambda q') = (\lambda q')\overline{q} = \lambda(q'\overline{q}) = \lambda R(q)(q'),$$

et $R(q)$ est bijective (d'inverse $R(\overline{q})$), d'où $R(q) \in GL_2(\mathbb{C})$. Ceci donne un morphisme injectif

$$R : \mathbb{S}^3 \hookrightarrow GL_2(\mathbb{C}).$$

De plus, pour $q \in \mathbb{S}^3$, on a (en écrivant $q = \lambda \cdot 1 + \mu \cdot j$)

$$M(q) := \mathrm{Mat}_{(1,j)}(R(q)) = \begin{pmatrix} \overline{\lambda} & \overline{\mu} \\ -\mu & \lambda \end{pmatrix}$$

avec $|\lambda|^2 + |\mu|^2 = 1$ puisque $q \in \mathbb{S}^3$. On a alors

$$M(q)M(q)^* = M(q)^*M(q) = I_2,$$

et $\det(M(q)) = 1$, donc $M(q) \in SU_2(\mathbb{C})$ et ceci nous donne un morphisme injectif

$$R : \mathbb{S}^3 \hookrightarrow SU_2(\mathbb{C}).$$

Il reste à montrer que R est surjectif. Si $M \in SU_2(\mathbb{C})$, on note

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

avec $a, b, c, d \in \mathbb{C}$. Alors $ad - bc = 1$, donc

$$M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

et comme $M^{-1} = M^* = {}^t\overline{M}$, on en déduit que $d = \overline{a}$ et $c = -\overline{b}$, d'où

$$M = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} = M(q), \quad \text{avec} \quad q := a \cdot 1 + b \cdot j,$$

d'où le résultat. □

Corollaire 13. *On a*

$$SU_2(\mathbb{C}) \Big/ \{\pm 1\} \simeq SO_3(\mathbb{R}).$$

En particulier, le groupe $SU_2(\mathbb{C}) \Big/ \{\pm 1\}$ *est simple.*

On peut enfin se demander s'il existe un autre corps que les quaternions qui soit une $\mathbb{R}$-algèbre de dimension finie, afin d'obtenir des paramétrisations des groupes orthogonaux en dimension supérieure. Le théorème suivant, dû à Frobenius, répond négativement à la question :

Théorème 13. *(Frobenius, 1877)*
Si $\Bbbk$ *est une* $\mathbb{R}$*-algèbre à division de dimension finie, dans laquelle* $\mathbb{R}$ *est central, alors* $\Bbbk$ *est isomorphe à* $\mathbb{R}$, $\mathbb{C}$ *ou* $\mathbb{H}$.

Démonstration. (Voir [16], Chapitre 7, Théorème 4.3)

1. On suppose dans un premier temps que $\Bbbk$ est commutatif et que $\Bbbk \neq \mathbb{R}$. Si $a \in \Bbbk \setminus \mathbb{R}$, comme $[\Bbbk : \mathbb{R}] < \infty$, a est algébrique sur $\mathbb{R}$ et si P désigne son polynôme minimal, comme P est irréductible sur $\mathbb{R}$, on a $\deg P = 2$ et on écrit $P(X) = X^2 + \alpha X + \beta$. Son discriminant Δ est strictement négatif mais on a $\Delta = (2a + \alpha)^2$, donc Δ est un carré dans $\Bbbk$, donc -1 aussi. Ainsi, $\Bbbk$ est une extension (finie donc) algébrique de $\mathbb{C}$ et comme $\mathbb{C}$ est algébriquement clos, on doit avoir $\Bbbk = \mathbb{C}$.
2. On suppose ici $\Bbbk$ non commutatif. Soit $a \in \Bbbk \setminus \mathbb{R}$. Comme $\mathbb{R}(a) \neq \mathbb{R}$ est un corps commutatif, on a par ce qui précède $\mathbb{R}(a) \simeq \mathbb{C}$, donc $\Bbbk$ contient un sous-corps isomorphe à $\mathbb{C}$, que l'on note encore $\mathbb{C}$ et on choisit i une racine de -1 dans $\mathbb{C}$. Alors, $\mathbb{C}$ est un sous-corps commutatif maximal de $\Bbbk$ (par le premier cas), donc si $x \in \Bbbk$ commute à i, alors $x \in \mathbb{C}$. En effet, dans ce cas x centralise $\mathbb{C}$, donc $\mathbb{C}(x)$ est une extension algébrique de $\mathbb{C}$ et donc $\mathbb{C}(x) = \mathbb{C}$ et $x \in \mathbb{C}$.
   On va chercher à reconstruire $\mathbb{H}$. Soit $y \in \Bbbk \setminus \mathbb{C}$. y ne commute pas à i et soit alors $z := yi - iy \neq 0$. Alors, $iz = iyi + y = -zi$, d'où $iz^2 = -ziz = z^2 i$ et donc $z^2 \in \mathbb{C}$. De plus, d'après le premier cas, comme $\mathbb{R}(z)$ est commutatif et $z \notin \mathbb{R}$, on a $[\mathbb{R}(z) : \mathbb{R}] = 2$ et puisque $\mathbb{R}(z) \neq \mathbb{C}$, on a $\mathbb{R}(z) \cap \mathbb{C} = \mathbb{R}$ et donc $z^2 \in \mathbb{R}$. On a même $z^2 \in \mathbb{R}_+^*$. En

effet, si $z^2 = a > 0$, alors $X^2 - a$ aurait quatre solutions $\{z, -z, \sqrt{a}, -\sqrt{a}\}$ dans $\mathbb{R}(z)$ qui est un corps et ceci serait absurde. Ainsi, $z^2 = -\alpha$ avec $\alpha \in \mathbb{R}_+^*$ et soit $j := \frac{z}{\sqrt{\alpha}}$. On a $ji = -ij$ et $j^2 = -1$. Si l'on pose $k := ij$, le sous-$\mathbb{R}$-espace vectoriel de $\Bbbk$ engendré par $\{1, i, j, k\}$ est une sous-algèbre à division de $\Bbbk$, que l'on note $\mathbb{H}$. On a $\mathbb{H} \subset \Bbbk$ et il nous reste à voir que l'on a égalité.

3. Supposons que $\mathbb{H} \subsetneq \Bbbk$ et soit $u \in \Bbbk \setminus \mathbb{H}$. Réitérons le processus précédent et soit $v := ui - iu$. Alors $vi = -iv$ et comme précédemment, il vient $v^2 \in \mathbb{R}_+^*$ et en posant $l := \frac{v}{\sqrt{-v^2}}$, on a $il = -li$ et $l^2 = -1$. Alors, on a $jli = -jil = ijl$, d'où $jl \in \mathbb{C} \subset \mathbb{H}$, donc $l \in \mathbb{H}$ et donc $v \in \mathbb{H}$. Soit enfin $w := ui + iu$. w commute à i, d'où $w \in \mathbb{C} \subset \mathbb{H}$, donc $ui = \frac{v+w}{2} \in \mathbb{H}$ et donc $u \in \mathbb{H}$, ce qui est absurde et termine la démonstration.

□

3.4 Classification des sous-groupes finis de $\mathbb{H}^\times$ et de $SU_2(\mathbb{C})$

Avant toute chose, rappelons les notations

$$\forall q, r \in \mathbb{S}^3,\ \forall v \in \mathbb{H},\ L(q)(v) := qv,\ R(r)(v) := v\overline{r}.$$

Nous allons nous intéresser ici aux sous-groupes finis des unités de $\mathbb{H}$ et l'on va voir que l'on peut en donner une description complète. Par la section 3.3, on aura alors aussi une classification des sous-groupes finis de $SU_2(\mathbb{C})$.

Nous allons tout d'abord construire ces groupes. On démarre avec un lemme :

Lemme 10. *Soient $q, r \in \mathbb{H}^\times$. Les assertions suivantes s'équivalent :*

i) $\mathrm{N}(q) = \mathrm{N}(r)$ *et* $\mathrm{Tr}(q) = \mathrm{Tr}(r)$,

ii) q *et* r *sont conjugués dans* $\mathbb{S}^3$,

iii) $\mathrm{N}(q)$ *est valeur propre de* $S_{q,r} = L(q)R(r)$.

Démonstration. Supposons *ii)* et montrons *i)*.
Si $q = hrh^{-1} = hr\overline{h}$ avec $h \in \mathbb{S}^3$, alors $\mathrm{N}(q) = \mathrm{N}(h)\mathrm{N}(r)\mathrm{N}(\overline{h}) = \mathrm{N}(r)$ et $\mathrm{Tr}(q) = hr\overline{h} + \overline{hr\overline{h}} = h(r + \overline{r})\overline{h} = h\mathrm{Tr}(r)\overline{h} = \mathrm{Tr}(r)$ car $\mathrm{Tr}(r) \in \mathbb{R}$.
Supposons *i)* et montrons *ii)* ainsi que *iii)*.

- Si $q \in \mathbb{R}$, on a

$$\mathrm{N}(q - r) = (q - r)(\overline{q} - \overline{r}) = \mathrm{N}(q) + \mathrm{N}(r) - q\overline{r} - r\overline{q} = 2\mathrm{N}(q) - q\mathrm{Tr}(r) = 0,$$

  donc $r = q$. Ainsi $h = 1$ convient et on obtient *ii)* et *iii)*.

- Si $q \notin \mathbb{R}$, alors $\mathbb{H}$ est un espace vectoriel de dimension 2 sur $\mathbb{R}(q) \simeq \mathbb{C}$ et $R(r) \in \mathrm{End}_{\mathbb{R}(q)}(\mathbb{H})$, et comme $X^2 - \mathrm{Tr}(r)X + \mathrm{N}(r)$ est annulateur de $R(r)$, les valeurs propres de $R(r)$ sont ses racines dans $\mathbb{R}(q)$, donc le spectre de $R(r)$ est $\{q, \overline{q}\}$. Soit $h \in \ker(R(r) - \overline{q}id_{\mathbb{H}}\}\setminus\{0\}$ un vecteur propre unitaire. Alors, on a $h\overline{r} = \overline{q}h$, d'où $q = hrh^{-1}$ et on obtient *ii)*. De plus, on obtient également $S_{q,r}(h) = qh\overline{r} = \mathrm{N}(q)h$, donc $\mathrm{N}(q)$ est valeur propre de $S_{q,r}$, d'où *iii)*.

Montrons enfin que *iii*) entraîne *ii*).
Si h est vecteur propre unitaire pour $\mathrm{N}(q)$ de $S_{q,r}$, on a $qh\overline{r} = \mathrm{N}(q)h$ d'où $h\overline{r} = \overline{q}h$ donc $q = hrh^{-1}$, d'où le résultat. □

Remarquons que si $q \in \mathbb{H}^\times$ est d'ordre finie, alors $\mathrm{N}(q)$ est d'ordre fini dans $\mathbb{R}_+^*$, donc $\mathrm{N}(q) = 1$ et $q \in \mathbb{S}^3$. Ainsi, tout sous-groupe fini de $\mathbb{H}^\times$ est en réalité un sous-groupe fini de $\mathbb{S}^3$.

Définissons à présent quelques groupes :

Groupes dicycliques

Pour $m \in \mathbb{N}^*$, on pose

$$\zeta_m := \exp\left(\frac{2i\pi}{m}\right),$$

ainsi que

$$\mathcal{C}_m := \langle \zeta_m \rangle < \mathbb{H}^\times \quad \text{et} \quad \mathcal{BD}_m := \langle \zeta_m, j \rangle < \mathbb{H}^\times.$$

Si $\alpha \in \mathcal{C}_m$, on a $j\alpha j^{-1} = j\alpha\overline{j} = -j\alpha j = \overline{\alpha} = \alpha^{-1}$, donc $\mathcal{C}_m \trianglelefteq \mathcal{BD}_m$. Remarquons que l'on a

$$j\zeta_m = \overline{\zeta_m} j = \zeta_m^{-1} j.$$

* Si $m = 2n+1$ est impair et si $x \in \mathcal{BD}_m$, x s'écrit $x = j^\epsilon \zeta_m^l$ avec $\epsilon \in \{-1, 0, 1\}$ et $1 \leq l \leq m$ et on a

$$x = j^\epsilon \exp\left(\frac{2il\pi}{m}\right) = j^\epsilon \exp\left(\frac{4il\pi}{2m}\right) = j^\epsilon \zeta_{2m}^{2l} \in \mathcal{BD}_{2m}.$$

  Réciproquement, si $x = j^\epsilon \zeta_{2m}^l \in \mathcal{BD}_{2m}$, on a deux cas :
  - Si $l = 2u$ est pair, alors $x = j^\epsilon \zeta_m^u \in \mathcal{BD}_m$,
  - Si $l = 2u+1$ est impair, alors $x = j^\epsilon \exp\left(\frac{il\pi}{m}\right) = j^\epsilon \zeta_m^{u-n} j^2 \in \mathcal{BD}_m$,

  d'où $\mathcal{BD}_{2m} = \mathcal{BD}_m$.
* Si $m = 2n$ est pair, soit $x = j^\epsilon \zeta_m^l \in \mathcal{BD}_m$. On a ici trois cas :
  - Si $\epsilon = 0$, $x \in \mathcal{C}_m$ donc $x^2 \in \mathcal{C}_m$,
  - Si $\epsilon = 1$, $x^2 = \zeta_m^{-l} j^2 \zeta_m^l = -1 = \zeta_m^n \in \mathcal{C}_m$,
  - Si $\epsilon = -1$, $x^2 = j^{-1}\zeta_m^l j^{-1}\zeta_m^l = j^{-2} j \zeta_m^l j^{-1} \zeta_m^l = -1 \in \mathcal{C}_m$,

  donc tout $x \in \mathcal{BD}_{2m} \setminus \mathcal{C}_{2m}$ vérifie $x^2 = -1$ et on a

$$|\mathcal{BD}_{2m}| = 2|\mathcal{C}_{2m}| = 4m.$$

Enfin, on a

$$\mathcal{BD}_{2m} \Big/ \langle -1 \rangle \simeq \mathcal{D}_{2m},$$

par factorisation canonique de

$$\begin{array}{ccc} \mathcal{BD}_{2m} & \to & \mathcal{D}_{2m} \\ j & \mapsto & \sigma \\ \zeta_m & \mapsto & \omega \end{array}$$

en utilisant la présentation usuelle du groupe diédral $\mathcal{D}_{2m}$ d'ordre $2m$.

Définition 19. Un groupe isomorphe à un certain $\mathcal{BD}_{2m}$ est appelé groupe dicyclique (ou groupe diédral binaire), d'ordre $4m$.
De plus, les groupes $\mathcal{BD}_{2^m}$ sont appelés groupes quaternioniques.

Remarque 20. On peut donner une présentation de $\mathcal{BD}_{2m}$:

$$\mathcal{BD}_{2m} = \left\langle x, y \mid x^{2m} = 1, y^2 = x^m, y^{-1}xy = x^{-1} \right\rangle.$$

Le groupe $\mathcal{Q} := \{\pm 1, \pm i, \pm j, \pm k\}$ des quaternions est isomorphe à $\mathcal{BD}_4$.

Groupes polyédraux binaires Par le Lemme 10, on sait que deux éléments de $\mathbb{S}^3$ sont conjugués si et seulement s'ils ont même trace. Ainsi, l'ordre d'un élément de $\mathbb{S}^3$ ne dépend que de sa trace. En fait, on a

Proposition 11. *En notant $\tau := \frac{1}{2}(1+\sqrt{5})$, on a la correspondance suivante :*

Ordre	3	4	5	6	8	10
Trace	-1	0	$-\tau,\ \tau^{-1}$	1	$\pm\sqrt{2}$	$\tau,\ -\tau^{-1}$

TABLE 1

Démonstration. Pour l'ordre 3, si $o(q) = 3$, on a

$$q^2 - \mathrm{Tr}(q)q + 1 = 0 \ \Rightarrow\ q^3 - \mathrm{Tr}(q)q^2 + q = 0 \ \Rightarrow\ 1 - \mathrm{Tr}(q^2)q + \mathrm{Tr}(q) + q = 0$$

$$\Rightarrow\ 1 + \mathrm{Tr}(q) + q(1 - \mathrm{Tr}(q)^2) = 0 \ \Rightarrow\ \mathrm{Tr}(q)^2 = 1 \ \Rightarrow\ \mathrm{Tr}(q) = \pm 1$$

car $q \notin \mathbb{R}$ et donc $\mathrm{Tr}(q) = -1$. Réciproquement, si $\mathrm{Tr}(q) = -1$, alors $q^2 + q + 1 = 0$, d'où $q^3 + q^2 + q = 0$, donc $q^3 - q - 1 + q = 0$ et donc $q^3 = 1$.
Pour l'ordre 4, si $o(q) = 4$, on a

$$q^2 - \mathrm{Tr}(q)q + 1 = 0 \ \Rightarrow\ q^4 - \mathrm{Tr}(q)q^3 + q^2 = 0 \ \Rightarrow\ \mathrm{Tr}(q^2) + (2\mathrm{Tr}(q) - \mathrm{Tr}(q)^3)q = 0 \ \Rightarrow\ \mathrm{Tr}(q) = 0,$$

et si $\mathrm{Tr}(q) = 0$, alors $q^2 + 1 = 0$ et donc $o(q) = 4$.
Pour l'ordre 5, si $o(q) = 5$, on a

$$q^2 - \mathrm{Tr}(q)q + 1 = 0 \ \Rightarrow\ g^5 - \mathrm{Tr}(q)q^4 + q^3 = 0 \ \Rightarrow\ \mathrm{Tr}(q)^3 - 2\mathrm{Tr}(q) + 1 + q(3\mathrm{Tr}(q)^2 - \mathrm{Tr}(q)^4 - 1) = 0$$

$$\Rightarrow\ (\mathrm{Tr}(q) - 1)(\mathrm{Tr}(q)^2 + \mathrm{Tr}(q) - 1) = 0 \ \Rightarrow\ \mathrm{Tr}(q) \in \{-\tau, \tau^{-1}\}.$$

On peut conclure de la même façon que dans les cas précédents.
Pour l'ordre 6, si $o(q) = 6$, alors $o(q^2) = 3$, donc $\mathrm{Tr}(q^2) = -1$ et $\mathrm{Tr}(q^2) = \mathrm{Tr}(q)^2 - 2$ d'où $\mathrm{Tr}(q) \in \{\pm 1\}$ et donc $\mathrm{Tr}(q) = 1$.
Pour l'ordre 8, de même, si $o(q) = 8$, alors $o(q^2) = 4$, d'où $\mathrm{Tr}(q^2) = 0$, donc $\mathrm{Tr}(q)^2 = 2$ et donc $\mathrm{Tr}(q) \in \{\pm\sqrt{2}\}$. Pour la réciproque, on peut prendre $\pm\frac{1+i}{\sqrt{2}}$.
Enfin, pour l'ordre 10, si $o(q) = 10$, alors $o(q^2) = 5$, donc $\mathrm{Tr}(q^2) \in \{-\tau, \tau^{-1}\}$, d'où $\mathrm{Tr}(q)^2 \in \{\tau^{-1} + 2, 2 - \tau\} = \{\tau + 1, 1 - \tau^{-1}\} = \{\tau^2, \tau^{-2}\}$, donc $\mathrm{Tr}(q) \in \{\pm\tau, \pm\tau^{-1}\}$ et q étant d'ordre 10, ceci implique $\mathrm{Tr}(q) \in \{-\tau^{-1}, \tau\}$, d'où le résultat. □

∗ Posons

$$\mathcal{Q} := \langle i, j \rangle = \{\pm 1, \pm i, \pm j, \pm k\},$$

ainsi que

$$\varpi := \frac{-1 + i + j + k}{2}.$$

On a $\mathrm{Tr}(\varpi) = -1$, donc ϖ est d'ordre 3. De plus, $\varpi \in N_{\mathbb{S}^3}(\mathcal{Q})$ donc le groupe

$$\mathcal{T} := \langle \mathcal{Q}, \varpi \rangle$$

est d'ordre 24 et on a $\mathcal{T} \setminus \mathcal{Q} = \left\{\frac{1}{2}(\pm 1 \pm i \pm j \pm k)\right\}$ avec $|\mathcal{T} \setminus \mathcal{Q}| = 16$. En fait, on voit que

$$\mathcal{T} = \langle i, \varpi \rangle .$$

Le groupe $\mathcal{T}$ est appelé groupe tétraédral binaire.

∗ Soit

$$\gamma := \frac{1 + i}{\sqrt{2}}.$$

γ est d'ordre 8 et on a $\gamma^2 = i$. Par construction de $\mathcal{T}$, on a $\gamma \in N_{\mathbb{S}^3}(\mathcal{Q}) \cap N_{\mathbb{S}^3}(\mathcal{T})$ et alors le groupe octaédral binaire

$$\mathcal{O} := \langle \mathcal{T}, \gamma \rangle = \langle \varpi, \gamma \rangle$$

est d'ordre 48 et on a $\mathcal{O} \setminus \mathcal{T} = \left\{\frac{1}{\sqrt{2}}(\pm u \pm u),\ u \neq v \in \{1, i, j, k\}\right\}$ et donc $|\mathcal{O} \setminus \mathcal{T}| = 24$. De plus, 12 des éléments de $\mathcal{O} \setminus \mathcal{T}$ sont d'ordre 4 et les 12 autres sont d'ordre 8, d'après la Table 1.

∗ Posons

$$\sigma := \frac{\tau^{-1} + i + \tau j}{2}.$$

Par la Table 1, σ est d'ordre 5 et agit sur $\mathcal{P}$ via $S : \mathbb{S}^3 \to SO_3(\mathbb{R})$. Les douze vecteurs $\pm\tau i \pm j$, $\pm\tau j \pm k$, $\pm i \pm \tau k$ forment les sommets d'un icosaèdre régulier $\mathscr{I}$ de $\mathcal{P} \simeq \mathbb{R}^3$ et sont permutés entre eux par $S(q)$ pout $q \in \mathcal{T}$ et $S(\sigma)$. Il est clair que seuls ± 1 fixent les six droites vectorielles joignant deux points opposés, donc $\langle \mathcal{T}, \sigma \rangle = S^{-1}(\mathrm{Is}^+(\mathscr{I}))$, où $\mathrm{Is}^+(\mathscr{I})$ est le groupe des isométries vectorielles directes préservant $\mathscr{I}$ (cf Annexe), et donc comme $\ker S = \{\pm 1\}$, on a que le groupe

$$\mathcal{I} := \langle \mathcal{T}, \sigma \rangle$$

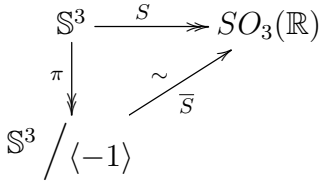
est fini. On l'appelle groupe icosaédral binaire.

Remarque 21. Les groupes $\mathcal{T}$, $\mathcal{O}$ et $\mathcal{I}$ sont ainsi nommés en raison du fait que leurs images dans $SO_3(\mathbb{R})$ sont les groupes de rotations du tétraèdre, octaèdre et icosaèdre, respectivement.

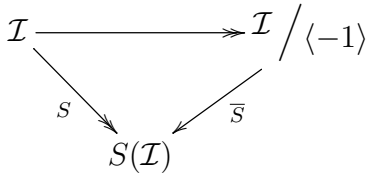
Contrairement aux cas de $\mathcal{T}$ et $\mathcal{O}$, l'ordre du groupe $\mathcal{I}$ n'est pas aisé à déterminer. Son calcul mérite un lemme :

Lemme 11. *Rappelons que $\mathcal{T}$ est d'ordre 12 et que $\mathcal{O}$ est d'ordre 48. De plus, le groupe icosaédral binaire $\mathcal{I}$ est d'ordre 120.*

Démonstration. (Voir [15], Chapter 5, §4.2)
Rappelons que l'on a le diagramme



dont on tire le diagramme



et donc $|\mathcal{I}| = 2|S(\mathcal{I})|$. Il s'agit donc de montrer que $|S(\mathcal{I})| = 60$. Comme $S(\mathcal{I})$ est formé d'isométries préservant l'icosaèdre régulier $\mathscr{I}$ défini ci-dessus, $S(\mathcal{I})$ agit sur les diagonales de $\mathscr{I}$ et on a donc un morphisme

$$S(\mathcal{I}) \to \mathfrak{S}_6.$$

De plus, ce morphisme est injectif car si $S(g) \in S(\mathcal{I})$ fixe toutes les diagonales de $\mathscr{I}$, alors $g \in \{\pm 1\}$ et donc $S(g) = 1$. Ensuite, toute isométrie de $S(\mathcal{I})$ étant directe, elle conserve l'orientation, donc les premutations correspondantes sont paires. Ceci donne un morphisme injectif

$$S(\mathcal{I}) \hookrightarrow \mathfrak{A}_6.$$

Ensuite, on a $\sigma \notin \mathcal{T}$, d'où $|\mathcal{I}| = |\langle \mathcal{T}, \sigma \rangle| \geq 5|\mathcal{T}| = 120$, d'où $|S(\mathcal{I})| \geq 60 > 45$, donc $[\mathfrak{A}_6 : S(\mathcal{I})] < 8$ et donc $[\mathfrak{A}_6 : S(\mathcal{I})] \leq 6$. Il reste à montrer que l'on a exactement $[\mathfrak{A}_6 : S(\mathcal{I})] = 6$. Comme $|\mathfrak{A}_6| = 360$, on a

$$[\mathfrak{A}_6 : S(\mathcal{I})] \in \{1, 2, 3, 4, 5, 6\}.$$

Si $[\mathfrak{A}_6 : S(\mathcal{I})] = 2$, alors $S(\mathcal{I})$ est distingué dans $\mathfrak{A}_6$ et $|S(\mathcal{I})| \in \{1, 360\}$ car $\mathfrak{A}_6$ est simple, ce qui est absurde.
Ensuite, faisons agir $\mathfrak{A}_6$ sur $\mathfrak{A}_6 \Big/ S(\mathcal{I})$ par translation. L'action est fidèle et donne un morphisme injectif

$$\mathfrak{A}_6 \hookrightarrow \mathfrak{S}\left(\mathfrak{A}_6 \Big/ S(\mathcal{I})\right) \simeq \mathfrak{S}_{[\mathfrak{A}_6 : S(\mathcal{I})]}.$$

Donc, si $[\mathfrak{A}_6 : S(\mathcal{I})] = 3$ (resp. $4, 5$), alors $\mathfrak{A}_6$ s'identifie à un sous-groupe de $\mathfrak{S}_3$ (resp. $\mathfrak{S}_4, \mathfrak{S}_5$), donc 360 divise 6 (resp. $24, 120$), ce qui est impossible.
Ainsi, $[\mathfrak{A}_6 : S(\mathcal{I})] \in \{1, 6\}$ et il reste alors à montrer que $S(\mathcal{I}) \neq \mathfrak{A}_6$. Supposons le contraire ; alors $S(\mathcal{I})$ contient un sous-groupe non-cyclique d'ordre 9 (car $\langle (1,2,3), (4,5,6) \rangle \leq \mathfrak{A}_6$ est un tel sous-groupe) et on peut alors choisir $q, r \in \mathcal{I}$ distincts qui commutent et tels que $q, r, qr = rq$ soit d'ordre 3. Par la Proposition 11, on a alors $\mathrm{Tr}(q) = \mathrm{Tr}(r) = \mathrm{Tr}(rq) = -1$. Ainsi, q, r s'écrivent $q = -\frac{1}{2} + u$ et $r = -\frac{1}{2} + v$ avec $u, v \in \mathcal{P}$ qui commutent et de norme $\frac{3}{4}$. Alors, on a

$$-1 = \mathrm{Tr}(qr) = \frac{1}{2} + \mathrm{Tr}(uv) \;\Rightarrow\; \mathrm{Tr}(uv) = -\frac{3}{2} \;\Rightarrow\; uv = -\frac{3}{2},$$

car $uv \in \mathbb{R}$ puisque $\overline{uv} = \overline{v}\,\overline{u} = vu = uv$ d'où

$$\mathrm{N}(u - v) = (u - v)(\overline{u} - \overline{v}) = (u - v)(v - u) = uv + vu - u^2 - v^2 = 0 \;\Rightarrow\; u = v \;\Rightarrow\; q = r,$$

et c'est une contradiction qui nous permet de conclure. □

Poursuivons un peu l'étude des groupes polyédraux binaires. On a le résultat fondamental suivant :

Proposition 12. *On a*

$$Z(\mathcal{T}) = Z(\mathcal{O}) = Z(\mathcal{I}) = \langle -1 \rangle = \{\pm 1\},$$

ainsi que les isomorphismes

$$\mathcal{T} \Big/ Z(\mathcal{T}) \simeq \mathfrak{A}_4, \quad \mathcal{O} \Big/ Z(\mathcal{O}) \simeq \mathfrak{S}_4, \quad \mathcal{I} \Big/ Z(\mathcal{I}) \simeq \mathfrak{A}_5.$$

Démonstration. 1. Montrons que

$$\mathcal{T} \Big/ \langle -1 \rangle \simeq \mathfrak{A}_4.$$

On considère pour cela le sous-groupe $\Omega := \langle \varpi \rangle$ d'ordre 3. On a alors

$$[\mathcal{T} : N_{\mathcal{T}}(\Omega)] = 4.$$

En effet, $\mathcal{T}$ est d'ordre $24 = 2^4 \times 3$ et ϖ est d'ordre 3, donc $\Omega \in \mathrm{Syl}_3(\mathcal{T})$. Si $n_3 := |\mathrm{Syl}_3(\mathcal{T})|$, la théorie de Sylow nous affirme que $n_3 \equiv 1 \pmod 3$ et $n_3 | 8$ donc $n_3 \in \{1, 4\}$. Mais, $i \notin N_{\mathcal{T}}(\Omega)$ donc Ω n'est pas distingué dans $\mathcal{T}$ et donc $n_3 = 4$. Or, par le lemme des orbites (ou le quatrième théorème de Sylow), on a

$$4 = n_3 = [\mathcal{T} : N_{\mathcal{T}}(\Omega)],$$

ce que l'on voulait. Au passage, notons que $-\varpi \in N_{\mathcal{T}}(\Omega)$ et $-\varpi$ étant d'ordre 6, on a

$$N_{\mathcal{T}}(\Omega) \simeq \mathbb{Z} / 6\mathbb{Z}.$$

En considérant l'action par translation de $\mathcal{T}$ sur $\mathcal{T} \Big/ N_{\mathcal{T}}(\Omega)$, on obtient un morphisme

$$\varphi : \mathcal{T} \to \mathfrak{S}_4.$$

Par calculs directs, on a $\varphi(i) = (1,2)(3,4)$ et $\varphi(\varpi) = (2,3,4)$, donc $\varphi(i\varpi^{-1}) = (1,2,3)$ et d'après le théorème 2 de l'Annexe, on en déduit que $\mathfrak{A}_4 \leq \operatorname{im}\varphi$ et donc que $\operatorname{im}\varphi \in \{\mathfrak{A}_4, \mathfrak{S}_4\}$. Or, $-1 \in \ker\varphi$, donc φ ne peut être injectif et pour des raisons d'ordre, on a donc $\operatorname{im}\varphi \neq \mathfrak{S}_4$. On en déduit que $\operatorname{im}\varphi = \mathfrak{A}_4$, donc $\ker\varphi = \langle -1 \rangle$ et l'isomorphisme désiré s'ensuit.

2. Montrons que

$$\mathcal{O} \Big/ \langle -1 \rangle \simeq \mathfrak{S}_4.$$

On note là encore $\Omega := \langle \varpi \rangle$. On a

$$[\mathcal{O} : N_{\mathcal{O}}(\Omega)] = 4.$$

En effet, on peut procéder comme précédemment et écrire $|\mathcal{O}| = 48 = 2^4 \times 3$ pour avoir $\Omega \in \mathrm{Syl}_3(\mathcal{O})$. Si $n_3 := |\mathrm{Syl}_3(\mathcal{O})|$, on a $n_3 \equiv 1 \pmod 3$ et $n_3 | 16$ d'où $n_3 \in \{1, 4, 16\}$. Ω n'étant pas distingué dans $\mathcal{T}$, il ne l'est pas non plus dans $\mathcal{O}$, et $n_3 \in \{4, 16\}$. Or, on a $N_{\mathcal{T}}(\Omega) < N_{\mathcal{O}}(\Omega)$, donc

$$n_3 = [\mathcal{O} : N_{\mathcal{O}}(\Omega)] \leq [\mathcal{O} : N_{\mathcal{T}}(\Omega)] = 8 \;\Rightarrow\; [\mathcal{O} : N_{\mathcal{O}}(\Omega)] = n_3 = 4.$$

$\mathcal{O}$ agit sur $\mathcal{O}\Big/N_{\mathcal{O}}(\Omega)$ et donne un morphisme

$$\psi : \mathcal{O} \to \mathfrak{S}_4.$$

Cependant, par calculs directs, on a $\psi(\varpi) = (2,3,4)$, $\psi(i) = (1,3)(2,4)$ et $\psi(\gamma) = (1,2,3,4)$, d'où $\psi(i\varpi^{-1}\gamma\varpi) = (1,2)$ et donc $\operatorname{im}\psi$ contient $\langle (1,2),(1,2,3,4)\rangle = \mathfrak{S}_4$ (cf Annexe, théorème 1) et donc ψ est surjectif. De plus, on a $\{\pm 1\} \subset \ker\psi$ et $|\operatorname{im}\psi| = 24$ entraîne que $|\ker\psi| = 2$, d'où le résultat.

3. Montrons que
$$\mathcal{I}\Big/\langle -1\rangle \simeq \mathfrak{A}_5.$$
On a ici $|\mathcal{T}| = 24$, donc $[\mathcal{I} : \mathcal{T}] = 5$ et $\mathcal{I}$ agit sur $\mathcal{I}/\mathcal{T}$ et ceci donne un morphisme
$$\chi : \mathcal{I} \to \mathfrak{S}_5.$$
Par calculs, on a là aussi $\chi(\sigma) = (1,2,3,4,5)$ et $\chi(i) = (2,3)(4,5)$, donc $\chi(\sigma^2 i \sigma^3 i) = (1,2,3)$ et par le théorème 2 de l'Annexe montre alors que $\mathfrak{A}_5 \leq \operatorname{im}\chi$ et donc $\operatorname{im}\chi \in \{\mathfrak{A}_5, \mathfrak{S}_5\}$. Or, si $\operatorname{im}\chi = \mathfrak{S}_5$, alors on aurait $|\mathcal{I}| = 120 = |\mathfrak{S}_5|$, donc χ serait un isomorphisme et contredirait $-1 \in \ker\chi$. Ainsi, $\operatorname{im}\chi = \mathfrak{A}_5$ et $\ker\chi = \langle -1\rangle$ et on a bien l'isomorphisme voulu.
4. Calculons enfin les centres. Si $q \in Z(\mathcal{T})$, alors q commute à i, donc s'écrit $q = a + bi$ avec a, b réels. Mais q commute également à ϖ, ce qui n'est pas le cas de i et donc $q \in \mathbb{R}$ et comme $q \in \mathbb{S}^3$, on obtient bien $q \in \{\pm 1\}$. Réciproquement, on a clairement $\{\pm 1\} \subset Z(\mathcal{T})$. De plus, si $q \in Z(\mathcal{O})$ (resp. $q \in Z(\mathcal{I})$), alors q commute à tout élément de $\mathcal{T}$, donc en particulier à ϖ et i et par ce qui précède, ceci implique $q = \pm 1$ et donc $Z(\mathcal{O}) = Z(\mathcal{I}) = \{\pm 1\}$.

□

Nous en arrivons donc aux deux résultats principaux de cette partie. Rappelons au préalable un résultat central démontré en Annexe (théorème 4) :

Théorème 14. *Tout sous-groupe fini de $SO_3(\mathbb{R})$ est conjugué (dans $SO_3(\mathbb{R})$) à l'un des groupes suivants :*

* *Le groupe cyclique $\mathcal{C}_m$ d'ordre m engendré par*
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(4\pi/m) & -\sin(4\pi/m) \\ 0 & \sin(4\pi/m) & \cos(4\pi/m) \end{pmatrix},$$
* *Le groupe diédral $\mathcal{D}_{2m}$ d'ordre $2m$ engendré par*
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(4\pi/m) & -\sin(4\pi/m) \\ 0 & \sin(4\pi/m) & \cos(4\pi/m) \end{pmatrix} \quad \textit{et} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$
* *Le groupe tétraédral $\mathrm{Is}^+(\mathscr{T}) \simeq \mathfrak{A}_4$ engendré par*
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \textit{et} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

∗ *Le groupe octaédral* $\mathrm{Is}^+(\mathscr{O}) \simeq \mathfrak{S}_4$ *engendré par*

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix},$$

∗ *Le groupe icosaédral* $\mathrm{Is}^+(\mathscr{I}) \simeq \mathfrak{A}_5$ *engendré par*

$$\frac{1}{2}\begin{pmatrix} 1 & \tau & \tau^{-1} \\ \tau & -\tau^{-1} & -1 \\ -\tau^{-1} & 1 & -\tau \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad avec \quad \tau := \frac{1+\sqrt{5}}{2}.$$

Théorème 15. *(Théorème de Stringham-Coxeter)*
Tout sous-groupe fini G *de* $\mathbb{H}^\times$ *est conjugué dans* $\mathbb{S}^3$ *à l'un des groupes suivants :*

∗ *Le groupe cyclique* $\mathcal{C}_m$ *d'ordre* m*,*

∗ *Le groupe dicyclique* $\mathcal{BD}_{2m}$ *d'ordre* $4m$*,*

∗ *Le groupe tétraédral binaire* $\mathcal{T}$*,*

∗ *Le groupe octaédral binaire* $\mathcal{O}$*,*

∗ *Le groupe icosaédral binaire* $\mathcal{I}$*.*

Démonstration. (Voir [13]. On pourra aussi consulter [15] pour une preuve directe)
Soit $G < \mathbb{H}^\times$ un tel sous-groupe. Alors, $G < \mathbb{S}^3$. Si G est cyclique, G est conjugué dans $\mathbb{S}^3$ à $\langle \zeta_m \rangle = \mathcal{C}_m$. Soit en effet $q \in G$ d'ordre m. Il s'agit de montrer qu'il existe $\alpha \in \mathcal{C}_m$ tel que $\mathrm{Tr}(\alpha) = \mathrm{Tr}(q)$. Pour le voir, on a $|\mathrm{Tr}(q)| \leq 2$, donc il existe $\theta \in \mathbb{R}$ tel que $\mathrm{Tr}(q) = 2\cos\theta$ et si $x := \exp(i\theta) \in \mathbb{S}^3$, alors $\mathrm{Tr}(q) = \mathrm{Tr}(x)$, donc $x^m = 1$ et donc $\cos(m\theta) = 1$ et il existe alors $k \in \mathbb{Z}$ tel que $m\theta = 2k\pi$ et $\alpha := \zeta_m^k$ convient.
Sinon, G est d'ordre pair car si $|G|$ est impair, alors $G \simeq S(G) < SO_3(\mathbb{R})$ et les seuls sous-groupes de $SO_3(\mathbb{R})$ d'ordre impair sont cycliques. Le seul élément d'ordre 2 de $\mathbb{S}^3$ est -1, donc $\{\pm 1\} < G$ et $S(G)$ est alors conjugué à $\mathcal{D}_{2m}$, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$. Ainsi, on vérifie que $G = S^{-1}(S(G))$ et si $S(G)$ est conjugué à $H \in \{\mathcal{D}_{2m}, \mathfrak{A}_4, \mathfrak{S}_4, \mathfrak{A}_5\}$, alors $G = S^{-1}(S(G))$ est conjugué dans $\mathbb{S}^3$ à $S^{-1}(H) \in \{\mathcal{BD}_{2m}, \mathcal{T}, \mathcal{O}, \mathcal{I}\}$, d'où le résultat. □

En utilisant le Théorème 12, on obtient finalement :

Corollaire 14. *Tout sous-groupe fini de* $SU_2(\mathbb{C})$ *est conjugué dans* $SU_2(\mathbb{C})$ *à l'un des groupes suivants :*

∗ *Le groupe cyclique* $\mathcal{C}_m$ *d'ordre* m *engendré par*

$$\begin{pmatrix} e^{\frac{2i\pi}{m}} & 0 \\ 0 & e^{-\frac{2i\pi}{m}} \end{pmatrix},$$

∗ *Le groupe diédral binaire* $\mathcal{BD}_{2m}$ *d'ordre* $4m$ *engendré par*

$$\begin{pmatrix} e^{\frac{i\pi}{m}} & 0 \\ 0 & e^{-\frac{i\pi}{m}} \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

∗ *Le groupe tétraédral binaire* $\mathcal{T}$ *d'ordre* 24 *engendré par*

$$\frac{1}{2}\begin{pmatrix}-1-i & 1-i\\ -1-i & -1+i\end{pmatrix} \qquad \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix},$$

∗ *Le groupe octaédral binaire* $\mathcal{O}$ *d'ordre* 48 *engendré par*

$$\frac{1}{2}\begin{pmatrix}-1-i & 1-i\\ -1-i & -1+i\end{pmatrix} \qquad \frac{1}{\sqrt{2}}\begin{pmatrix}1-i & 0\\ 0 & 1+i\end{pmatrix},$$

∗ *Le groupe icosaédral binaire* $\mathcal{I}$ *d'ordre* 120 *engendré par*

$$\frac{1}{2}\begin{pmatrix}\tau^{-1}-\tau i & 1\\ -1 & \tau^{-1}+\tau i\end{pmatrix} \qquad \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}.$$

Le premier générateur de $\mathcal{I}$ ci-dessus correspond au conjugué de σ par $\frac{1}{\sqrt{2}}(i+j)$. Enfin, notons que l'on a deux isomorphismes exceptionnels :

Proposition 13. *On a*

$$\mathcal{I} \simeq SL_2(\mathbb{F}_5) \quad \textit{et} \quad \mathcal{T} \simeq SL_2(\mathbb{F}_3).$$

Démonstration. (Voir [15], Chapter 5, §5.1)

1. Dans $\mathbb{F}_5$, on a

$$X^2+1=(X-2)(X-3) \text{ et } X^2-X-1=(X-3)^2,$$

ce qui nous donne un morphisme

$$\begin{array}{rccc}\varphi & : & \mathbb{Z}[i,\tau] & \to & \mathbb{F}_5\\ & & i,\tau & \mapsto & 3\end{array}$$

Notons que l'on a $\varphi(2)\neq 0$. On a aussi une suite exacte courte

$$1 \longrightarrow \langle -1\rangle \longrightarrow \mathcal{I} \xrightarrow{\pi} \mathfrak{A}_5 \longrightarrow 1\,.$$

Définissons

$$\chi \;:\; \mathcal{I} \longrightarrow GL_2(\mathbb{Z}[i,\tau]) \xrightarrow{GL(\varphi)} GL_2(\mathbb{F}_5)$$

tel que

$$\chi(i)=GL(\varphi)\left(\begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix}\right)=\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix}$$

et

$$\chi(\sigma)=GL(\varphi)\left(\begin{pmatrix}\tau^{-1}-\tau i & 1\\ -1 & \tau^{-1}+\tau i\end{pmatrix}\right)=2^{-1}\begin{pmatrix}-2 & 1\\ -1 & 1\end{pmatrix}=\begin{pmatrix}4 & 3\\ 2 & 3\end{pmatrix}.$$

En fait, on voit que $\chi(\mathcal{I})\subset SL_2(\mathbb{F}_5)$. Ensuite, comme $\pi(\ker\chi)\trianglelefteq\mathfrak{A}_5$ et $\mathfrak{A}_5$ est simple, si $\pi(\ker\chi)=\mathfrak{A}_5$, comme $-1\notin\ker\chi$, il vient $\pi(\ker\chi)\simeq\ker\chi$, d'où $\pi(\ker\chi)=1$, donc $\ker\chi\subset\{\pm 1\}$ et on a $\ker\chi=1$. Pour des raisons d'ordre on en déduit que χ est un isomorphisme, ce que l'on voulait.

2. Comme le polynôme X^2+1 est irréductible sur $\mathbb{F}_3$, on a $\mathbb{F}_9 = \mathbb{F}_3(\theta)$ avec $\theta^2+1=0$, d'où un morphisme

$$\begin{array}{rccc} \psi & : & \mathbb{Z}[i,\tau] & \to & \mathbb{F}_9 \\ & & i & \mapsto & \theta \\ & & \tau & \mapsto & \theta+2 \end{array}$$

et comme précédemment, on obtient

$$\widetilde{\chi} \ : \ \mathcal{I} \longrightarrow GL_2(\mathbb{Z}[i,\tau]) \xrightarrow{GL(\psi)} SL_2(\mathbb{F}_9)$$

De plus, on a

$$\widetilde{\chi}(i) = GL(\psi)\left(\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\right) = \begin{pmatrix} -\theta & 0 \\ 0 & \theta \end{pmatrix}$$

et

$$\widetilde{\chi}(\varpi) = GL(\psi)\left(\frac{1}{2}\begin{pmatrix} -1-i & 1-i \\ -1-i & -1+i \end{pmatrix}\right) = \begin{pmatrix} \theta+1 & \theta-1 \\ \theta+1 & 1-\theta \end{pmatrix}.$$

Comme ci-dessus, on a $\pi(\ker\widetilde{\chi}) \trianglelefteq \mathfrak{A}_5$ et $-1 \notin \ker\widetilde{\chi}$ entraînent $\ker\widetilde{\chi} = 1$. Ainsi, $\widetilde{\chi}$ est injectif, donc

$$\mathcal{T} \simeq \widetilde{\chi}(\mathcal{T}) = \left\langle \begin{pmatrix} \theta+1 & \theta-1 \\ \theta+1 & 1-\theta \end{pmatrix}, \begin{pmatrix} -\theta & 0 \\ 0 & \theta \end{pmatrix} \right\rangle$$

$$\simeq \left\langle \begin{pmatrix} \theta+1 & \theta-1 \\ \theta+1 & 1-\theta \end{pmatrix}\begin{pmatrix} -\theta+1 & \theta+1 \\ -1 & \theta \end{pmatrix}, \begin{pmatrix} -\theta & 0 \\ 0 & \theta \end{pmatrix}\begin{pmatrix} -\theta+1 & \theta+1 \\ -1 & \theta \end{pmatrix} \right\rangle$$

$$= \left\langle \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq SL_2(\mathbb{F}_3),$$

et pour des raisons d'ordre, on a que $\widetilde{\chi} : \mathcal{T} \to SL_2(\mathbb{F}_3)$, d'où le résultat.

□

Remarque 22. On voit qu'ainsi, $\mathcal{T} \leq GL_2(\mathbb{F}_3)$ est d'indice 2 et $\mathcal{T}$ est aussi d'indice 2 dans $\mathcal{O}$. Cependant, $\mathcal{O}$ et $GL_2(\mathbb{F}_3)$ ne sont pas isomorphes car $\mathcal{O}$ contient un seul élément d'ordre 2, ce qui n'est pas le cas de $GL_2(\mathbb{F}_3)$. De plus, on peut montrer que $SL_2(\mathbb{F}_7)$ est le plus petit groupe de la forme $SL_2(\mathbb{F}_q)$ contenant $\mathcal{O}$.

Quatrième partie
Groupes primitifs de rang 2

4.1 Sous-groupes de réflexions primitifs de $U_2(\mathbb{C})$

Notons $I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U_2(\mathbb{C})$ et $\mathcal{C}_m := \langle \zeta_m I_2 \rangle \leq U_2(\mathbb{C})$. Par le Corollaire 12 et le Théorème 12, on a

$$U_2(\mathbb{C}) \simeq L(\mathbb{S}^1) \circ R(\mathbb{S}^3) \simeq L(\mathbb{S}^1) \circ SU_2(\mathbb{C}).$$

Rendons cette décomposition plus explicite :

Soit G un sous-groupe fini de $U_2(\mathbb{C})$. Pour $g \in G$, on peut choisir $\lambda_g \in \mathbb{C}$ tel que $\lambda_g^2 = \det g$. On pose alors

$$\widehat{G} := \{\pm\lambda_g^{-1} g,\ g \in G\}$$

et on a

Proposition 14. *Avec les notations précédentes, $\widehat{G}$ est un sous-groupe fini de $SU_2(\mathbb{C})$, G est un sous-groupe de $\mathcal{C}_m \circ \widehat{G}$ où m est un exposant de $\widehat{G}$ et on a*

$$G \Big/ Z(G) \simeq \widehat{G} \Big/ Z(\widehat{G}).$$

Démonstration. Pour $g \in G$, on a $\det(\pm\lambda_g^{-1} g) = \lambda_g^{-2} \det g = 1$, donc $\widehat{G}$ est bien un sous-groupe de $SU_2(\mathbb{C})$, fini car G est fini. Soit m un exposant de $\widehat{G}$. Pour $g \in G$, on a $\lambda_g^m I_2 = g^m = (-1)^m \lambda_g^m I_2$, donc m est pair. On en déduit que si $g \in G$, on a

$$I_2 = (\pm\lambda_g g)^m = \lambda_g^m g^m = \lambda_g^{2m} I_2 \ \Rightarrow\ \lambda_g^{2m} = 1 \ \Rightarrow\ \lambda_g^m \in \{\pm 1\},$$

d'où un morphisme

$$G \to (\mathcal{C}_m \times \widehat{G}) \Big/ \{\pm(1,1)\} \overset{\text{def}}{=} \mathcal{C}_m \circ \widehat{G},$$

injectif car si $(\lambda_g, \lambda_g^{-1} g) = \pm(1,1)$, alors $g = 1$ et G est isomorphe à un sous-groupe de $\mathcal{C}_m \circ \widehat{G}$. De plus, on a un morphisme

$$\begin{array}{ccccc} G & \to & \widehat{G} & \to & \widehat{G} \Big/ Z(\widehat{G}) \\ q & \mapsto & \lambda_g^{-1} g & \mapsto & \overline{\lambda_g^{-1} g} \end{array}$$

surjectif car $\{\pm 1\} \leq Z(\widehat{G})$ et de noyau $Z(G)$, d'où l'isomorphisme annoncé. □

Proposition-Définition 4. *Si G est primitif, alors $\widehat{G}$ est conjugué à $\mathcal{T}$, $\mathcal{O}$ ou $\mathcal{I}$. On dit alors que G est de type $\mathcal{T}$, $\mathcal{O}$ ou $\mathcal{I}$ suivant que $\widehat{G}$ est conjugué à $\mathcal{T}$, $\mathcal{O}$ ou $\mathcal{I}$.*

Démonstration. Comme $\widehat{G}$ est un sous-groupe fini de $SU_2(\mathbb{C})$, $\widehat{G}$ est conjugué à un $\mathcal{C}_n$, un $\mathcal{BD}_{2n}$, $\mathcal{T}$, $\mathcal{O}$ ou $\mathcal{I}$ par le Théorème de Stringham-Coxeter (Théorème 15).

Si $\widehat{G} = \mathcal{C}_n$, alors $G \leq \mathcal{C}_m \circ \mathcal{C}_n$. Comme G est primitif, $\mathcal{C}_m \circ \mathcal{C}_n$ l'est aussi et comme $\mathcal{C}_m \circ \mathcal{C}_n$ est un sous-groupe distingué abélien de $\mathcal{C}_m \circ \widehat{G}$, il est cyclique par le Théorème 5, donc G est cyclique, disons engendré par g_0. Soit λ une valeur propre de g_0. Si l'espace propre associé est de dimension 1, alors G n'est pas irréductible, donc ne saurait être primitif. Ainsi, $g_0 = \lambda I_2$ est une homothétie et $\lambda \in \mathbb{S}^1$ et alors $\mathbb{C}\lambda$ est G-stable, donc G n'est pas irréductible. Cette contradiction indique que $\widehat{G}$ n'est pas cyclique.

Si $\widehat{G} = \mathcal{BD}_{2n}$, alors $\mathcal{C}_m \circ \mathcal{C}_{2n}$ est un sous-groupe distingué abélien de $\mathcal{C}_m \circ \mathcal{BD}_{2n}$, donc $\mathcal{C}_m \circ \mathcal{C}_{2n} \leq Z(\mathcal{C}_m \circ \mathcal{BD}_{2n})$. Ceci implique que ζ_{2n} et j commutent, ce qui est absurde.

Finalement, $\widehat{G}$ ne peut être conjugué qu'à $\mathcal{T}$, $\mathcal{O}$, ou $\mathcal{I}$. □

Théorème 16. *Si G est un sous-groupe de réflexions primitif de $U_2(\mathbb{C})$, alors (à conjugaison près), G est un sous-groupe distingué de $\mathcal{C}_{12} \circ \mathcal{T}$, de $\mathcal{C}_{24} \circ \mathcal{O}$ ou de $\mathcal{C}_{60} \circ \mathcal{I}$, suivant que G est de type $\mathcal{T}$, $\mathcal{O}$ ou $\mathcal{I}$.*

Démonstration. Soient $g \in \widehat{G}$ et θ, θ^{-1} les valeurs propres de g. Si $g \neq \pm 1$, on a $\theta \neq \theta^{-1}$. Alors, θg et $\theta^{-1} g$ sont des réflexions de G, car d'ordre fini et fixant exactement une droite. De plus, si $r \in G$ est une réflexion de spectre $\{\lambda, \mu\}$ alors $\lambda_r^{-1} r \in \widehat{G}$ est de spectre $\{\lambda_r^{-1}\lambda, \lambda_r^{-1}\mu\}$ et comme $\lambda\mu = \det r = \lambda_r^2$, le spectre de $\lambda_r^{-1} r$ est $\{\lambda_r^{-1}\lambda, \lambda_r^{-1}\mu\}$. Donc, toute réflexion de G s'obtient de cette manière. On voit ainsi par calcul direct que G est un sous-groupe distingué de $\mathcal{C}_m \circ \widehat{G}$, où m est un exposant de $\widehat{G}$, et ce car G est engendré par des réflexions. Il reste à voir que 12, 24 et 60 sont les exposants respectifs de $\mathcal{T}$, $\mathcal{O}$ et $\mathcal{I}$. Par exemple, comme on a $\mathcal{T} \Big/ Z(\mathcal{T}) = \mathcal{T} \Big/ \langle -1 \rangle \simeq \mathfrak{A}_4$, pour $x \in \mathcal{T}$, on a $x^{12} \in \{\pm 1\}$ et si $x^{12} = -1$, alors x est d'ordre 24 et $\mathcal{T}$ serait cyclique, ce qui est faux, donc $x^{12} = 1$, pour tout $x \in \mathcal{T}$. On procède de même pour $\mathcal{O}$ et $\mathcal{I}$ pour obtenir le résultat. □

En posant

$$\mathbb{T} := \mathcal{C}_{12} \circ \mathcal{T}, \quad \mathbb{O} := \mathcal{C}_{24} \circ \mathcal{O}, \quad \mathbb{I} := \mathcal{C}_{60} \circ \mathcal{I},$$

le résultat précédent se reformule en disant qu'un sous-groupe de réflexions primitif de $U_2(\mathbb{C})$ est un sous-groupe distingué de $\mathbb{T}$, $\mathbb{O}$ ou $\mathbb{I}$, en fonction de son type.

Ensuite, on a

$$\mathbb{T} = \mathbb{O} \cap \mathbb{I}.$$

En effet, $\mathcal{O} \cap \mathcal{I} = \mathcal{T}$ car $\mathcal{T} \leq \mathcal{O} \cap \mathcal{I}$ puisque $\mathcal{O} = \langle \mathcal{T}, \gamma \rangle$, $\mathcal{I} = \langle \mathcal{T}, \sigma \rangle$ et l'ordre que $\mathcal{O} \cap \mathcal{I}$ divise 48 et 120, donc divise $24 = \operatorname{pgcd}(48, 120)$ et donc $24 = |\mathcal{T}| \leq |\mathcal{O} \cap \mathcal{I}| \leq 24$. De plus, si $\overline{(\zeta, x)} \in \mathbb{O} \cap \mathbb{I}$, l'ordre de ζ divise 24 et 60, donc divise $12 = \operatorname{pgcd}(24, 60)$, donc $\zeta \in \mathcal{C}_{12}$ et $x \in \mathcal{O} \cap \mathcal{I} = \mathcal{T}$, donc $\overline{(\zeta, x)} \in \mathbb{T}$. Réciproquement, si $\overline{(\zeta, x)} \in \mathbb{T}$, alors $x \in \mathcal{T} = \mathcal{O} \cap \mathcal{I}$ et $\zeta^{12} = 1$ donc $\zeta \in \mathcal{C}_{24} \cap \mathcal{C}_{60}$ et donc $\overline{(\zeta, x)} \in \mathbb{O} \cap \mathbb{I}$ et on en déduit bien l'égalité annoncée.

Le Théorème 16 implique donc que si G est un sous-groupe de réflexions primitif de $U_2(\mathbb{C})$, alors G est un sous-groupe distingué de $\mathbb{O}$ ou $\mathbb{I}$.

Remarque 23. Le Corollaire 4 nous donne :

$$|\mathbb{T}| = \frac{|\mathcal{C}_{12}||\mathcal{T}|}{2} = 12^2 = 144, \qquad |\mathbb{O}| = \frac{|\mathcal{C}_{24}||\mathcal{O}|}{2} = 24^2 = 576, \qquad |\mathbb{I}| = \frac{|\mathcal{C}_{60}||\mathcal{I}|}{2} = 60^2 = 3600.$$

On peut déduire du Théorème précédent que $GZ(H) = H$ où $H \in \{\mathbb{T}, \mathbb{O}, \mathbb{I}\}$. En effet, si par exemple $G \trianglelefteq \mathbb{T}$, on a $GZ(\mathbb{T}) \leq \mathbb{T}$ et

$$|GZ(\mathbb{T})| = \frac{|G|\ |Z(\mathbb{T})|}{\underbrace{|G \cap Z(\mathbb{T})|}_{\leq Z(G)}} \geq \frac{12\ |Z(G)|\ |Z(\mathbb{T})|}{|Z(G)|} = 12\ |Z(\mathbb{T})| = 144 = |\mathbb{T}|$$

et ce car $Z(\mathbb{T}) \simeq \mathcal{C}_{12}$, donc $|GZ(\mathbb{T})| = |\mathbb{T}|$ et donc $GZ(\mathbb{T}) = \mathbb{T}$. Les autres cas sont tout à fait analogues.

On voit alors que $g_1, g_2 \in G$ sont conjugués dans G si et seulement s'ils sont conjugués dans H, ce qui s'écrit encore

$$\forall g \in G,\ g^G = g^H.$$

Ainsi, pour déterminer les possibilités pour G, il suffit de trouver des générateurs de H, représentants de classes de conjugaison de sous-groupes cycliques de réflexions de H et ensuite, calculer la clôture normale (dans H) de tous les sous-ensembles de ces représentants.

En effet, si $G = \langle s_1, \ldots, s_m \rangle \trianglelefteq H$, avec s_i des réflexions de H et si $\{r_1, \ldots, r_n\}$ est un ensemble de générateurs de H, représentants de classes de conjugaison de sous-groupes cycliques engendrés par des réflexions de H, alors

$$\forall 1 \leq i \leq m,\ \exists 1 \leq k_i \leq n,\ s_i^H = r_{k_i}^H,$$

et alors

$$G = \langle s_1, \ldots, s_m \rangle = \left\langle s_1^G, \ldots, s_m^G \right\rangle = \left\langle s_1^H, \ldots, s_m^H \right\rangle = \left\langle r_{k_1}^H, \ldots, r_{k_m}^H \right\rangle.$$

Comme nous l'avons vu dans la preuve du Théorème 16, chaque $g \in H$ donne deux réflexions

$$\begin{cases} r_1 := \theta_1^{-1} g \\ r_2 := \theta_2^{-1} g \end{cases}$$

où θ_1, θ_2 sont les valeurs propres de g. De plus, si $z \in Z(H)$, z est scalaire car, par calculs aisés, on a

$$Z(\mathbb{T}) = \mathcal{C}_{12}, \quad Z(\mathbb{O}) = \mathcal{C}_{24}, \quad Z(\mathbb{I}) = \mathcal{C}_{60}.$$

Donc, g et gz donnent la même pair de réflexions. Ainsi, pour trouver les classes de conjugaison de réflexions de H, on obtient deux réflexions r_1, r_2 de chaque classe de conjugaison non triviale de $H \Big/ Z(H)$ et on regarde si r_1 et r_2 sont ou non conjuguées dans H.

4.2 Groupes de type $\mathcal{T}$

Nous avons à présent tous les ingrédients nécessaires à notre classification.

$\mathcal{T}$ est engendré par les matrices

$$a := \frac{1}{2}\begin{pmatrix} -1-i & 1-i \\ -1-i & -1+i \end{pmatrix} \quad \text{et} \quad b := \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

d'ordres respectifs 3 et 4 d'après le Corollaire 14 et les classes de conjugaison non triviales de

$$\mathbb{T} \Big/ Z(\mathbb{T}) \simeq \mathcal{T} \Big/ Z(\mathcal{T}) \simeq \mathfrak{A}_4$$

sont représentées par $\overline{a}$, $\overline{a}^2$ et $\overline{b}$. Comme b et $-b$ sont conjugués dans $\mathcal{T}$ (voir la définition de $\mathcal{T}$ plus haut), les réflexions ib et $-ib$ sont conjuguées dans $\mathbb{T}$. De plus, le polynôme caractéristique de a est $\chi_a(X) = X^2 + X + 1$, donc le spectre de a est $\{\omega, \omega^2\}$, où $\omega := \exp\left(\frac{2i\pi}{3}\right)$ et ωa, $\omega^2 a$ ne sont pas conjugués dans $\mathbb{T}$, sinon a et ωa le seraient et si $\omega a = tat^{-1}$ pour $t = \overline{(\zeta, q)} \in \mathbb{T}$, alors $\overline{(\omega, a)} = \omega a = \overline{(\zeta, g)}\overline{(1, a)}\overline{(\zeta^{-1}, g^{-1})} = \overline{(1, gag^{-1})}$, d'où $\omega = \pm 1$, ce qui est absurde.
De même, ωa^2 et $\omega^2 a^2$ ne sont pas conjugués dans $\mathbb{T}$. Ainsi, $\mathbb{T}$ possède cinq classes de conjugaison de réflexions représentées par

$$r := ib, \quad r_1 := \omega a, \quad r_2 := \omega a^2, \quad r_1^2 = \omega^2 a^2, \quad r_2^2 = \omega^2 a.$$

Leurs représentations matricielles sont alors

$$r = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad r_1 = \frac{\omega}{2}\begin{pmatrix} -1-i & 1-i \\ -1-i & -1+i \end{pmatrix} \quad r_2 = \frac{\omega}{2}\begin{pmatrix} -1+i & -1+i \\ 1+i & -1-i \end{pmatrix},$$

d'ordres respectifs 2, 3 et 3.

Comme la clôture normale de b dans $\mathcal{T}$ est le groupe $\mathcal{Q}_8$ des quaternions, la clôture normale de r dans $\mathbb{T}$ est le groupe imprimitif

$$\mathcal{C}_4 \circ \mathcal{Q}_8 \simeq G(4,2,2)$$

et c'est l'unique 2-sous-groupe de Sylow de $\mathbb{T}$.

Remarque 24. On voit que $\gamma = \frac{1+i}{\sqrt{2}}$ et $\varpi = \frac{1}{2}(-1+i+j+k)$ normalisent $\mathcal{Q}_8$, donc $\mathcal{Q}_8 \trianglelefteq \mathcal{O}$ et donc

$$G(4,2,2) = \mathcal{C}_4 \circ \mathcal{Q}_8 \trianglelefteq \mathcal{C}_{24} \circ \mathcal{O} = \mathbb{O}.$$

De plus, $\sigma = \frac{1}{2}(\tau^{-1} + i + \tau j)$ ne normalise pas $\mathcal{Q}_8$, donc $G(4,2,2)$ n'est pas distingué dans $\mathbb{I}$. Ainsi, $\mathbb{O}$ est le plus grand sous-groupe de réflexions primitif de $U_2(\mathbb{C})$ contenant $G(4,2,2)$ comme sous-groupe distingué.

Pour avoir $G \Big/ Z(G) \simeq \mathcal{T} \Big/ Z(\mathcal{T}) \simeq \mathfrak{A}_4$, G doit contenir $r_1^{\mathbb{T}}$ ou $r_2^{\mathbb{T}}$. Supposons en effet le contraire. Si $r_2^{2^{\mathbb{T}}} \subset G$, alors $r_2^2 \in G$ donc G contient

$$r_2^4 = (r_2^2)^2 = \omega^4 a^2 = \omega a^2 = r_2,$$

ce qui est exclus. De même, G ne peut contenir $r_1^{2^{\mathbb{T}}}$. Ainsi, la seule possibilité restante est $G = \left\langle r^{\mathbb{T}} \right\rangle = G(4,2,2)$ qui est imprimitif, contredisant la situation. Les seuls sous-groupes de réflexions primitifs de $\mathbb{T}$ sont alors les clôtures normales

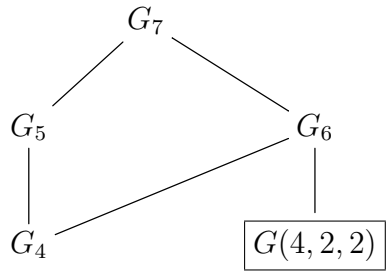
$$\left\langle r_1^{\mathbb{T}} \right\rangle, \quad \left\langle r_2^{\mathbb{T}} \right\rangle, \quad \left\langle r_1^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle \quad \left\langle r^{\mathbb{T}}, r_1^{\mathbb{T}} \right\rangle, \quad \left\langle r^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle, \quad \left\langle r^{\mathbb{T}}, r_1^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle.$$

Mais, on a $\gamma r_1^{\mathbb{T}} \gamma^{-1} = r_2^{\mathbb{T}}$ (ce qui reste vrai pour tout élément de $\mathbb{O} \setminus \mathbb{T}$) et donc, à conjugaison près, les seules possibilités restantes pour G sont

$$\begin{cases} G_4 := \left\langle r_1^{\mathbb{T}} \right\rangle \\ G_5 := \left\langle r_1^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle \\ G_6 := \left\langle r^{\mathbb{T}}, r_1^{\mathbb{T}} \right\rangle \\ G_7 := \left\langle r^{\mathbb{T}}, r_1^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle = \mathbb{T} \end{cases}$$

(on adopte ici la notation de Shephard-Todd, que l'on retrouve dans [15] et [19] naturellement.)

Avec ces définitions, on peut exhiber le treillis des sous-groupes de réflexions de $\mathbb{T}$:



(Le groupe $G(4,2,2)$ est encadré afin de rappeler qu'il est imprimitif.)

Définissons les réflexions d'ordre 3 suivantes :

$$r_1' := rr_1r = \frac{\omega}{2}\begin{pmatrix} -1-i & -1+i \\ 1+i & -1+i \end{pmatrix} \qquad r_2' := rr_2r = \frac{\omega}{2}\begin{pmatrix} -1+i & 1-i \\ -1-i & -1-i \end{pmatrix}.$$

Montrons que

$$G_5 = \langle r_1, r_2' \rangle, \quad |G_5| = 72, \quad |Z(G_5)| = 6.$$

Par définition, on a $G_5 = \left\langle r_1^{\mathbb{T}}, r_2^{\mathbb{T}} \right\rangle$ et posons $\Omega_5 := \left\langle a^{\mathcal{T}}, (a^2)^{\mathcal{T}} \right\rangle$, (rappelons que $\mathcal{T} = \langle a, b \rangle$). Comme

$$b^2a^2b^{-2} = b^2a^2b^2 = a^2 \in \left\langle a, ba^2b \right\rangle,$$

on a

$$\left\langle a, ba^2b \right\rangle \leq \Omega_5 \ \text{ et } \ \left\langle a, ba^2b \right\rangle \trianglelefteq \mathcal{T} \ \Rightarrow \ \Omega_5 = \left\langle a, ba^2b \right\rangle.$$

On en déduit que $G_5 = \langle r_1, rr_2r \rangle = \langle r_1, r_2' \rangle$. Ensuite, comme $r_1, r_2 \in G_5$, on a $\omega \in G_5$, d'où

$$\{(1, \pm 1), (\omega, \pm 1), (\omega^2, \pm 1)\} \subset Z(G_5) \ \Rightarrow \ |Z(G_5)| \geq 6 \ \Rightarrow \ |G_5| \geq 72,$$

cette dernière inégalité provenant de $G_5 \Big/ Z(G_5) \simeq \mathfrak{A}_4$. De plus, comme G_5 est un sous-groupe de $\mathbb{T}$, les possibilités restantes sont alors $|G_5| \in \{72, 144\}$ et si $|G_5| = 144$, alors $\Omega_5 = \mathcal{T}$ donc $b \in \langle a, ba^2b \rangle$, ce qui est faux. Ainsi, $|G_5| = 72$ et donc $|Z(G_5)| = \frac{72}{12} = 6$.

En suivant le même procédé (ou en utilisant la méthode de [15], Chapter 6, §2), on peut obtenir les générateurs et les ordres des groupes G_4, G_6 et G_7 ; informations que l'on peut récapituler dans la table suivante :

G	Structure	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$k[m]l$
G_4	$\langle r_1, r_1' \rangle \simeq SL_2(\mathbb{F}_3)$	24	2	3[3]3
G_5	$\langle r_1, r_2' \rangle \simeq \mathcal{C}_3 \times \mathcal{T}$	72	6	3[4]3
G_6	$\langle r, r_1 \rangle \simeq \mathcal{C}_4 \circ G_4$	48	4	2[6]3
G_7	$\langle r, r_1, r_2 \rangle \simeq \mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{T}) = \mathbb{T}$	144	12	$\emptyset$

TABLE 2 – Sous-groupes de $\mathbb{T}$

La notation $k[m]l$ indique que les générateurs donnés r et s sont d'ordres respectifs k et l et satisfont la "relation de tresses"

$$\underbrace{rsr\cdots}_{m} = \underbrace{srs\cdots}_{m}.$$

Autrement dit, on a une présentation

$$k[m]l := \left\langle r, s \mid r^k = 1, s^l = 1, \underbrace{rsr\cdots}_{m} = \underbrace{srs\cdots}_{m} \right\rangle.$$

Ces groupes sont appelés groupes de Shephard.

Remarque 25. On peut montrer (voir [10]) que le groupe abstrait $k[m]l$ est fini si et seulement si $(k+l)m > kl(m-2)$, auquel cas son ordre est

$$\frac{8}{m}\left(\frac{1}{k}+\frac{2}{m}+\frac{1}{l}-1\right)^{-2}.$$

De plus, on voit que $2[m]2$ est le groupe diédral $G(m,m,2)$ d'ordre $2m$ et que $2[4]m \simeq G(m,1,2)$. Enfin, on peut montrer (voir [15]) que les groupes $k[m]l$ sont exactement les sous-groupes de réflexions de $U_2(\mathbb{C})$ qui peuvent être engendrés par deux réflexions.

4.3 Groupes de type $\mathcal{O}$

Nous allons procéder ici de façon similaire à ce qui précède ; mais nous verrons quelques difficultés supplémentaires apparaître.

Le groupe $\mathcal{O}$ est engendré par

$$a := \frac{1}{2}\begin{pmatrix}-1-i & 1-i\\ -1-i & -1+i\end{pmatrix} \quad \text{et} \quad c := \frac{1}{\sqrt{2}}\begin{pmatrix}1-i & 0\\ 0 & 1+i\end{pmatrix}$$

d'ordres respectifs 3 et 8. Les classes de conjugaison non triviales de $\mathcal{O}\Big/Z(\mathcal{O}) \simeq \mathfrak{S}_4$ sont représentées par $\overline{a}$, $\overline{b}$, $\overline{c}$ et $\overline{d}$ où $b := c^2$, $d := c^3a^2c^2 = \frac{1}{\sqrt{2}}(i-k)$, de matrice $\frac{i}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}$, de telle sorte que $d^{-1}ad = a^{-1}$. On peut faire correspondre $\overline{a},\overline{b},\overline{c},\overline{d}$ aux permutations $(1,2,3),(1,3)(2,4),(1,2,3,4),(2,3)$ dans $\mathfrak{S}_4$.

On sait déjà que ib et $-ib$ sont conjugués dans $\mathbb{T}$. De même, d et $-d$ sont conjugués (par j) dans $\mathcal{O}$, donc id et $-id$ sont conjugués dans $\mathbb{O}$. $\mathbb{O}$ possède donc six classes de conjugaison de réflexions représentées par ib, ωa, $\omega^2 a$, id, $\frac{1-i}{\sqrt{2}}c$ et $\frac{1+i}{\sqrt{2}}c$.

Or, on a vu que $r_1 = \omega a$ et $r_2 = \omega a^2$ sont conjugués dans $\mathbb{O}$ et comme $\omega^2 a = r_2^2$, un sous-groupe de réflexions primitif de $\mathbb{O}$ contient $(\omega a)^{\mathbb{O}}$ si et seulement s'il contient $(\omega^2 a)^{\mathbb{O}}$. De même, un tel sous-groupe contient $\left(\frac{1+i}{\sqrt{2}}c\right)^{\mathbb{O}}$ ei et seulement s'il contient $\left(\frac{1-i}{\sqrt{2}}c\right)^{\mathbb{O}}$. Ainsi, $\mathbb{O}$ a quatre classes de conjugaison de sous-groupes cycliques de réflexions, représentées par

$$r = ib, \quad r_1 = \omega a, \quad r_3 := id, \quad r_4 := \frac{1+i}{\sqrt{2}}c,$$

de matrices

$$r = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \quad r_1 = \frac{\omega}{2}\begin{pmatrix}-1-i & 1-i\\ -1-i & -1+i\end{pmatrix}, \quad r_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix}, \quad r_4 = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}.$$

Lemme 12. *Pour avoir* $G\Big/Z(G) \simeq \mathcal{O}\Big/Z(\mathcal{O}) \simeq \mathfrak{S}_4$, *$G$ doit contenir $r_3^{\mathbb{O}}$ ou $r_4^{\mathbb{O}}$.*

Démonstration. En effet, sinon G ne contient que $r^{\mathbb{O}}$ ou $r_1^{\mathbb{O}}$, c'est-à-dire que

$$G \in \left\{ \left\langle r^{\mathbb{O}} \right\rangle,\ \left\langle r_1^{\mathbb{O}} \right\rangle,\ \left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle \right\}.$$

Éliminons ces cas les uns après les autres.

- Supposons que $G = \left\langle r_1^{\mathbb{O}} \right\rangle$. Alors $a, cac^{-1} \in \left\langle a^{\mathcal{O}} \right\rangle$, donc $\Omega_G := \langle a, cac^{-1} \rangle \leq \left\langle a^{\mathcal{O}} \right\rangle$. Mais, $c^2ac^{-2} = (cac^{-1})a(ca^2c^{-1}) \in \Omega_G$, donc $\Omega_G \trianglelefteq \mathcal{O}$ car $\mathcal{O} = \langle c, a \rangle$, d'où $\Omega_G = \left\langle a^{\mathcal{O}} \right\rangle$. De même, on obtient
$$G = \left\langle r_1, r_4 r_1 r_4^{-1} \right\rangle.$$
De plus, $r_2 = r_3 r_1 r_3^{-1} \in G$, donc $a \in G$ et donc $\omega \in G$ et comme $-1 = (acac^{-1})^2$, il vient
$$\{\overline{(1, \pm 1)}, \overline{(\omega, \pm 1)}, \overline{(\omega^2, \pm 1)}\} \subset Z(G).$$
On en déduit que $|Z(G)| \geq 6$ et comme $G \Big/ Z(G) \simeq \mathfrak{S}_4$, on a $|G| \geq 144$ et donc
$$|G| \in \{144, 288, 576\}.$$
Si $|G| = 576$, on a $G = \mathbb{O}$, donc $r_3 \in G$ et ceci est manifestement exclus. Si $|G| = 288$, alors G est d'indice 2 dans $\mathbb{O}$, donc $r = r_4^2 \in G$ et c'est également impossible. Si $|G| = 144$, G est d'indice 4 dans $\mathbb{O}$, donc $\zeta_6 = \zeta_{24}^4 \in G$, donc $Z(G) = \left\langle \overline{(\zeta_6, 1)} \right\rangle$. Notons
$$p_1 : \mathcal{C}_{24} \times \mathcal{O} \twoheadrightarrow \mathcal{C}_{24}, \quad p_2 : \mathcal{C}_{24} \times \mathcal{O} \twoheadrightarrow \mathcal{O}, \quad \pi : \mathcal{C}_{24} \times \mathcal{O} \twoheadrightarrow \mathbb{O},$$
les flèches naturelles. On a $\Omega_G = p_2(\pi^{-1}(G))$ et comme $Z(G) = \left\langle \overline{(\zeta_6, 1)} \right\rangle$, l'application $\overline{(\zeta_6, 1)} \mapsto \zeta_6$ est un isomorphisme $Z(G) \to p_1(\pi^{-1}(Z(G)))$. De plus, on a clairement que $p_1(\pi^{-1}(Z(G)))$ est un sous-groupe de $p_1(\pi^{-1}(G))$. Si $x = p_1(x, y)$ avec $\overline{(x, y)} \in G$, alors $x = p_1(x, 1)$ et comme $G = \left\langle r_1, r_4 r_1 r_4^{-1} \right\rangle$, on a $x \in \{\pm 1, \pm\omega, \pm\omega^2\} \subset \langle \zeta_6 \rangle$ d'où $\overline{(x, 1)} \in \left\langle \overline{(\zeta_6, 1)} \right\rangle = Z(G)$ donc $x \in p_1(\pi^{-1}(Z(G)))$ et donc $p_1(\pi^{-1}(G)) \simeq Z(G)$. Ainsi, on a
$$2\,|G| = |\pi^{-1}(G)| \leq |p_1(\pi^{-1}(G))|\ |p_2(\pi^{-1}(G))| = |Z(G)|\ |\Omega_G|$$
$$\Rightarrow\ |\Omega_G| \geq \frac{2\,|G|}{|Z(G)|} = 48\ \Rightarrow\ \Omega_G = \mathcal{O}\ \Rightarrow\ c \in \left\langle a, cac^{-1} \right\rangle$$
et ceci est absurde.
- Si $G = \left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle$, on a $\Omega_G := \left\langle a^{\mathcal{O}}, b^{\mathcal{O}} \right\rangle = \langle b, a, cac^{-1} \rangle$ et, de même,
$$G = \left\langle r, r_1, r_4 r_1 r_4^{-1} \right\rangle.$$
On a encore $\omega \in G$ d'où $|Z(G)| \geq 6$ et donc
$$|G| \in \{144, 288, 576\}.$$
Si $|G| = 576$, alors $G = \mathbb{O}$ d'où $r_3 \in G$, ce qui est exclus. Si $|G| = 144$, alors par ce qui précède, $G = \left\langle r_1, r_4 r_1 r_4^{-1} \right\rangle$ d'où $r \in G$ et ceci est également exclus. Si $|G| = 288$, G est d'indice 2 dans $\mathbb{O}$, et $|Z(G)| = 12$. Comme précédemment, $\zeta_{12} = \zeta_{24}^2 \in G$ donc $Z(G) = \left\langle \overline{(\zeta_{12}, 1)} \right\rangle$. On a encore $\Omega_G = p_2(\pi^{-1}(G))$ et si $x = p_1(x, y) \in p_1(\pi^{-1}(G))$, comme $G = \left\langle r, r_1, r_4 r_1 r_4^{-1} \right\rangle$, on doit avoir $x \in \{\pm 1, \pm i, \pm\omega, \pm\omega^2, \pm i\omega, \pm i\omega^2\} \subset \langle \zeta_{12} \rangle$, donc

$\overline{(x,1)} \in \left\langle \overline{(\zeta_{12},1)} \right\rangle = Z(G)$ et donc $x \in p_1(\pi^{-1}(Z(G)))$. On en déduit que $|p_1(\pi^{-1}(G))| = |Z(G)| = 12$. Ainsi

$$2\,|G| = |\pi^{-1}(G)| \leq |p_1(\pi^{-1}(G))|\;|p_2(\pi^{-1}(G))| = |Z(G)|\;|\Omega_G| = 12\;|\Omega_G|$$

$$\Rightarrow\;\; |\Omega_G| \geq \frac{|G|}{6} = 48 \;\Rightarrow\; \Omega_G = \mathcal{O} \;\Rightarrow\; c \in \Omega_G$$

et ceci est absurde.

- Enfin, si $G = \left\langle r^{\mathbb{O}} \right\rangle$, comme $G(4,2,2) = \left\langle r^{\mathbb{T}} \right\rangle \leq G$, on a $\zeta_4 \in G(4,2,2)$, donc $|Z(G)| \geq 4$ et donc $|G| \geq 96$ et on en déduit que

$$|G| \in \{96, 144, 192, 288, 576\}.$$

Si $|G| = 576$, alors $r_1 \in G$: exclus. Si $|G| = 288$, G est d'indice 2 donc $r_1 = (r_1^{-1})^2 \in G$: exclus également. Si $|G| = 192$, alors $[\mathbb{O} : G] = 3$, donc $r_3 = r_3^3 \in G$, et c'est impossible. Si $|G| = 144$, alors $r_1 = r_1^4 \in G$, ce qui est absurde. Finalement, si $|G| = 96$, G est d'indice 6 et G est un sous-groupe de $\left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle$ donc $|\left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle|$ est multiple de 96 et on a vu que $|\left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle| \notin \{144, 288, 576\}$, donc $|\left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle| \in \{96, 192\}$. Si c'est 96, alors $G = \left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle$ d'où $r_1 \in G$, ce qui est exclus et si c'est 192, alors $[\left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}} \right\rangle : G] = 2$, donc $r_1 = (r_1^{-1})^2 \in G$. Cette contradiction finale achève la preuve.

□

Revenons à notre classification. Comme $r = r_4^2$, il ne reste à considérer la clôture normale que de huit des sous-ensembles non vides de $\{r, r_1, r_3, r_4\}$. Posons

$$r_3' := r r_3 r, \qquad r_3'' := (r_1^2 r_4)^{-1} r_3 (r_1^2 r_4), \qquad r_4' := r_3^{-1} r_4 r_3;$$

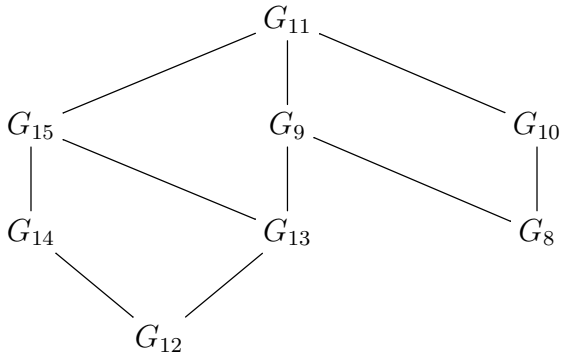
matriciellement, ceci s'écrit

$$r_3' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad r_3'' = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1+i \\ 1-i & 0 \end{pmatrix}, \qquad r_4' = \frac{1}{2} \begin{pmatrix} 1+i & -1+i \\ -1+i & 1+i \end{pmatrix}.$$

Les seuls groupes possibles sont alors (notation de Shephard-Todd) :

$$\begin{cases} G_8 := \left\langle r_4^{\mathbb{O}} \right\rangle \\ G_9 := \left\langle r_3^{\mathbb{O}}, r_4^{\mathbb{O}} \right\rangle \\ G_{10} := \left\langle r_1^{\mathbb{O}}, r_4^{\mathbb{O}} \right\rangle \\ G_{11} := \left\langle r_1^{\mathbb{O}}, r_3^{\mathbb{O}}, r_4^{\mathbb{O}} \right\rangle = \mathbb{O} \\ G_{12} := \left\langle r_3^{\mathbb{O}} \right\rangle \\ G_{13} := \left\langle r^{\mathbb{O}}, r_3^{\mathbb{O}} \right\rangle \\ G_{14} := \left\langle r_1^{\mathbb{O}}, r_3^{\mathbb{O}} \right\rangle \\ G_{15} := \left\langle r^{\mathbb{O}}, r_1^{\mathbb{O}}, r_3^{\mathbb{O}} \right\rangle \end{cases}$$

On peut là aussi dessiner le treillis des sous-groupes de $\mathbb{O}$:



Remarquons ensuite que G_4 et G_5 sont des sous-groupes de G_{14}, G_6 et G_7 sont des sous-groupes de G_{10} et G_{15} et que $G(4,2,2)$ est un sous-groupe de G_8 et de G_{13}. Tout comme avant, on peut dresser la table récapitulative suivante :

G	Structure	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$k[m]l$
G_8	$\langle r_4, r_4'\rangle \simeq \mathcal{TC}_4$	96	4	4[3]4
G_9	$\langle r_3, r_4\rangle \simeq \mathcal{C}_8 \circ \mathcal{O}$	192	8	2[6]4
G_{10}	$\langle r_1, r_4'\rangle \simeq \mathcal{C}_3 \times \mathcal{TC}_4$	288	12	3[4]4
G_{11}	$\langle r_1, r_3, r_4\rangle \simeq \mathcal{C}_3 \times (\mathcal{C}_8 \circ \mathcal{O}) = \mathbb{O}$	576	24	$\emptyset$
G_{12}	$\langle r_3, r_3', r_3''\rangle \simeq GL_2(\mathbb{F}_3)$	48	2	$\emptyset$
G_{13}	$\langle r, r_3, r_3''\rangle \simeq \mathcal{C}_4 \circ \mathcal{O}$	96	4	$\emptyset$
G_{14}	$\langle r_1, r_3'\rangle \simeq \mathcal{C}_3 \times G_{12}$	144	6	3[8]2
G_{15}	$\langle r, r_1, r_3\rangle \simeq \mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{O})$	288	12	$\emptyset$

TABLE 3 – Sous-groupes de $\mathbb{O}$

La notation $\mathcal{TC}_4$ signifie que

$$G_8 \simeq \mathcal{T} \rtimes \langle r_4\rangle .$$

Remarque 26. On peut montrer que $\mathcal{T}$ est le groupe dérivé de $\mathcal{O}$. De plus, comme G_{12} est un sous-groupe de tous les groupes de la table sauf G_8 et G_{10}, on a $G_8 \nsim G_{13}$ et $G_{10} \nsim G_{15}$.

4.4 Groupes de type $\mathcal{I}$

Les générateurs de $\mathcal{I}$ sont

$$e := \frac{1}{2}\begin{pmatrix} \tau^{-1} - \tau i & 1 \\ -1 & \tau^{-1} + \tau i \end{pmatrix}, \qquad b := \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

d'ordre 5 et 4, respectivement. (On a noté, comme à notre habitude $\tau := \frac{1+\sqrt{5}}{2}$.) Les classes de conjugaison non triviales de $\mathcal{I}\Big/Z(\mathcal{I}) \simeq \mathfrak{A}_5$ sont représentées par $\overline{a}, \overline{b}, \overline{e}, \overline{e}^2$, où $a = (be)^3 e^2 b^3$. Les éléments a et b sont les générateurs de $\mathcal{T}$ et $\overline{a}, \overline{b}, \overline{e}$ correspondent aux premutations $(3,5,4), (2,3)(4,5)$ et $(1,2,4,3,5)$. Soit ζ une valeur propre de e. Alors $\zeta \in \mu_5$ et on peut supposer que $\zeta = \zeta_5 = \exp\left(\frac{2i\pi}{5}\right)$ et comme $\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}$, il vient $\zeta + \zeta^{-1} + 1 = \tau$. De même que précédemment, on obtient que $\mathbb{I}$ possède sept classes de conjugaison de réflexions représentées par

$$ib,\ \omega a,\ \omega^2 a,\ \zeta e,\ \zeta^{-1} e,\ \zeta^2 e^2,\ \zeta^{-2} e^2.$$

De plus, comme $\zeta^{-1} e = (\zeta^2 e^3)^2$ et $\zeta^{-2} e^2 = (\zeta^2 e^3)^{-1}$, $\mathbb{I}$ possède trois classes de conjugaison de sous-groupes de cycliques de réflexions représentées par

$$r = ib, \qquad r_1 = \omega a, \qquad r_5 := \zeta^2 e^3,$$

qui sont d'ordres respectifs 2, 3 et 5, de matrices

$$r = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad r_1 = \frac{\omega}{2}\begin{pmatrix} -1-i & 1-i \\ -1-i & -1+i \end{pmatrix}, \quad r_5 = \frac{\zeta^2}{2}\begin{pmatrix} -\tau+i & -\tau+1 \\ \tau-1 & -\tau-i \end{pmatrix}.$$

Ensuite, il se trouve que les clôtures normales des sept sous-ensembles non vides de $\{r, r_1, r_5\}$ sont distinctes et on les notes (Shephard-Todd) :

$$\begin{cases} G_{16} := \left\langle r_5^{\mathbb{I}} \right\rangle \\ G_{17} := \left\langle r^{\mathbb{I}}, r_5^{\mathbb{I}} \right\rangle \\ G_{18} := \left\langle r_1^{\mathbb{I}}, r_5^{\mathbb{I}} \right\rangle \\ G_{19} := \left\langle r^{\mathbb{I}}, r_1^{\mathbb{I}}, r_5^{\mathbb{I}} \right\rangle = \mathbb{I} \\ G_{20} := \left\langle r_1^{\mathbb{I}} \right\rangle \\ G_{21} := \left\langle r^{\mathbb{I}}, r_1^{\mathbb{I}} \right\rangle \\ G_{22} := \left\langle r^{\mathbb{I}} \right\rangle \end{cases}$$

On définit

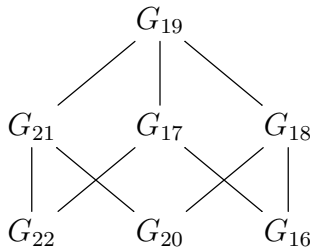
$$r' := r_1^{-2} r r_1^2, \quad r'' := r_5^{-1} r r_5, \quad r_1'' := r_5 r_1 r_5^{-1}, \quad r_5' := r^{-1} r_5 r,$$

matriciellement

$$r' = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r'' = \frac{1}{2}\begin{pmatrix} \tau & (\tau-1)i+1 \\ (1-\tau)i+1 & -\tau \end{pmatrix},$$

$$r_1'' = \frac{\omega}{2}\begin{pmatrix} -\tau i - 1 & (1-\tau)i \\ (1-\tau)i & \tau i - 1 \end{pmatrix}, \quad r_5' = -\frac{\zeta^2}{2}\begin{pmatrix} \tau - i & 1-\tau \\ \tau - 1 & \tau + i \end{pmatrix}.$$

On a le treillis des sous-groupes



ainsi que la table

G	Structure	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$k[m]l$
G_{16}	$\langle r_5, r_5' \rangle \simeq \mathcal{C}_5 \times \mathcal{I}$	600	10	5[3]5
G_{17}	$\langle r, r_5 \rangle \simeq \mathcal{C}_5 \times (\mathcal{C}_4 \circ \mathcal{I})$	1200	20	2[6]5
G_{18}	$\langle r_1^2, r_5 \rangle \simeq \mathcal{C}_{15} \times \mathcal{I}$	1800	30	3[4]5
G_{19}	$\langle r, r_1, r_5 \rangle \simeq \mathcal{C}_{15} \times (\mathcal{C}_4 \circ \mathcal{I}) = \mathbb{I}$	3600	60	$\emptyset$
G_{20}	$\langle r_1, r_1'' \rangle \simeq \mathcal{C}_3 \times \mathcal{I}$	360	6	3[5]3
G_{21}	$\langle r, r_1'' \rangle \simeq \mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{I})$	720	12	2[10]3
G_{22}	$\langle r, r', r'' \rangle \simeq \mathcal{C}_4 \circ \mathcal{I}$	240	4	$\emptyset$

TABLE 4 – Sous-groupes de $\mathbb{I}$

Remarque 27. On peut montrer (voir [15], Chapter 6, §6) que $G_{22} = \mathcal{C}_4 \circ \mathcal{I}$ est isomorphe au groupe $SL_2^{\pm}(\mathbb{F}_5)$ des matrices de déterminant ± 1 sur le corps fini à cinq éléments.

4.5 Conclusion

En faisant les comptes des résultat acquis jusqu'à présent, on obtient :

Théorème 17. ∗ *Si G est un groupe de réflexions unitaires irréductible et imprimitif de rang $n \geq 2$, alors G est conjugué dans $U_n(\mathbb{C})$ à un certain $G(m,p,n)$ pour $m > 1$ et $p|m$.*

∗ *Si G est un groupe de réflexions unitaires irréductible primitif de rang 2, alors G est conjugué dans $U_2(\mathbb{C})$ à l'un des groupes exceptionnels de Shephard-Todd G_k, pour $4 \leq k \leq 22$.*

Remarque 28. On peut classifier totalement les groupes de réflexions unitaires primitifs de tout rang. Il reste pour cela à construire quinze groupes primitifs de rang ≥ 3, notés G_i pour $23 \leq i \leq 37$, le plus petit étant G_{23} d'ordre 120 et le plus grand étant G_{37}, d'ordre 696 729 600 (voir [15], Chapter 8, §7, Theorem 8.29 et Tables D.1 et D.2, p.272-273).

Définition 20. Pour compléter la numérotation, il reste à introduire G_1, G_2 et G_3 :

$$\begin{cases} G_1 := \mathfrak{S}_n \simeq G(1,1,n),\ n > 1 \\ G_2 := G(m,p,n),\ n \geq 2,\ m > 1 \\ G_3 := \mathcal{C}_m \simeq G(m,1,1),\ m > 1 \end{cases}$$

Les G_m avec $1 \leq m \leq 37$ forment donc toutes les familles de groupes de réflexions possibles.

On peut enfin donner quelques tables synthétiques finales :

Table des groupes imprimitifs et des groupes primitifs de rang 2 :

G	Structure	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$k[m]l$
G_1	$\mathfrak{S}_n,\ n \geq 2$	$n!$	1	$\emptyset$
G_2	$G(m,p,n),\ m > 1,\ n \geq 2$	$\frac{n!m^n}{p}$	$\frac{mn}{p \vee n}$	$\emptyset$
G_3	$\mathcal{C}_m,\ m > 1$	m	m	$m[2]1$

TABLE 5 – Groupes imprimitifs de rang $n \geq 2$

Type	G	Structure	$\lvert G\rvert$	$\lvert Z(G)\rvert$	$k[m]l$	Nombre de réflexions d'ordre...			
						2	3	4	5
$\mathcal{T}$	G_4	$SL(2,3)$	$2^3 \cdot 3$	2	3[3]3		8		
	G_5	$\mathcal{C}_3 \times \mathcal{T}$	$2^3 \cdot 3^2$	6	3[4]3		16		
	G_6	$\mathcal{C}_4 \circ SL(2,3)$	$2^4 \cdot 3$	4	2[6]3	6	8		
	G_7	$\mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{T})$	$2^4 \cdot 3^2$	12	$\emptyset$	6	16		
$\mathcal{O}$	G_8	$\mathcal{T}\mathcal{C}_4$	$2^5 \cdot 3$	4	4[3]4	6		12	
	G_9	$\mathcal{C}_8 \circ \mathcal{O}$	$2^6 \cdot 3$	8	2[6]4	18		12	
	G_{10}	$\mathcal{C}_3 \times \mathcal{T}\mathcal{C}_4$	$2^5 \cdot 3^2$	12	3[4]4	6	16	12	
	G_{11}	$\mathcal{C}_3 \times (\mathcal{C}_8 \circ \mathcal{O})$	$2^6 \cdot 3^2$	24	$\emptyset$	18	16	12	
	G_{12}	$GL(2,3)$	$2^4 \cdot 3$	2	$\emptyset$	12			
	G_{13}	$\mathcal{C}_4 \circ \mathcal{O}$	$2^5 \cdot 3$	4	$\emptyset$	18			
	G_{14}	$\mathcal{C}_3 \times GL(2,3)$	$2^4 \cdot 3^2$	6	3[8]2	12	16		
	G_{15}	$\mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{O})$	$2^5 \cdot 3^2$	12	$\emptyset$	18	16		
$\mathcal{I}$	G_{16}	$\mathcal{C}_5 \times \mathcal{I}$	$2^3 \cdot 3 \cdot 5^2$	10	5[3]5				48
	G_{17}	$\mathcal{C}_5 \times (\mathcal{C}_4 \circ \mathcal{I})$	$2^4 \cdot 3 \cdot 5^2$	20	2[6]5	30			48
	G_{18}	$\mathcal{C}_{15} \times \mathcal{I}$	$2^3 \cdot 3^2 \cdot 5^2$	30	3[4]5		40		48
	G_{19}	$\mathcal{C}_{15} \times (\mathcal{C}_4 \circ \mathcal{I})$	$2^4 \cdot 3^2 \cdot 5^2$	60	$\emptyset$	30	40		48
	G_{20}	$\mathcal{C}_3 \times \mathcal{I}$	$2^3 \cdot 3^2 \cdot 5$	6	3[5]3		40		
	G_{21}	$\mathcal{C}_3 \times (\mathcal{C}_4 \circ \mathcal{I})$	$2^4 \cdot 3^2 \cdot 5$	12	2[10]3	30	40		
	G_{22}	$\mathcal{C}_4 \circ \mathcal{I}$	$2^4 \cdot 3 \cdot 5$	4	$\emptyset$	30			

TABLE 6 – Groupes primitifs de rang 2

On peut reprendre également les treillis des sous-groupes de réflexions de $\mathbb{T}$, $\mathbb{O}$ et $\mathbb{I}$:

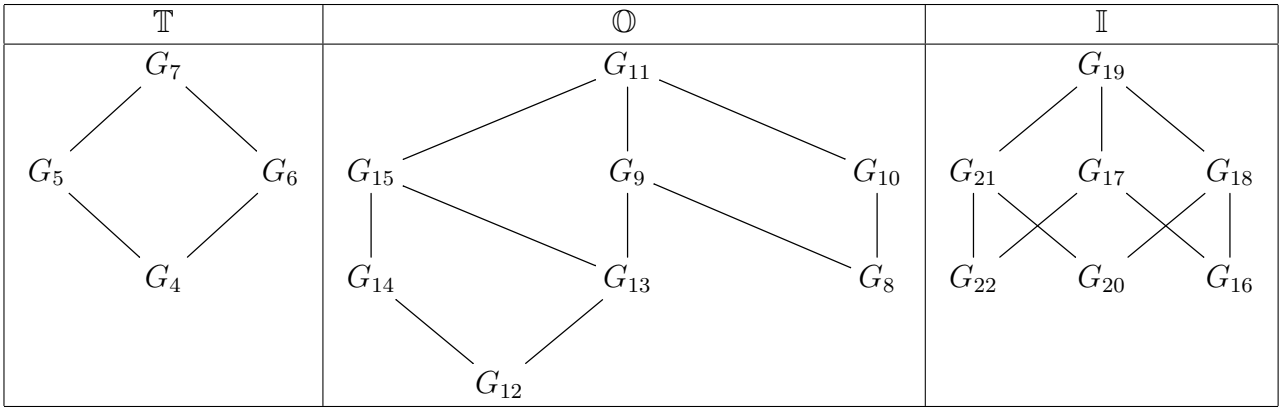
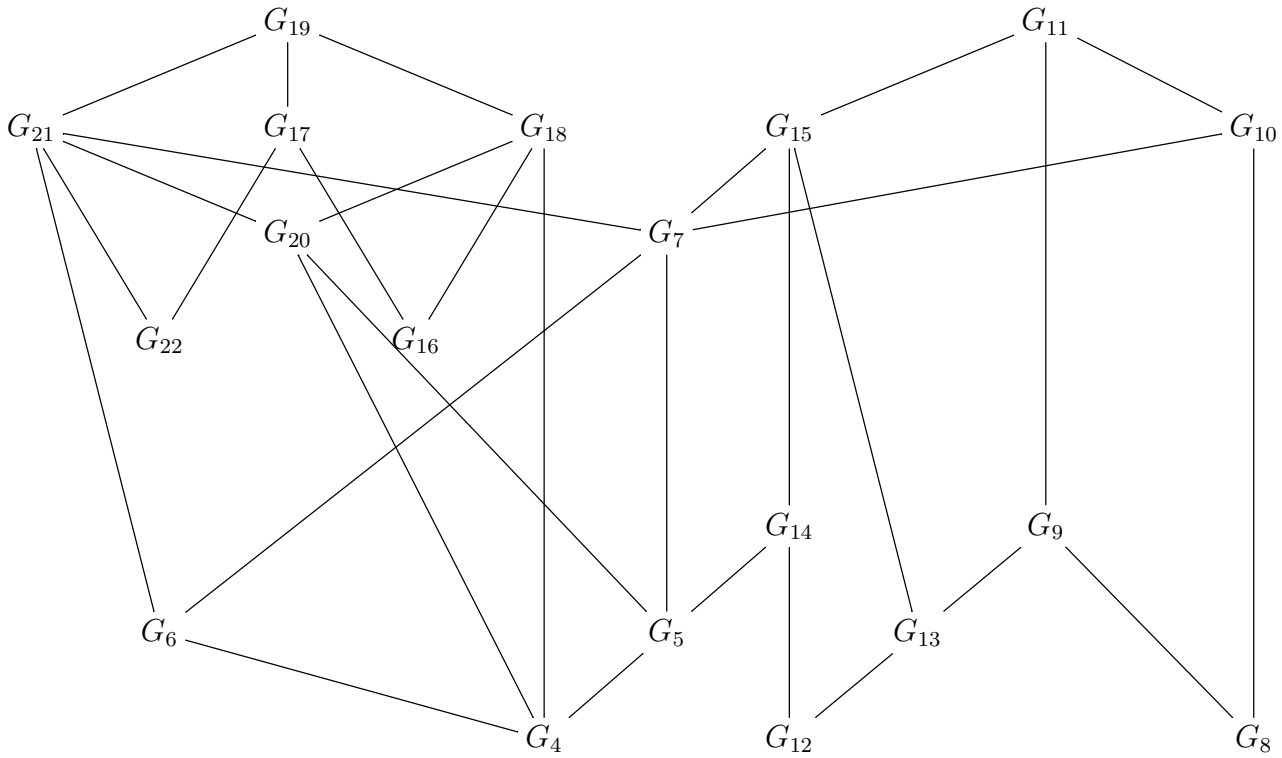


TABLE 7 – Treillis des sous-groupes de réflexions de $\mathbb{T}$, $\mathbb{O}$ et $\mathbb{I}$

Pour finir, on peut combiner ces trois derniers treillis pour obtenir un treillis partiel des sous-groupes de réflexions de $U_2(\mathbb{C})$:



Annexe

Générateurs des groupes symétriques, alternés et orthogonaux euclidiens

Déterminons tout d'abord le centre des groupes symétriques, qui nous est utile dans le calcul du centre des $G(m,p,n)$:

Proposition 1. *Si $n \geq 3$, alors $Z(\mathfrak{S}_n) = 1$.*

Démonstration. (Voir [16], Chapitre 1, §3)
Soit $\sigma \in Z(\mathfrak{S}_n)$ et supposons par l'absurde que $\sigma \neq 1$. Il existe donc $1 \leq i, j \leq n$ tels que $j := \sigma(i) \neq i$. On peut alors choisir $k \notin \{i, j\}$ et posons $\tau := (j, k)$. On a alors $\sigma\tau(i) = \sigma(i) = j \neq k = \tau(j) = \tau\sigma(i)$, ce qui est absurde. □

Passons aux générateurs de $\mathfrak{S}_n$. Les preuves données ci-après sont celles que l'on trouve par exemple dans [7]. Commençons par un lemme :

Lemme 1. *Soit $n \geq 2$. Alors $\mathfrak{S}_n$ est engendré par ses $(n-1)$ transpositions consécutives.*

Démonstration.

1. Montrons que $\mathfrak{S}_n$ est engendré par les transpositions. Ceci est clair pour $n = 2$. Pour $n \geq 3$, tout cycle de taille > 2 est produit de transpositions :

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k),$$

et comme les cycles engendrent $\mathfrak{S}_n$, notre assertion est prouvée.

2. Il suffit maintenant de montrer que toute transposition $(a, b) \in \mathfrak{S}_n$ est produit de transpositions de la forme $(i, i+1)$ avec $i < n$. Comme $(a, b) = (b, a)$, on peut supposer que $a < b$. On procède alors par récurrence sur $b - a$. Si $b - a = 1$, le résultat est clair. Supposons donc $b - a = k > 1$ et que l'assertion soit vraie pour toute transposition dont le support est constitué de deux entiers distants d'au plus $k - 1$. On a

$$(a, b) = (a, a+1)(a+1, b)(a, a+1),$$

donc en appliquant l'hypothèse de récurrence à $(a+1, b)$, on obtient bien le résultat.

□

Théorème 1. *Pour $n \geq 2$, $\mathfrak{S}_n$ est engendré par la transposition $(1, 2)$ et le n-cycle $(1, 2, \ldots, n)$.*

Démonstration. Par le Lemme, il suffit de montrer que $(1,2)$ et $(1,\dots,n)$ donnent toutes les transpositions consécutives. On peut, pour cela, supposer que $n \geq 3$. Posons $\sigma := (1,2,\dots,n)$. Alors, on a

$$\sigma(1,2)\sigma^{-1} = (\sigma(1),\sigma(2)) = (2,3),$$

et plus généralement, si $1 \leq k \leq n-2$, on a

$$\sigma^k(1,2)\sigma^{-k} = (\sigma^k(1),\sigma^k(2)) = (k+1,k+2),$$

comme souhaité. □

Passons enfin aux générateurs de $\mathfrak{A}_n$ et commençons là encore par un lemme :

Lemme 2. *Pour $n \geq 3$, le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles $(i,i+1,i+2)$, pour $1 \leq i \leq n-2$.*

Démonstration. Procédons par étapes :

1. Montrons que $\mathfrak{A}_n$ est engendré par les 3-cycles.
   Tout d'abord, on a $1 = (1,2,3)^3$. Soit donc $\sigma \in \mathfrak{A}_n \setminus \{1\}$, que l'on écrit comme produit de transpositions $\sigma = \tau_1 \cdots \tau_r \in \mathfrak{S}_n$. Si τ_i et τ_{i+1} ont un élément en commun, écrivons $\tau_i = (a,b)$ et $\tau_{i+1} = (a,c)$, avec $b \neq c$. Alors $\tau_i\tau_{i+1} = (a,c,b)$. Sinon, τ_i et τ_{i+1} sont disjoints, on écrit $\tau_i = (a,b)$ et $\tau_{i+1} = (b,c)$, avec a,b,c,d distincts et alors $\tau_i\tau_{i+1} = (a,b)(b,c)^2(c,d) = (b,c,d)(c,d,b)$. Comme $\sigma \in \mathfrak{A}_n$, r est pair et notre première assertion est alors prouvée.
2. $\mathfrak{A}_n$ est engendré par les 3-cyles $(1,i,j)$.
   Ceci découle directement de 1., en remarquant que si (a,b,c) ne contient pas 1, alors $(a,b,c) = (1,a,b)(1,b,c)$.
3. $\mathfrak{A}_n$ est engendré par les 3-cycles $(1,2,i)$.
   En effet, si $n = 3$, alors $\mathfrak{A}_3 = \{1,(1,2,3),(1,3,2)\}$. Si $n \geq 4$, alors $(1,2,i)^{-1} = (1,i,2)$, donc tout 3-cycle contenant 1 et 2 est produit de 3-cycles de la forme $(1,2,i)$. Pour un 3-cycle contenant 1 et pas 2, disons $(1,i,j)$, on a $(1,i,j) = (1,2,j)^2(1,2,i)(1,2,j)$ et on obtient l'assertion par 2.
4. Montrons maintenant le lemme.
   Si $n = 3$, le résultat est acquis. Si $n = 4$, l'assertion 3. entraîne que $\mathfrak{A}_4 = \langle (1,2,3),(1,2,4)\rangle$. Comme $(1,2,4) = (1,2,3)^2(2,3,4)(1,2,3)$, $\mathfrak{A}_4$ est engendré par $(1,2,3)$ et $(2,3,4)$. Si $n \geq 5$, l'assertion 3. s'écrit $\mathfrak{A}_n = \langle (1,2,i),\ 3 \leq i \leq n\rangle$. Par récurrence sur i, chacun de ces cycles est produit de cycles consécutifs. On a vu que c'était vrai si $i = 3,4$. Si $i \geq 5$ et $j > i$, on a

   $$(1,2,j) = (1,2,j-2)(1,2,j-1)(j-2,j-2,j)(1,2,j-2)(1,2,j-1),$$

   d'où le résultat.

□

Théorème 2. *Si $n \geq 3$, alors $\mathfrak{A}_n$ est engendré par*

$$\begin{cases} (1,2,3) \quad et \quad (1,2,\dots,n) & \text{si } n \text{ est impair} \\ (1,2,3) \quad et \quad (2,3,\dots,n) & \text{si } n \text{ est pair} \end{cases}$$

Démonstration. Il suffit, par le Lemme 2, de montrer que les permutations données permettent d'atteindre les 3-cycles $(i, i+1, i+2)$.
Si n est impair, soit $\sigma := (1, 2, \ldots, n) \in \mathfrak{A}_n$ et alors, pour $1 \leq k \leq n-3$, on a

$$\sigma^k(1,2,3)\sigma^{-k} = (\sigma^k(1), \sigma^k(2), \sigma^k(3)) = (k+1, k+2, k+3).$$

Si n est pair, soit $\sigma := (2, 3, \ldots, n) \in \mathfrak{A}_n$ et, pour $1 \leq k \leq n-3$, on a

$$\sigma^k(1,2,3)\sigma^{-k} = (\sigma^k(1), \sigma^k(2), \sigma^k(3)) = (1, k+2, k+3)$$

et, comme $(k, k+1, k+2) = (1, k, k+1)(1, k+1, k+2)$, le résultat est démontré. □

Passons maintenant aux générateurs de $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$. Pour les définitions et les preuves qui vont suivre, nous renvoyons le lecteur à [16], Chapitre 6, §2.

Théorème 3. *1. Le groupe $O_n(\mathbb{R})$ est engendré par les réflexions orthogonales. Plus précisément, si $u \in O_n(\mathbb{R})$, u est produit d'au plus n réflexions.*

2. Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les renversements. Plus précisément, tout élément $u \in SO_n(\mathbb{R})$ est produit d'au plus n renversements.

Démonstration. 1. Soit $u \in O_n(\mathbb{R})$ et considérons

$$F_u := \{x \in \mathbb{R}^n \ ; \ u(x) = x\}$$

l'espace des points fixes de u. Posons $p_u := \operatorname{codim}(F_u) = n - \dim F_u$. Nous allons prouver que u est produit d'au plus p_u réflexions, en convenant que id est produit de zéro réflexion.
Raisonnons par récurrence sur p_u. Si $p_u = 0$, alors $u = id$ et il n'y a rien à démontrer.
Supposons $p_u > 0$, soit $x \in F_u^\perp$ non nul et soit $y := u(x)$. On a $y \neq x$ et $y \in F_u^\perp$ car F_u, donc aussi $F_u^\perp$ est u-stable. De plus, comme on a $\|x\| = \|y\|$, on en déduit que $(x-y|x+y) = 0$ de sorte que $x-y$ est orthogonal à $x+y$.
Soit alors τ la réflexion définie par le vecteur $x-y$. On a $\tau(x-y) = y-x$ et $\tau(x+y) = x+y$, donc $\tau(y) = x$. De plus, comme $x-y \in F_u^\perp$, on a $\tau_{|F_u} = id$. On a donc l'inclusion $F_u \subset F_{\tau u}$ et, comme $x \in F_{\tau u} \setminus F_u$, on a $p_{\tau u} < p_u$. Par hypothèse de récurrence, on peut écrire $\tau u = \tau_1 \cdots \tau_r$ où les τ_i sont des réflexions et $r \leq p_{\tau u}$, mais alors on a aussi $u = \tau\tau_1 \cdots \tau_r$ et $r+1 \leq p_u$.

2. Supposons dans un premier temps que $n = 3$. Si $u \neq id$, on a $u = \tau_1\tau_2$ où τ_1, τ_2 sont des réflexions. Mais, comme on a $n = 3$, $-\tau_i =: \sigma_i$ est un renversement (comme on le voit immédiatement grâce aux matrices) et on a $u = \sigma_1\sigma_2$.
Pour $n \geq 3$ quelconque, soit $u \in SO_n(\mathbb{R})$. On écrit $u = \tau_1 \cdots \tau_{2p}$ avec $2p \leq n$, les τ_i étant des réflexions. Il suffit alors de montrer que si τ_1, τ_2 sont des réflexions, alors il existe des renversements σ_1, σ_2 tels que $\tau_1\tau_2 = \sigma_1\sigma_2$. Posons en effet $u := \tau_1\tau_2$. Soient H_1, H_2 les hyperplans de τ_1, τ_2 et soit V un sous-espace de dimension $n-3$ de $H_1 \cap H_2$. On a $u_{|V} = id$ et donc $V^\perp$ est u-stable. D'après le cas $n = 3$, on a $u_{|V^\perp} = \sigma_1\sigma_2$ où σ_i est un renversement de $V^\perp$, et on obtient le résultat en prolongeant les σ_i par l'identité sur V.

□

Groupes de déplacements des solides platoniciens et sous-groupes finis de $SO_3(\mathbb{R})$

Nous allons établir ici quelques résultats fondamentaux pour l'étude des sous-groupes finis de $\mathbb{H}^*$ et de $SU_2(\mathbb{C})$. Plus précisément, nous allons classifier (à conjugaison près) les sous-groupes finis du groupe des isométries $SO_3(\mathbb{R})$. Nous verrons dans la preuve apparaître les groupes d'isométries directes laissant globalement invariants quelques solides particuliers (les solides de Platon), dont il nous faut au préalable déterminer la structure.

Rappelons tout d'abord que les solides de Platon sont au nombre de cinq ; à savoir le tétraèdre, le cube, l'octaèdre, le dodécaèdre et l'icosaèdre. Nous donnons ici un tableau représentant ces cinq solides, réalisé par Owen Garnier, à l'aide du logiciel GeoGebra :

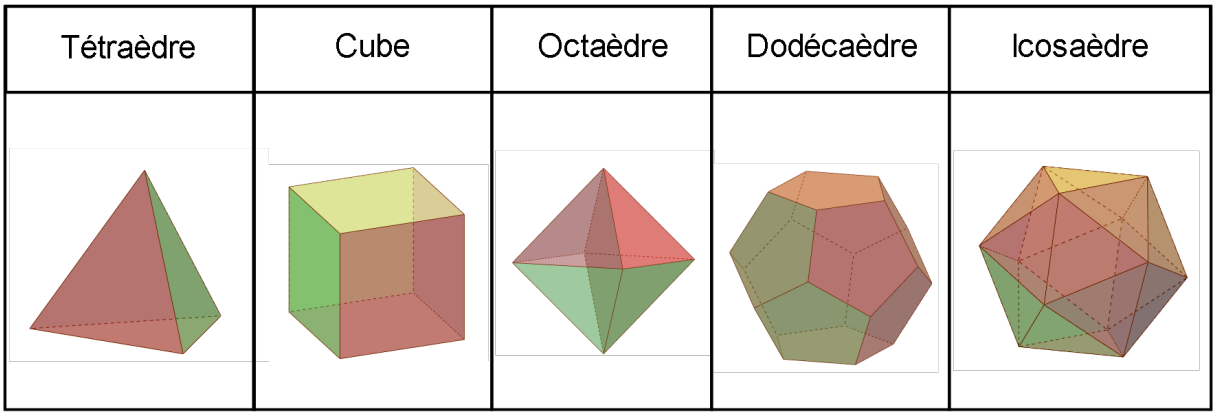


FIGURE 1 – Les Solides de Platon

Dans la suite, pour une partie X de $\mathbb{R}^3$, on note $\mathrm{Is}(X)$ (resp. $\mathrm{Is}^+(X)$) le groupe formé des isométries affines laissant globalement invariante la partie X. Aussi noterons-nous, par abus, $\mathscr{T}$ (resp. $\mathscr{K}$, $\mathscr{O}$, $\mathscr{D}$, $\mathscr{I}$) le tétraèdre (resp. cube, octaèdre, dodécaèdre, icosaèdre) régulier, dont l'origine O est l'isobarycentre des sommets.

Proposition 2. *On a*

$$\mathrm{Is}^+(\mathscr{T}) \simeq \mathfrak{A}_4.$$

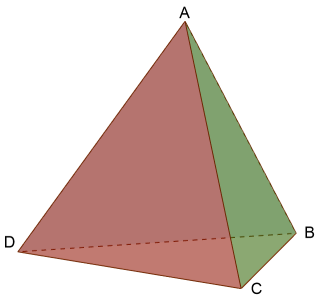


FIGURE 2 – Tétraèdre régulier

Démonstration. (Voir [5], Chapitre 12, §3)
La distance entre deux sommets est la distance maximale entre deux points quelconques de $\mathscr{T}$, donc $\mathrm{Is}^+(\mathscr{T})$ agit sur les sommets de $\mathscr{T}$, notés A, B, C, D, d'où un morphisme

$$\varphi : \mathrm{Is}^+(\mathscr{T}) \to \mathfrak{S}_4.$$

φ est injectif car si $\rho \in \mathrm{Is}^+(\mathscr{T})$ fixe tout sommet, ρ fixe un repère affine, donc $\rho = Id_{\mathbb{R}^3}$. Ensuite, grâce aux rotations d'axes $[OA], [OB], [OC], [OD]$, et d'angles $\frac{2\pi}{3}, \frac{4\pi}{3}$, et celles d'axes $\left[\frac{A+D}{2}, \frac{B+C}{2}\right], \left[\frac{C+D}{2}, \frac{A+B}{2}\right], \left[\frac{B+D}{2}, \frac{A+C}{2}\right]$ et d'angle π, on voit que tout 3-cycle et toute double transposition sont dans $\mathrm{im}\,(\varphi)$ et on en déduit que $\mathfrak{A}_4 \leq \mathrm{im}\,\varphi$. Or, s'il existe $\rho \in \mathrm{Is}^+(\mathscr{T})$ tel que $\varepsilon(\varphi(\rho)) = -1$, $\varphi(\rho)$ est produit d'un nombre impair de transpositions et comme $\mathfrak{A}_4 \leq \mathrm{im}\,\varphi$, il existe $g \in \mathrm{Is}^+(\mathscr{T})$ tel que $\varphi(g)$ soit une transposition, donc échange deux sommets, disons A et B. Alors, g fixe O, C, D, donc $g_{|(OCD)} = id_{(OCD)}$ et échange A et B, donc g est la réflexion d'hyperplan (OCD), donc $\det g < 0$ et ceci contredit $g \in SO_3(\mathbb{R})$. Ainsi, $\mathrm{im}\,\varphi = \mathfrak{A}_4$, d'où le résultat. □

Proposition 3. *On a*

$$\mathrm{Is}^+(\mathscr{C}) \simeq \mathfrak{S}_4.$$

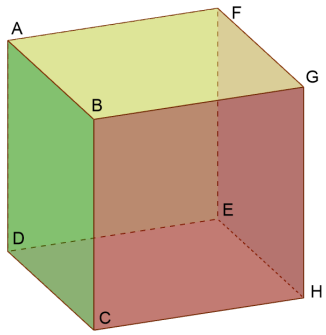


FIGURE 3 – Cube

Démonstration. (Voir [5], Chapitre 12, §3)
O est l'isobarycentre des sommets A, B, C, D, E, F, G, H de $\mathscr{C}$, donc il est fixé sous l'action de $\mathrm{Is}^+(\mathscr{C})$; donc ce dernier agit sur les sommets du cube. Comme $\mathrm{Is}^+(\mathscr{C})$ est formé d'isométries, une diagonale est envoyée sur une autre diagonale, d'où une action sur les diagonales, notées $D_1 := [AH]$, $D_2 := [DG]$, $D_3 := [BE]$ et $D_4 := [CF]$ et ceci donne un morphisme

$$\varphi : \mathrm{Is}^+(\mathscr{C}) \to \mathfrak{S}_4.$$

Pour échanger D_1 et D_2, on peut considérer la rotation d'axe $\left[\frac{A+D}{2}, \frac{G+H}{2}\right]$ et d'angle π. On en déduit que les transpositions $(1, i)$, $1 \leq i \leq 4$ sont atteintes et donc φ est surjectif. Ensuite, si $\rho \in \mathrm{Is}^+(\mathscr{C})$ fixe toutes les diagonales, alors ρ envoie A sur A ou sur H. Si $\rho(A) = H$, comme ρ est une isométrie, on a $\rho(B) = E$ et de même, ρ envoie chaque sommet sur son opposé, donc est une isométrie indirecte, ce qui est exclus. Ainsi, $\rho(A) = A$ et $\rho(H) = H$ et donc ρ fixe tout sommet, donc un repère affine et donc $\rho = 1$. φ est par conséquent injectif, comme voulu. □

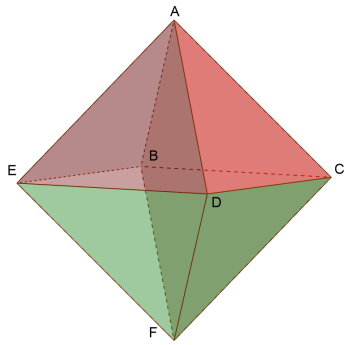


FIGURE 4 – Octaèdre régulier

Proposition 4. *On a*

$$\mathrm{Is}^+(\mathscr{O}) \simeq \mathfrak{S}_4.$$

Démonstration. On procède de façon analogue au cas du cube. Là encore, comme O est l'isobarycentre des sommets A, B, C, D, E, F de $\mathscr{O}$, O est fixé et ainsi $\mathrm{Is}^+(\mathscr{O})$ agit sur les sommets. Pour des raisons de distance, $\mathrm{Is}^+(\mathscr{O})$ agit également sur les faces de $\mathscr{O}$, et l'image par une isométrie de l'isobarycentre d'une face est l'isobarycentre de l'image par cette même isométrie de la face considérée. Or, la distance entre isobarycentres de faces est conservée, donc deux faces opposées sont envoyées sur deux faces opposées et donc $\mathrm{Is}^+(\mathscr{O})$ agit sur les couples de faces opposées, qui sont au nombre de quatre, d'où un morphisme

$$\varphi : \mathrm{Is}^+(\mathscr{O}) \to \mathfrak{S}_4.$$

Notons, de façon naturelle, les couples de faces : $CF_1 := (ACD, BEF), CF_2 := (CDF, ABE)$, $CF_3 := (ADE, BCD), CF_4 := (ABC, DEF)$. Pour échanger CF_1 et CF_2, on peut considérer la rotation d'axe $\left[\frac{B+E}{2}, \frac{C+D}{2}\right]$ et d'angle π. Ainsi, les transpositions $(1, i)$ sont atteintes et donc φ est surjectif. De plus, si $\rho \in \mathrm{Is}^+(\mathscr{O})$ fixe les couples de faces opposées, la face (ACD) en fixée ou envoyée sur (BEF). Si $\rho(ACD) = (BEF)$, alors (CDF) étant adjacente à (ACD), $\rho(CDF)$ doit être adjacente à (BEF), donc $\rho(CDF) = (ABE)$ et de même, chaque face est envoyée sur son opposé, donc $\det \rho < 0$ et ceci est absurde. Donc ρ fixe (ACD) et pour les mêmes raisons, ρ fixe toutes les faces, donc tous les sommets, donc un repère affine et donc $\rho = 1$. Ceci montre que φ est injectif et termine la preuve. □

Proposition 5. *On a*

$$\mathrm{Is}^+(\mathscr{D}) \simeq \mathfrak{A}_5.$$

Démonstration. (Voir [3])
On voit que les rotations d'axes joignant deux sommets opposés et d'angles $\frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}$ ou d'axes joignant deux barycentres de faces opposés et d'angles $\frac{2\pi}{3}, \frac{4\pi}{3}$ ou encore d'axes joignant les milieux d'arêtes opposés et d'angle π préservent $\mathscr{D}$. On voit aussi que ces axes sont au nombre de 6 pour le premier type, 10 pour le second et 12 pour le troisième. Incluant l'identité, on obtient

$$|\mathrm{Is}^+(\mathscr{D})| = 1 + 6 \times 4 + 10 \times 2 + 15 \times 1 = 60. \tag{4}$$

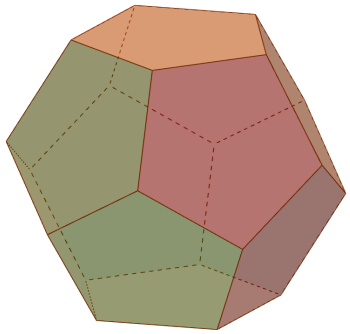


FIGURE 5 – Dodécaèdre régulier

Notons ensuite que $\mathrm{Is}^+(\mathscr{D})$ est un groupe simple. En effet, un sous-groupe distingué propre est d'ordre divisant 60 et son ordre doit être la somme de certains termes de droite de l'équation (4), incluant 1 et aucun tel entier n'existe, donc $\mathrm{Is}^+(\mathscr{D})$ n'admet aucun sous-groupe distingué propre. On voit que l'on peut inscrire cinq cubes dans $\mathscr{D}$ et on peut faire agir $\mathrm{Is}^+(\mathscr{D})$ sur l'ensemble de ces cinq cubes, ce qui donne un morphisme

$$\varphi : \mathrm{Is}^+(\mathscr{D}) \to \mathfrak{S}_5.$$

C'est une action non triviale et comme $\ker\varphi \trianglelefteq \mathrm{Is}^+(\mathscr{D})$, φ doit être injectif. Soit maintenant $\varepsilon : \mathfrak{S}_5 \to \{\pm 1\}$ la signature et composons avec φ pour obtenir un morphisme $\varepsilon\circ\varphi : \mathrm{Is}^+(\mathscr{D}) \to \{\pm 1\}$. Si $\varepsilon \circ \varphi$ était surjectif, on aurait $\ker(\varepsilon \circ \varphi) = 1$ et alors $\mathrm{Is}^+(\mathscr{D})$ serait d'ordre au plus 2, ce qui est faux. Ainsi, $\varepsilon \circ \varphi = 1$, donc $\mathrm{im}\,\varphi \leq \ker\varepsilon = \mathfrak{A}_5$ et pour des raisons d'ordre, on obtient que $\varphi : \mathrm{Is}^+(\mathscr{D}) \to \mathfrak{A}_5$ est un isomorphisme, comme souhaité. □

Proposition 6. *On a*

$$\mathrm{Is}^+(\mathscr{I}) \simeq \mathfrak{A}_5.$$

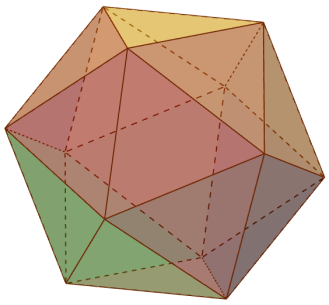


FIGURE 6 – Icosaèdre régulier

Démonstration. On procède de la même façon que pour le groupe du dodécaèdre (Proposition 5). □

Nous sommes maintenant en mesure de classifier les sous-groupes finis de $SO_3(\mathbb{R})$:

Théorème 4. *Tout sous-groupe fini de $SO_3(\mathbb{R})$ est conjugué (dans $SO_3(\mathbb{R})$) à l'un des groupes suivants :*

* *Le groupe cyclique $\mathcal{C}_m$ d'ordre m engendré par*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(4\pi/m) & -\sin(4\pi/m) \\ 0 & \sin(4\pi/m) & \cos(4\pi/m) \end{pmatrix},$$

* *Le groupe diédral $\mathcal{D}_{2m}$ d'ordre $2m$ engendré par*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(4\pi/m) & -\sin(4\pi/m) \\ 0 & \sin(4\pi/m) & \cos(4\pi/m) \end{pmatrix} \quad et \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

* *Le groupe tétraédral $\mathrm{Is}^+(\mathscr{T}) \simeq \mathfrak{A}_4$ engendré par*

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

* *Le groupe octaédral $\mathrm{Is}^+(\mathscr{O}) \simeq \mathfrak{S}_4$ engendré par*

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix},$$

* *Le groupe icosaédral $\mathrm{Is}^+(\mathscr{I}) \simeq \mathfrak{A}_5$ engendré par*

$$\frac{1}{2}\begin{pmatrix} 1 & \tau & \tau^{-1} \\ \tau & -\tau^{-1} & -1 \\ -\tau^{-1} & 1 & -\tau \end{pmatrix} \quad et \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad avec \quad \tau := \frac{1+\sqrt{5}}{2}.$$

Démonstration. (Voir [1], Theorem 19.2)

- Soit donc G un sous-groupe fini de $SO_3(\mathbb{R})$. Tout élément de $G\setminus\{1\}$ est une rotation de $\mathbb{R}^3$ autour d'un axe qui est une droite vectorielle. Soit $\mathbb{S}^2$ la sphère unité de $\mathbb{R}^3$. Alors, chaque $g \in G \setminus \{1\}$ donne deux pôles sur $\mathbb{S}^2$ qui sont l'intersection avec $\mathbb{S}^2$ de l'axe de g et notons X l'ensemble de tels pôles. Nous prétendons que G agit sur X. En effet, si $g \in G$ et $x \in X$ est un pôle de $h \in G \setminus \{1\}$, alors on a $ghg^{-1}(g(x)) = gh(x) = g(x)$, donc $g(x)$ est pôle de $ghg^{-1} \neq 1$ et donc $g(x) \in X$.
- Soit N le nombre d'orbites sous action et soient $x_1, \ldots, x_N$ des représentants des orbites. *id* fixe tout pôle et $g \in G\setminus\{1\}$ fixe exactement deux pôles (les siens), donc par la formule de Burnside, il vient

$$N = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}\,(g)| = \frac{1}{|G|}(|X| + 2(|G|-1)) = \frac{1}{|G|}\left(2(|G|-1) + \sum_{i=1}^{N}|\mathcal{O}(x_i)|\right)$$

et, par le lemme des orbites, il vient

$$2\left(1 - \frac{1}{|G|}\right) = N - \frac{1}{|G|}\sum_{i=1}^{N}|\mathcal{O}(x_i)| = N - \sum_{i=1}^{N}\frac{|\mathcal{O}(x_i)|}{|G|}$$

$$= N - \sum_{i=1}^{N} \frac{1}{|G_{x_i}|} = \sum_{i=1}^{N} \left(1 - \frac{1}{|G_{x_i}|}\right).$$

Si $G \neq 1$, on a $1 \leq 2\left(1 - \frac{1}{|G|}\right) < 2$ et $|G_{x_i}| \geq 2$ puisque G_{x_i} contient au moins l'identité et une rotation ; donc $\frac{1}{2} \leq 1 - \frac{1}{|G_{x_i}|} < 1$, pour tout $1 \leq i \leq N$. Ceci implique $2 \leq N < 4$ et donc $N = 2$ ou $N = 3$.

- Si $N = 2$, on a $|\mathcal{O}(x_1)| + |\mathcal{O}(x_2)| = 2$, d'où $|X| = 2$. Ainsi, toutes les rotations de G ont le même axe. Le plan vectoriel normal à cet axe est globalement stable par G, donc G est un sous-groupe fini de $SO_2(\mathbb{R}) \simeq \mathbb{S}^1$. Ainsi, G est cyclique, et conjugué à un certain $\mathcal{C}_m$.
- Si $N = 3$, soient $x := x_1$, $y := x_2$ et $z := x_3$. Alors on a

$$1 + \frac{2}{|G|} = \frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|} > 1.$$

Donc, à réarrangement près, quatre cas sont possibles :

(a) $\frac{1}{|G_x|} = \frac{1}{2}$, $\frac{1}{|G_y|} = \frac{1}{2}$, $\frac{1}{|G_z|} = \frac{1}{n}$, $n \geq 2$,

(b) $\frac{1}{|G_x|} = \frac{1}{2}$, $\frac{1}{|G_y|} = \frac{1}{3}$, $\frac{1}{|G_z|} = \frac{1}{3}$,

(c) $\frac{1}{|G_x|} = \frac{1}{2}$, $\frac{1}{|G_y|} = \frac{1}{3}$, $\frac{1}{|G_z|} = \frac{1}{4}$,

(d) $\frac{1}{|G_x|} = \frac{1}{2}$, $\frac{1}{|G_y|} = \frac{1}{3}$, $\frac{1}{|G_z|} = \frac{1}{5}$,

- Premier cas :
$* |G_x| = |G_y| = |G_z| = 2 \Rightarrow |G| = 4$. Comme G est d'ordre 4, il est conjugué à $\mathcal{C}_4$ ou $\mathcal{D}_4$.
$* |G_x| = |G_y| = 2$, $|G_z| = n \geq 3 \Rightarrow |G| = 2n$. Le groupe G_z des rotations d'axe passant par z et $-z$ est cyclique d'ordre n et on écrit

$$G_z = \{1, g, g^2, \ldots, g^{n-1}\} = \langle g \rangle .$$

Alors, $x, gx, g^2x, \ldots, g^{n-1}x$ sont distincts. En effet, si $g^i(x) = g^j(x)$ avec $i > j$, alors $g^{i-j}(x) = x$. Mais, z et $-z$ sont les seuls points fixés par g^{i-j} et $x \neq \pm z$ car $|G_x| = 2$ et $|G_z| = |G_{-z}| = n \geq 3$. Comme g préserve les distances, on a

$$\|x - gx\| = \|gx - g^2x\| = \cdots = \|g^{n-1}x - x\| \text{ et } \|z - x\| = \|z - g^i x\|, \ \forall 1 \leq i \leq n,$$

donc les points $x, gx, \ldots, g^{n-1}x$ forment les sommets d'un n-gône régulier $\mathscr{P}$. De plus, on a $|\mathcal{O}(x)| = \frac{|G|}{|G_x|} = n$, donc

$$\mathcal{O}(x) = \{x, gx, \ldots, g^{n-1}x\}$$

et donc G agit sur $\mathscr{P}$ et on a un morphisme d'action $\varphi : G \to \mathrm{Is}^+(\mathscr{P}) \simeq \mathcal{D}_{2n}$. Toute rotation non triviale de G ne fixe que deux points, donc aucune ne fixe ponctuellement $\mathscr{P}$ et ainsi $\ker \varphi = 1$. Comme $|G| = 2n = |\mathcal{D}_{2n}|$, on obtient $G \simeq \mathcal{D}_{2n}$.

- Second cas : $|G_x| = 2$, $|G_y| = |G_z| = 3 \Rightarrow |G| = 12$.
On a $|\mathcal{O}(z)| = 4$. Soit $u \in \mathcal{O}(z)$ tel que $0 < \|z - u\| < 2$ (ceci est possible car $X \subset \mathbb{S}^2$ et $|\mathcal{O}(z)| > 2$). En particulier, on a $u \neq \pm z$. De plus, $|G_z| = 3$, donc $G_z =: \langle g \rangle$ est cyclique d'ordre 3. Par le même argument que précédemment, u, gu, g^2u sont distincts.

Comme g est une isométrie, ils forment un triangle équilatéral et sont équidistants de z. L'orbite

$$\mathcal{O}(z) = \{z, u, gu, g^2u\}$$

est stable sous l'action de G. Pour $h \in G_u$, on a $hu = u$ et h permute z, gu et g^2u. Comme h est une isométrie, les distances entre u, z, gu et g^2u sont toutes égales, donc $\{u, z, gu, g^2u\}$ est un tétraèdre régulier $\mathscr{T}$ et on a un morphisme $\varphi : G \to \mathrm{Is}^+(\mathscr{T}) \simeq \mathfrak{A}_4$. Aucun élément de G ne fixe ponctuellement $\mathscr{T}$, donc φ est injectif et pour des raisons d'ordre, on a $G \simeq \mathfrak{A}_4$.

- Troisième cas : $|G_x| = 2,\ |G_y| = 3,\ |G_z| = 4 \ \Rightarrow\ |G| = 24$.
On a $|\mathcal{O}(z)| = 6$. Soit $u \in \mathcal{O}(z)$ avec $u \neq \pm z$. $G_z =: \langle g \rangle$ est cyclique d'ordre 4. Comme avant, on voit que u, gu, g^2u, g^3u sont équidistants de z et forment un carré. Comme $-z \notin \mathcal{O}(z)$ ou $\mathcal{O}(y)$ (puisque $|G_x| \neq |G_{-z}| \neq |G_y|$), on a

$$\mathcal{O}(z) = \{z, -z, u, gu, g^2u, g^3u\}.$$

Mais $-u \in \mathcal{O}(z)$ (car $|G_{-u}| = |G_u| = |G_z|$) et $-u \neq \pm z$ donc $\|gu - u\| = \|g^3u - u\| < 2$ puisque u, gu, g^2u, g^3u sont les sommets d'un carré. Donc $-u \neq gu, g^3u$ et ceci implique que $-u = g^2u$. Ainsi, $z, -z, u, gu, g^2u, g^3u$ sont les sommets d'un octaèdre régulier $\mathscr{O}$. Comme dans le cas précédent, on obtient un monomorphisme $\varphi : G \hookrightarrow \mathrm{Is}^+(\mathscr{O}) \simeq \mathfrak{S}_4$ et $G \simeq \mathfrak{S}_4$.

- Quatrième cas : $|G_x| = 2,\ |G_y| = 3,\ |G_z| = 5 \ \Rightarrow\ |G| = 60$.
On a ici $|\mathcal{O}(z)| = 12$. Écrivons $G_z =: \langle g \rangle$, groupe d'ordre 5, cyclique. Choisissons $u \neq v$ tels que $0 < \|z - u\| < \|z - v\| < 2$. Ceci est possible car $u, gu, \ldots, g^4u$ sont distincts, équidistants de z et forment un pentagone régulier et de même, $v, \ldots, g^4v$ dont distincts et équidistants de z (de distance à z strictement supérieure à celle de u à z ; en fait, on peut prendre $v := -u$). Ainsi, il vient

$$\mathcal{O}(z) = \{z, -z, u, v, gu, gv, g^2u, g^2v, g^3u, g^3v, g^4u, g^4v\}.$$

Les cinq points les plus proches de u doivent être équidistants de u, ce sont z, gu, g^2v, g^3v, g^4u, d'où $\|u - z\| = \|u - gu\| = \|u - g^2v\|$. Ainsi, les points de $\mathcal{O}(z)$ sont les sommets d'un icosaèdre régulier $\mathscr{I}$, d'où un morphisme $\varphi : G \hookrightarrow \mathrm{Is}^+(\mathscr{I}) \simeq \mathfrak{A}_5$ et pour des raisons d'ordre, on obtient $G \simeq \mathfrak{A}_5$.

- Dans tous les cas, on peut, à conjugaison près dans $SO_3(\mathbb{R})$, supposer que z est le pôle nord $(1, 0, 0)$ de $\mathbb{S}^2$. Ainsi, G est bien conjugué à l'un des groupes engendrés par les matrices données, et ceci achève la démonstration.

□

Algorithmes pour GAP

Construction des $G(m,p,n)$:

```
gap> G:=function(m,p,n)
> local i,l,mu,M,L,B,S,Bgen,mug,k,g,h,f,stru,A,G,phi12,phi1N,List1,ListN,phi;
> mu:=Group([[[E(m)]]]); groupe scalaire μ_m des racines m^èmes de l'unité
> M:=[ ];
> for i in [1..n] do
> Add(M,mu);
> od;
> B:=DirectProduct(M); on construit le produit direct B := μ_m^n
> S:=SymmetricGroup(n); groupe symétrique 𝔖_n
> Bgen:=[ ];; générateurs particuliers de B
> mug:=[ ]; image de Bgen par x ↦ x^(m/p)
> for i in [1..n] do
> Add(Bgen,Image(Embedding(B,i),[[E(m)]]));
> od;
> k:=m/p;
> for i in [1..n] do
> Add(mug,[[E(m)^k]]);
> od;
> stru:=GroupHomomorphismByImages(B,mu,Bgen,mug); morphisme x ↦ x^(m/p)
> A:=Kernel(stru); construction de A(m,p,n)
> if n=1 distinction des cas n = 1, n = 2 et n ≥ 3, suivant les générateurs de 𝔖_n
> then G:=A;
> elif n=2
> then L:=GeneratorsOfGroup(A);
> List1:=[ ];; image de L sous action de (1,2) ∈ 𝔖_2 sur A(m,p,2)
> for l in L do
> h:=One(B);
> g:=[ ];
> Add(g,Image(Projection(B,1),l));
> Add(g,Image(Projection(B,2),l));
> h:=h*Image(Embedding(B,2),g[1]);
> h:=h*Image(Embedding(B,1),g[2]);
> Add(List1,h);
> od;
> phi12:=GroupHomomorphismByImages(A,A,L,List1); image de (1,2) dans Aut(A(m,p,2))
> phi:=GroupHomomorphismByImages(S,AutomorphismGroup(A),
GeneratorsOfGroup(S),[phi12]); morphisme structurel d'action de 𝔖_2 sur A(m,p,2)
> G:=SemidirectProduct(S,phi,A); groupe G(m,p,2) = A(m,p,2) ⋊ 𝔖_2
> else
> L:=GeneratorsOfGroup(A);
> List1:=[ ]; image de L sous action de τ := (1,2) ∈ 𝔖_n sur A(m,p,n)
> ListN:=[ ]; image de L sous action de σ := (1,2,...,n) ∈ 𝔖_n sur A(m,p,n)
> for l in L do
```

```
> g:=[ ];
> h:=One(B);
> f:=One(B);
> for i in [1..n] do
> Add(g,Image(Projection(B,i),l));
> od;
> h:=h*Image(Embedding(B,1),g[2]);
> h:=h*Image(Embedding(B,2),g[1]);
> for i in [3..n] do
> h:=h*Image(Embedding(B,i),g[i]);
> od;
> Add(List1,h);
> f:=f*Image(Embedding(B,1),g[n]);
> for i in [2..n] do
> f:=f*Image(Embedding(B,i),g[i-1]);
> od;
> Add(ListN,f);
> od;
> phi12:=GroupHomomorphismByImages(A,A,L,List1); image de τ dans Aut (A(m,p,n))
> phi1N:=GroupHomomorphismByImages(A,A,L,ListN); image de σ dans Aut (A(m,p,n))
> phi:=GroupHomomorphismByImages(S,AutomorphismGroup(A),
GeneratorsOfGroup(S),[phi1N,phi12]); morphisme structurel d'action de 𝔖_n sur A(m,p,n)
> G:=SemidirectProduct(S,phi,A); construction de G(m,p,n) = A(m,p,n) ⋊ 𝔖_n
> fi;
> return G; renvoie le groupe G(m,p,n)
> end;;
```

Construction des groupes primitifs exceptionnels de rang 2 :

```
gap> i:=E(4);; définition du complexe i = √(-1), racine 4ème de l'unité
gap> WM:=1/2*[[-1-i,1-i],[-1-i,-1+i]];; matrices génératrices
gap> IM:=[[-i,0],[0,i]];;
gap> GM:=1/ER(2)*[[1-i,0],[0,1+i]];;
gap> t:=(1+ER(5))/2;;
gap> SM:=1/2*[[1/t-i,t],[-t,1/t+i]];;
gap> T:=Group([WM,IM]);; groupes 𝒯, 𝒪 et ℐ
gap> O:=Group([WM,GM]);;
gap> I:=Group([IM,SM]);;
gap> ZM12:=[[E(12),0],[0,E(12)^(-1)]];; générateurs des groupes cycliques scalaires
gap> ZM24:=[[E(24),0],[0,E(24)^(-1)]];;
gap> ZM60:=[[E(60),0],[0,E(60)^(-1)]];;
gap> C12:=Group([ZM12]);; copies matricielles de groupes cycliques scalaires
gap> C24:=Group([ZM24]);;
gap> C60:=Group([ZM60]);;
gap> 2Tbar:=DirectProduct(C12,T);; produits directs préliminaires
gap> 2Obar:=DirectProduct(C24,O);;
gap> 2Ibar:=DirectProduct(C60,I);;
gap> z:=[[-1,0,0,0],[0,-1,0,0],[0,0,-1,0],[0,0,0,-1]];;
```

```
gap> Cen:=Group([z]);; sous-groupe normal pour les produits centraux
gap> Tbar:=FactorGroup(2Tbar,Cen);; groupes primitifs 𝕋, 𝕆 et 𝕀
gap> Obar:=FactorGroup(2Obar,Cen);;
gap> Ibar:=FactorGroup(2Ibar,Cen);;
gap> eo1:=Embedding(2Obar,1);; plongements canoniques pour les produits directs
gap> eo2:=Embedding(2Obar,2);;
gap> et1:=Embedding(2Tbar,1);;
gap> et2:=Embedding(2Tbar,2);;
gap> ei1:=Embedding(2Ibar,1);;
gap> ei2:=Embedding(2Ibar,2);;
gap> pit:=NaturalHomomorphismByNormalSubgroup(2Tbar,Cen);; projections canoniques
gap> pio:=NaturalHomomorphismByNormalSubgroup(2Obar,Cen);;
gap> pii:=NaturalHomomorphismByNormalSubgroup(2Ibar,Cen);;
gap> r1g:=Image(et1,[[E(3),0],[0,E(3)^(-1)]]);; réflexions particulières
gap> r1d:=Image(et2,WM);;
gap> r2g:=Image(et2,WM^2);;
gap> rg:=Image(et1,[[i,0],[0,-i]]);;
gap> rd:=Image(et2,IM);;
gap> r1t:=Image(pit,r1g*r1d);;
gap> r2t:=Image(pit,r1g*r2g);;
gap> rt:=Image(pit,rg*rd);;
gap> r1g:=Image(eo1,[[E(3),0],[0,E(3)^(-1)]]);;
gap> r1d:=Image(eo2,WM);;
gap> rg:=Image(eo1,[[i,0],[0,-i]]);;
gap> rd:=Image(eo2,IM);;
gap> r4g:=Image(eo1,[[E(8),0],[0,E(8)^(-1)]]);;
gap> r4d:=Image(eo2,GM);;
gap> DM:=GM^3*WM^2*GM^2;;
gap> r3d:=Image(eo2,DM);;
gap> ro:=Image(pio,rg*rd);;
gap> r1o:=Image(pio,r1g*r1d);;
gap> r3o:=Image(pio,rg*r3d);;
gap> r4o:=Image(pio,r4g*r4d);;
gap> r2o:=r3o*r1o*r3o^(-1);;
gap> rg:=Image(ei1,[[i,0],[0,-i]]);;
gap> rd:=Image(ei2,IM);;
gap> r1g:=Image(ei1,[[E(3),0],[0,E(3)^(-1)]]);;
gap> r1d:=Image(ei2,WM);;
gap> r5g:=Image(ei1,[[E(5),0],[0,E(5)^(-1)]]^2);;
gap> r5d:=Image(ei2,SM^3);;
gap> ri:=Image(pii,rg*rd);;
gap> r1i:=Image(pii,r1g*r1d);;
gap> r5i:=Image(pii,r5g*r5d);;
gap> G4:=NormalClosure(Tbar,Group([r1t]));; Groupes exceptionnels de rang 2
gap> G5:=NormalClosure(Tbar,Group([r1t,r2t]));;
gap> G6:=NormalClosure(Tbar,Group([rt,r1t]));;
gap> G7:=NormalClosure(Tbar,Group([rt,r1t,r2t]));;
gap> G8:=NormalClosure(Obar,Group([r4o]));;
gap> G9:=NormalClosure(Obar,Group([r3o,r4o]));;
```

```
gap> G10:=NormalClosure(Obar,Group([r1o,r4o]));;
gap> G11:=NormalClosure(Obar,Group([r1o,r3o,r4o]));;
gap> G12:=NormalClosure(Obar,Group([r3o]));;
gap> G13:=NormalClosure(Obar,Group([ro,r3o]));;
gap> G14:=NormalClosure(Obar,Group([r1o,r3o]));;
gap> G15:=NormalClosure(Obar,Group([ro,r1o,r3o]));;
gap> G16:=NormalClosure(Ibar,Group([r5i]));;
gap> G17:=NormalClosure(Ibar,Group([ri,r5i]));;
gap> G18:=NormalClosure(Ibar,Group([r1i,r5i]));;
gap> G19:=NormalClosure(Ibar,Group([ri,r1i,r5i]));;
gap> G20:=NormalClosure(Ibar,Group([r1i]));;
gap> G21:=NormalClosure(Ibar,Group([ri,r1i]));;
gap> G22:=NormalClosure(Ibar,Group([ri]));;
```

Références

[1] T. Y. Armstrong, Groups and Symmetry, Springer-Verlag, 1988.

[2] M. Artin, Algebra, Prentice Hall, 1991.

[3] S. Bandyopadhyay, *Construction and properties of the icosahedron*, 2013.

[4] M. Broué, Introduction to Complex Reflection Groups and their Braid Groups, Springer-Verlag, 2010.

[5] P. Caldero and J. Germoni, Histroires Hédonistes de Groupes et de Géométries, Calvage-Mounet, 2013.

[6] A. Cohen, *Finite Complex Reflection Groups*, Annales scientifiques de l'ENS, p. 379-436, 1976.

[7] K. Conrad, *Generating Sets*, Expository Papers.

[8] H. S. M. Coxeter, *Quaternions and Reflections*, Arch. Math. Monthly, 53 : 136-146, 1946.

[9] H. S. M. Coxeter, Regular Complex Polytopes, Cambridge University Press, 1991.

[10] H. S. M. Coxeter *The symmetry Groups of regular complex polytopes*, Arch. Math., 13 : 86-97, 1962.

[11] J. Humphreys, A Course in Group Theory, Oxford University Press, 1996.

[12] J. Humphreys, Reflection Groups and Coxeter Groups, Cambridge University Press, 1990.

[13] T. Y. Lam, *Hamilton Quaternions*, in Hazewinkel's Handbook of Algebra, (6.9), p.450, Elsevier, 2003.

[14] S. Lang, Algebra, Springer-Verlag, 1994.

[15] G. I. Lehrer and D. E. Taylor, Unitary Reflection Groups, Cambridge University Press, 2009.

[16] D. Perrin, Cours d'Algèbre, Ellipses, 1996.

[17] J. J. Rotman, An Introduction to the Theory of Groups, Springer-Verlag, 1995.

[18] J. P. Serre, Représentations linéaires de Groupes finis, Hermann, 1998.

[19] G. C. Shephard and J. A. Todd, *Finite Unitary Reflection Groups*, Canad. J. Math., 6 : 274-304, 1954.

[20] F. Ulmer, Théorie des Groupes, Ellipses, 1996.

[21] H. J. Zassenhaus, The Theory of Groups, Chelsea Publishing Company, 1958.

[22] A. Zimmermann, Representation Theory, Springer, 2014.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.6* ; 2016, (`http://www.gap-system.org`).