4

Actions de groupes. Exemples et applications

$(G,\cdot)$ est un groupe multiplicatif et on note 1 (ou 1_G si nécessaire) l'élément neutre.
E est un ensemble non vide et $\mathcal{S}(E)$ est le groupe des permutations de E.

4.1 Définitions et exemples

Définition 4.1 *On dit que G opère à gauche sur E si on a une application :*

$$\begin{array}{ccc} G\times E & \to & E \\ (g,x) & \mapsto & g\cdot x \end{array}$$

telle que :

$$\begin{cases} \forall x\in E,\ 1\cdot x = x \\ \forall\,(g,g',x)\in G^2\times E,\ g\cdot(g'\cdot x) = (gg')\cdot x \end{cases}$$

Une telle application est aussi appelée action à gauche de G sur E.

Remarque 4.1 *On peut définir de manière analogue la notion d'action à droite d'un groupe sur un ensemble non vide comme une application :*

$$\begin{array}{ccc} G\times E & \to & E \\ (g,x) & \mapsto & x\cdot g \end{array}$$

telle que :

$$\begin{cases} \forall x\in E,\ x\cdot 1 = x \\ \forall\,(g,g',x)\in G^2\times E,\ (x\cdot g)\cdot g' = x\cdot(gg') \end{cases}$$

Pour tout $g\in G$, l'application :

$$\begin{array}{rccc} \varphi(g): & E & \to & E \\ & x & \mapsto & g\cdot x \end{array}$$

est alors une bijection de E sur E, c'est-à-dire que $\varphi(g)\in\mathcal{S}(E)$. En effet, de $1\cdot x = x$ pour tout $x\in E$, on déduit que $\varphi(1) = Id_E$ et avec $g\cdot(g^{-1}\cdot x) = (gg^{-1})\cdot x = 1\cdot x = x$ et $g^{-1}\cdot(g\cdot x) = x$ on déduit que $\varphi(g)\circ\varphi(g^{-1}) = \varphi(g^{-1})\circ\varphi(g) = Id_E$, ce qui signifie que $\varphi(g)$ est bijective d'inverse $\varphi(g^{-1})$.

De plus avec $g \cdot (g' \cdot x) = (gg') \cdot x$, pour tous g, g', x, on déduit que $\varphi(gg') = \varphi(g) \circ \varphi(g')$, c'est-à-dire que l'application φ est un morphisme de groupes de $(G, \cdot)$ dans $(\mathcal{S}(E), \circ)$.

Le noyau de ce morphisme φ est le noyau de l'action à gauche de G sur E.

Réciproquement un tel morphisme φ définit une action à gauche de G sur E avec :

$$g \cdot x = \varphi(g)(x)$$

Exemple 4.1 *G agit sur lui même par translations à gauche :*

$$(g, h) \in G \times G \mapsto g \cdot h = gh$$

Exemple 4.2 *Un groupe G agit sur lui même par conjugaison :*

$$(g, h) \in G \times G \mapsto g \cdot h = ghg^{-1}$$

le morphisme de groupes correspondant de $(G, \cdot)$ dans $(\mathcal{S}(G), \circ)$ est noté :

$$\begin{array}{rccc} \mathrm{Ad}(g): & G & \to & G \\ & h & \mapsto & ghg^{-1} \end{array}$$

L'image de Ad *est le groupe* $\mathrm{Int}(G)$ *des automorphismes intérieurs de G.*

Exercice 4.1 *Montrer que* $\mathrm{Int}(G)$ *est isomorphe au groupe quotient $G/Z(G)$, où $Z(G)$ est le centre de G.*

Solution 4.1 *Le noyau du morphisme de groupes* $\mathrm{Ad} : G \to \mathcal{S}(G)$ *est formé des $g \in G$ tels que* $\mathrm{Ad}(g) = Id_G$, *c'est-à-dire des $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$, ce qui équivaut à $gh = hg$ pour tout $h \in G$. Le noyau de* Ad *est donc le centre $Z(G)$ de G. Comme* $\mathrm{Im}(\mathrm{Ad}) = \mathrm{Int}(G)$, *on en déduit que $G/Z(G) = G/\ker(\mathrm{Ad})$ est isomorphe à* $\mathrm{Im}(\mathrm{Ad}) = \mathrm{Int}(G)$.

Exemple 4.3 *Un groupe G agit sur tout sous-groupe distingué H par conjugaison :*

$$(g, h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$$

Exemple 4.4 *Le groupe $\mathcal{S}(E)$ agit naturellement sur E par :*

$$(\sigma, x) \in \mathcal{S}(E) \times E \mapsto \sigma \cdot x = \sigma(x) \in E$$

4.2 Orbites et stabilisateurs

Définition 4.2 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in E$, le sous-ensemble de E :*

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

est appelé orbite de x sous l'action de G.

On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur E ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.

Exemple 4.5 *Pour l'action de $\mathcal{S}(E)$ sur E il y a une seule orbite. En effet, pour tout $x \in E$, on a :*

$$\mathcal{S}(E) \cdot x = \{\sigma(x) \mid \sigma \in \mathcal{S}(E)\} = E$$

(tout $y \in E$ s'écrit $y = \tau(x)$, où τ est la transposition $\tau = (x, y)$ si $y \neq x$, $\tau = Id$ si $y = x$).

Exemple 4.6 *Pour l'action de G sur lui même par conjugaison, les orbites sont appelées classes de conjugaison :*

$$\forall h \in G,\ G \cdot h = \left\{ghg^{-1} \mid g \in G\right\}$$

Le groupe G est commutatif si, et seulement si, $G \cdot h = \{h\}$ pour tout $h \in G$.

Exemple 4.7 *Si H est un sous-groupe de G, il agit par translation à droite sur G :*

$$(h, g) \in H \times G \mapsto h \cdot g = gh^{-1}$$

($1 \cdot g = g1 = g$ et $h_1 \cdot (h_2 \cdot g) = \left(gh_2^{-1}\right) h_1^{-1} = g(h_1 h_2)^{-1} = (h_1 h_2) \cdot g$) et pour tout $g \in G$ l'orbite de g est la classe à gauche modulo H :

$$\begin{aligned} H \cdot g &= \{h \cdot g \mid h \in H\} = \left\{gh^{-1} \mid h \in H\right\} \\ &= \{gk \mid k \in H\} = gH \end{aligned}$$

L'ensemble de ces orbites est l'ensemble quotient G/H des classes à gauche modulo H.
En utilisant les translation à gauche sur G :

$$(h, g) \in H \times G \mapsto h \cdot g = hg$$

les orbites sont les classes à droite modulo H :

$$H \cdot g = \{hg \mid h \in H\} = Hg$$

Exemple 4.8 *Soit E un ensemble non vide. Pour $\sigma \in \mathcal{S}(E)$, on fait agir le groupe cyclique $H = \langle\sigma\rangle$ sur E par :*

$$(\sigma^r, x) \in H \times E \mapsto \sigma^r \cdot x = \sigma^r(x)$$

et l'orbite de $x \in E$ pour cette action est l'ensemble :

$$H \cdot x = \{\gamma \cdot x \mid \gamma \in H\} = \{\sigma^r(x) \mid r \in \mathbb{Z}\}$$

On dit $H \cdot x$ est l'orbite de la permutation σ. On note, dans ce contexte, $Orb_\sigma(x)$ une telle orbite.

Un cycle est une permutation $\sigma \in \mathcal{S}(E)$ pour laquelle il n'existe qu'une seule orbite non réduite à un point.

En utilisant le fait que les σ-orbites forment une partition de E et que chaque σ-orbite non réduite à un point permet de définir un cycle, on déduit que toute permutation $\sigma \in \mathcal{S}(E) \backslash \{Id_E\}$ se décompose en produit de cycles de supports deux à deux disjoints (théorème 3.6).

Définition 4.3 *On dit que l'action de G sur E est transitive [resp. simplement transitive] si :*

$$\forall (x, y) \in E^2,\ \exists g \in G \mid y = g \cdot x$$

$$\textit{resp. } \forall (x, y) \in E^2,\ \exists! g \in G \mid y = g \cdot x$$

Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

Définition 4.4 *On dit que l'action de G sur E est fidèle si le morphisme de groupes :*

$$\varphi : g \in G \mapsto (\varphi(g) : x \mapsto g \cdot x) \in \mathcal{S}(E)$$

est injectif, ce qui signifie que :

$$(g \in G \text{ et } \forall x \in E,\ g \cdot x = x) \Leftrightarrow (g = 1)$$

Une action fidèle permet d'identifier G à un sous-groupe de $\mathcal{S}(E)$.

Théorème 4.1 (Cayley) *L'action de G sur lui même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.*

Démonstration. Pour $g \in G$, on a $g \cdot h = gh = h$ pour tout $h \in G$ si, et seulement si, $g = 1$, donc φ est injectif. ■

Exercice 4.2 *On considère, pour $n \geq 1$, l'action de $\mathcal{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$ définie par :*

$$\forall (A, x) \in \mathcal{O}_n(\mathbb{R}) \times \mathbb{R}^n,\ A \cdot x = A(x)$$

Montrer que les orbites sont les sphères de centre 0.

Solution 4.2 *Pour $x \in \mathbb{R}^n$, on a :*

$$\mathcal{O}_n(\mathbb{R}) \cdot x = \{A(x) \mid A \in \mathcal{O}_n(\mathbb{R})\}$$

Pour tout $y \in \mathcal{O}_n(\mathbb{R}) \cdot x$, il existe $A \in \mathcal{O}_n(\mathbb{R})$ telle que $y = A(x)$ et $\|y\| = \|A(x)\| = \|x\|$, donc $\mathcal{O}_n(\mathbb{R}) \cdot x \subset S(0, \|x\|)$.
Réciproquement si $y \in S(0, \|x\|)$ avec $x \neq 0$, on a $y \neq 0$ et on peut construire deux bases orthonormées $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ et $\mathcal{B}' = (e'_i)_{1 \leq i \leq n}$ de $\mathbb{R}^n$ telles que $e_1 = \dfrac{1}{\|x\|}x$ et $e'_1 = \dfrac{1}{\|y\|}y$. La matrice de base de $\mathcal{B}$ à $\mathcal{B}'$ est alors orthogonale et $y = \|y\| e'_1 = \|x\| A(e_1) = A(x)$, donc $y \in \mathcal{O}_n(\mathbb{R}) \cdot x$. On a donc $\mathcal{O}_n(\mathbb{R}) \cdot x = S(0, \|x\|)$ pour $x \neq 0$.
Pour $x = 0$, on a $\mathcal{O}_n(\mathbb{R}) \cdot x = \{0\} = S(0, \|x\|)$.

Exercice 4.3 *Soient n, m deux entiers naturels non nuls et $\mathbb{K}$ un corps commutatif. On fait agir le groupe produit $G = GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$ sur l'ensemble $E = \mathcal{M}_{n,m}(\mathbb{K})$ des matrices à n lignes et m colonnes par :*

$$\forall (P, Q) \in G,\ \forall A \in E,\ (P, Q) \cdot A = PAQ^{-1}$$

Montrer que les orbites correspondantes sont les ensembles :

$$\mathcal{O}_r = \{A \in E \mid \operatorname{rg}(A) = r\}$$

où r est compris entre 0 et $\min(n, m)$.

Solution 4.3 *On rappelle qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est de rang r si et seulement si elle est équivalente à $A_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.*
Rappelons une démonstration de ce résultat.
Pour $r = 0$, on a $A = 0 = A_0$. Pour $r \geq 1$, en désignant par $u \in \mathcal{L}(\mathbb{K}^n)$ l'endomorphisme de matrice A dans la base canonique de $\mathbb{K}^n$, H un supplémentaire de $\ker(u)$ dans $\mathbb{K}^n$, $\mathcal{B}_1 = (e_i)_{1\leq i\leq r}$ une base de H et $\mathcal{B}_2$ une base de $\ker(u)$, le système $u(\mathcal{B}_1) = (u(e_1))_{1\leq i\leq r}$ qui est libre dans $\mathbb{K}^n$ (si $\sum_{k=1}^{r} \lambda_k u(e_k) = 0$, alors $\sum_{k=1}^{r} \lambda_k e_k \in H \cap \ker(u) = \{0\}$ et tous les λ_k sont nuls) se complète en une base $\mathcal{B} = \{u(e_1), \cdots, u(e_r), f_{r+1}, \cdots, f_n\}$ de $\mathbb{K}^n$ et la matrice de u dans les bases $\mathcal{B}_1 \cup \mathcal{B}_2$ et $\mathcal{B}$ a alors la forme indiquée. La réciproque est évidente.
Il en résulte que :

$$\begin{aligned}\mathcal{O}_r &= \{A \in E \mid \operatorname{rg}(A) = r\} \\ &= \left\{A \in E \mid \exists (P,Q) \in G \mid A = PI_rQ^{-1}\right\} = G \cdot I_r\end{aligned}$$

et :

$$E = \bigcup_{r=0}^{\min(n,m)} \mathcal{O}_r = \bigcup_{r=0}^{\min(n,m)} G \cdot I_r$$

ce qui nous donne toutes les orbites.

Définition 4.5 *Soit G un groupe opérant sur un ensemble non vide E. Pour tout $x \in X$, le sous-ensemble de G :*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

est le stabilisateur de x sous l'action de G.

On vérifie facilement que ces stabilisateurs G_x sont des sous-groupes de G (en général non distingués).

Exemple 4.9 *En faisant agir $G = \mathcal{S}(E)$ sur un ensemble E non réduit à un point par $\sigma \cdot x = \sigma(x)$, le stabilisateur de $x \in E$ est isomorphe à $\mathcal{S}(E \setminus \{x\})$. À $\sigma \in G_x$, on associe la restriction σ' de σ à $E \setminus \{x\}$, ce qui définit un isomorphisme de G_x sur $\mathcal{S}(E \setminus \{x\})$.*

Théorème 4.2 *Soit $(G, \cdot)$ est un groupe opérant sur un ensemble E. Pour tout $x \in E$ l'application :*

$$\begin{array}{rccc} \varphi_x : & G/G_x & \to & G \cdot x \\ & \overline{g} = gG_x & \mapsto & g \cdot x \end{array}$$

est bien définie et bijective. Dans le cas où G fini, on a :

$$\operatorname{card}(G \cdot x) = [G : G_x] = \frac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$$

(donc $\operatorname{card}(G \cdot x)$ divise $\operatorname{card}(G)$).

Démonstration. En remarquant que pour g, h dans G et $x \in E$, l'égalité $g \cdot x = h \cdot x$ équivaut à $(h^{-1}g) \cdot x = x$, soit à $h^{-1}g \in G_x$ ou encore à $\overline{g} = \overline{h}$ dans G/G_x, on déduit que l'application φ_x est bien définie et injective. Cette application étant clairement surjective, elle définie une bijection de G/G_x sur $G \cdot x$. Dans le cas où G fini, on a :

$$\operatorname{card}(G \cdot x) = \operatorname{card}(G/G_x) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_x)}$$

■

Exercice 4.4 *En utilisant l'action naturelle de $\mathcal{S}(E)$ sur E, montrer que si E est un ensemble fini à n éléments, on a alors* $\operatorname{card}(\mathcal{S}(E)) = n!$

Solution 4.4 *On utilise l'action de $\mathcal{S}(E)$ sur E définie par :*

$$\forall (\sigma, x) \in \mathcal{S}(E) \times E,\ \sigma \cdot x = \sigma(x)$$

Cette action est transitive (il y a une seule orbite), donc $\mathcal{S}(E) \cdot x = E$ pour tout $x \in E$. Le stabilisateur de $x \in E$ est :

$$\mathcal{S}(E)_x = \{\sigma \in \mathcal{S}(E) \mid \sigma(x) = x\}$$

et l'application qui associe à $\sigma \in \mathcal{S}(E)_x$ sa restriction à $F = E \setminus \{x\}$ réalise un isomorphisme de $\mathcal{S}(E)_x$ sur $\mathcal{S}(F)$. On a donc $\operatorname{card}(\mathcal{S}(E)_x) = \operatorname{card}(\mathcal{S}(F))$ *et :*

$$\begin{aligned}\operatorname{card}(\mathcal{S}(E)) &= \operatorname{card}(\mathcal{S}(E) \cdot x) \operatorname{card}(\mathcal{S}(E)_x) \\ &= \operatorname{card}(E) \operatorname{card}(\mathcal{S}(F)) = n \operatorname{card}(\mathcal{S}(F))\end{aligned}$$

On conclut alors par récurrence sur $n \geq 1$.

4.3 Équation des classes

Théorème 4.3 (équation des classes) *Soit $(G, \cdot)$ est un groupe fini opérant sur un ensemble fini E. En notant $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes, on a :*

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

Démonstration. Si E est fini, on a alors un nombre fini d'orbites $G \cdot x_1, \cdots, G \cdot x_r$ qui forment une partition de E et :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i).$$

En utilisant la bijection de G/G_x sur $G \cdot x_i$, on déduit que si G est aussi fini, on a alors :

$$\operatorname{card}(E) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}.$$

■

Si $(G, \cdot)$ est un groupe opérant sur un ensemble E, on note alors :

$$E^G = \{x \in E \mid G \cdot x = \{x\}\}$$

C'est l'ensemble des éléments de E dont l'orbite est réduite à un point.
En séparant dans la formule des classes les orbites réduites à un point des autres, elle s'écrit :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G \cdot x_i) \geq 2}}^{r} \operatorname{card}(G \cdot x_i)$$

(la somme étant nulle si toutes les orbites sont réduites à un point).

Définition 4.6 *Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où α est un entier naturel non nul.*

Corollaire 4.1 *Si $p \geq 2$ est un nombre premier et $(G, \cdot)$ est un p-groupe opérant sur un ensemble fini E, alors :*

$$\operatorname{card}\left(E^G\right) \equiv \operatorname{card}(E) \pmod{p}.$$

Démonstration. Dans le cas d'un p-groupe de cardinal p^α avec $\alpha \geq 1$, pour toute orbite $G \cdot x_i$ non réduite à un point (s'il en existe), on a :

$$\operatorname{card}(G \cdot x_i) = \operatorname{card}\left(\frac{G}{G_{x_i}}\right) = \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})} \geq 2$$

donc $\operatorname{card}(G_{x_i}) = p^{\beta_i}$ avec $0 \leq \beta_i < \alpha$ et $\operatorname{card}(G \cdot x_i) = p^{\alpha-\beta_i}$ avec $1 \leq \alpha - \beta_i \leq \alpha$. Il en résulte que :

$$\operatorname{card}(E) = \operatorname{card}\left(E^G\right) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot x_i)\geq 2}}^{r} \operatorname{card}(G \cdot x_i) \equiv \operatorname{card}\left(E^G\right) \pmod{p}$$

■

Corollaire 4.2 *Soit G un groupe fini que l'on fait opérer sur lui même par conjugaison ($g \cdot h = ghg^{-1}$, pour $(g, h) \in G \times G$). En notant $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites deux à deux distinctes, on a :*

$$\begin{aligned} \operatorname{card}(G) &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \operatorname{card}(G \cdot h_i) \\ &= \operatorname{card}(Z(G)) + \sum_{\substack{i=1 \\ \operatorname{card}(G\cdot h_i)\geq 2}}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})}. \end{aligned}$$

Démonstration. Une orbite $G \cdot h$ est réduite à $\{h\}$ si et seulement si $ghg^{-1} = h$ pour tout $g \in G$, ce qui revient à dire que $gh = hg$, ou encore que $h \in Z(G)$. On a donc $Z(G) = G^G$ et le résultat annoncé. ■

Théorème 4.4 *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Démonstration. Soit G un p-groupe à p^α éléments.
On a, avec les notations des corollaires qui précèdent :

$$\operatorname{card}(Z(G)) = \operatorname{card}\left(G^G\right) \equiv \operatorname{card}(G) \pmod{p}$$

et comme $\operatorname{card}(Z(G)) \geq 1$, il en résulte que $\operatorname{card}(Z(G)) \geq p$ et $Z(G)$ est non trivial. ■

Théorème 4.5 *Tout groupe d'ordre p^2 avec p premier est commutatif.*

Démonstration. Soit G d'ordre p^2. On sait que $Z(G)$ est non trivial, il est donc de cardinal p ou p^2 et il s'agit de montrer qu'il est de cardinal p^2.
Si $Z(G)$ est de cardinal p, il est alors cyclique, soit $Z(G) = \langle g \rangle$.
Un élément h de $G \setminus Z(G)$ ne pouvant être d'ordre p^2 (sinon $G = \langle h \rangle$ et G serait commutatif ce qui contredit l'hypothèse $G \neq Z(G)$), il est d'ordre p et $Z(G) \cap \langle h \rangle = \{1\}$ (exercice 1.21)

En utilisant l'application :

$$\begin{array}{rccc}\varphi: & \{0,1,\cdots,p-1\}^2 & \to & G \\ & (i,j) & \mapsto & g^ih^j\end{array}$$

nous déduisons que tout élément de G s'écrit de manière unique g^ih^j. Pour ce faire il suffit de montrer que φ est injective. Si $g^ih^j = g^{i'}h^{j'}$, alors $g^{i-i'} = h^{j'-j} \in Z(G) \cap \langle h\rangle = \{1\}$ et $g^{i-i'} = h^{j'-j} = 1$ ce qui entraîne que p divise $i-i'$ et $j-j'$ et comme $|i-i'| < p$, $|j-j'| < p$, on a nécessairement $i = i'$, $j = j'$. Avec les cardinaux il en résulte que φ est une bijection.

Si k, k' sont dans G, il s'écrivent $k = g^ih^j$ et $k' = g^{i'}h^{j'}$ et comme g commute à tout G, on en déduit que k et k' commutent. Le groupe G serait alors commutatif ce qui est contraire à l'hypothèse $G \neq Z(G)$.

En définitive $Z(G)$ ne peut être de cardinal p, il est donc de cardinal p^2 et G est commutatif.

■

Remarque 4.2 *Si G d'ordre p^2 a un élément d'ordre p^2, il est alors cyclique isomorphe à $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$. Dans le cas où tous ses éléments sont d'ordre p, il est isomorphe à $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$.*

4.4 Le théorème de Cauchy

Soient G un groupe fini de cardinal $n \geq 2$, $p \geq 2$ un nombre premier et :

$$E = \{(g_1,\cdots,g_p) \in G^p \mid g_1\cdots g_p = 1\}$$

Lemme 4.1 *Avec ces notations, on a :*

$$\text{card}(E) = n^{p-1}.$$

Démonstration. L'application $(g_1,\cdots,g_{p-1}) \mapsto \left(g_1,\cdots,g_{p-1},(g_1\cdots g_{p-1})^{-1}\right)$ réalise une bijection de G^{p-1} sur E (de l'égalité $g_1\cdots g_p = 1$, on déduit que la connaissance des g_i pour $1 \leq i \leq p-1$ détermine g_p de manière unique). On a donc :

$$\text{card}(E) = n^{p-1}.$$

■

On désigne par $H = \langle\sigma\rangle$ le sous-groupe de $\mathcal{S}_p$ engendré par le p-cycle $\sigma = (1,2,\cdots,p)$ et on fait agir H sur E par :

$$\left(\sigma^k,(g_1,\cdots,g_p)\right) \mapsto \left(g_{\sigma^k(1)},\cdots,g_{\sigma^k(p)}\right)$$

Pour $g = (g_1,\cdots,g_p) \in E$, on a :

$$g_2\cdots g_pg_1 = g_1^{-1}g_1 = 1$$

donc $\left(g_{\sigma(1)},\cdots,g_{\sigma(p)}\right) = (g_2,\cdots,g_p,g_1) \in E$. Il en résulte que pour tout entier k compris entre 0 et $p-1$, $\left(g_{\sigma^k(1)},\cdots,g_{\sigma^k(p)}\right) \in E$ et l'application :

$$\left(\sigma^k,(g_1,\cdots,g_p)\right) \mapsto \sigma^k\cdot(g_1,\cdots,g_p) = \left(g_{\sigma^k(1)},\cdots,g_{\sigma^k(p)}\right)$$

est bien à valeurs dans E. Cette application définit bien une action puisque :

$$Id\cdot(g_1,\cdots,g_p) = (g_1,\cdots,g_p)$$

et

$$\begin{aligned}\sigma^j\cdot\left(\sigma^k\cdot(g_1,\cdots,g_p)\right) &= \sigma^j\cdot\left(g_{\sigma^k(1)},\cdots,g_{\sigma^k(p)}\right) = \left(g_{\sigma^{j+k}(1)},\cdots,g_{\sigma^{k+j}(p)}\right) \\ &= \sigma^{j+k}\cdot(g_1,\cdots,g_p) = \left(\sigma^j\circ\sigma^k\right)\cdot(g_1,\cdots,g_p)\end{aligned}$$

Lemme 4.2 *Avec ces notations, on a :*

$$E^H = \{x \in E \mid H \cdot x = \{x\}\} \neq \emptyset$$

et $\text{card}\left(E^H\right)$ *est divisible par* p *si* p *est un diviseur premier de* n.

Démonstration. En remarquant que $x = (1, \cdots, 1)$ est dans E^H, on déduit que E^H est non vide.

Comme H est de cardinal p (un p-cycle est d'ordre p dans $\mathcal{S}_p$), on a :

$$\text{card}\left(E^H\right) \equiv \text{card}\,(E) \pmod{p}$$

(corollaire 4.1) avec $\text{card}\,(E) = n^{p-1}$ divisible par p comme n, ce qui entraîne que $\text{card}\left(E^H\right)$ est également divisible par p. ■

Théorème 4.6 (Cauchy) *Si* G *est un groupe fini d'ordre* $n \geq 2$, *alors pour tout diviseur premier* p *de* n, *il existe dans* G *un élément d'ordre* p *(et donc un sous-groupe d'ordre* p*).*

Démonstration. On utilise les notations qui précèdent.

De $\text{card}\left(E^H\right) \geq 1$ et $\text{card}\left(E^H\right)$ divisible par p, on déduit que $\text{card}\left(E^H\right) \geq p \geq 2$ et en remarquant que $x = (g_1, \cdots, g_p) \in E^H$ équivaut à dire que $g_1 = \cdots = g_p = g$ avec $g \in G$ tel que $g^p = 1$, on déduit qu'il existe $g \neq 1$ tel que $g^p = 1$, ce qui signifie que g est d'ordre p. ■

Exercice 4.5 *Soit* $(G, \cdot)$ *est un groupe fini opérant sur un ensemble fini* E. *Pour tout* $g \in G$, *on note :*

$$\text{Fix}\,(g) = \{x \in E \mid g \cdot x = x\}$$

Montrer que le nombre d'orbites est :

$$r = \frac{1}{\text{card}\,(G)} \sum_{g \in G} \text{card}\,(\text{Fix}\,(g))$$

(formule de Burnside).

Solution 4.5 *L'idée est de calculer le cardinal de l'ensemble :*

$$F = \{(g, x) \in G \times E \mid g \cdot x = x\}$$

de deux manières en utilisant les partitions :

$$F = \bigcup_{g \in G} \{(g, x) \mid x \in \text{Fix}\,(g)\} = \bigcup_{x \in E} \{(g, x) \mid g \in G_x\}$$

ce qui donne :

$$\text{card}\,(F) = \sum_{g \in G} \text{card}\,(\text{Fix}\,(g))$$

et en notant $G \cdot x_1, \cdots, G \cdot x_r$ *les orbites distinctes :*

$$\begin{aligned}
\text{card}\,(F) &= \sum_{x \in E} \text{card}\,(G_x) = \sum_{x \in E} \frac{\text{card}\,(G)}{\text{card}\,(G \cdot x)} \\
&= \sum_{i=1}^{r} \sum_{x \in G \cdot x_i} \frac{\text{card}\,(G)}{\text{card}\,(G \cdot x)} = \sum_{i=1}^{r} \text{card}\,(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\text{card}\,(G \cdot x)} \right) \\
&= \sum_{i=1}^{r} \text{card}\,(G) \left(\sum_{x \in G \cdot x_i} \frac{1}{\text{card}\,(G \cdot x_i)} \right) = \sum_{i=1}^{r} \text{card}\,(G) = r\,\text{card}\,(G)
\end{aligned}$$

du fait que $G \cdot x = G \cdot x_i$ *pour* $x \in G \cdot x_i$ *(la relation* $x \sim y$ *si* $y = g \cdot x$ *est d'équivalence et les classes d'équivalence sont les orbites). Ce qui donne le résultat annoncé.*

4.5 Le groupe des isométries du cube

On se place dans l'espace vectoriel euclidien $\mathbb{R}^3$ muni d'un repère orthonormé, $A_1, \cdots, A_8$ sont les huit points de coordonnées $(\pm 1, \pm 1, \pm 1)$ et $\mathcal{C}$ est le cube de sommets $A_1, \cdots, A_8$, où $A_1 \cdots A_4$ et $A_5 \cdots A_8$ sont deux faces parallèles, comme indiqué sur la figure 4.1.

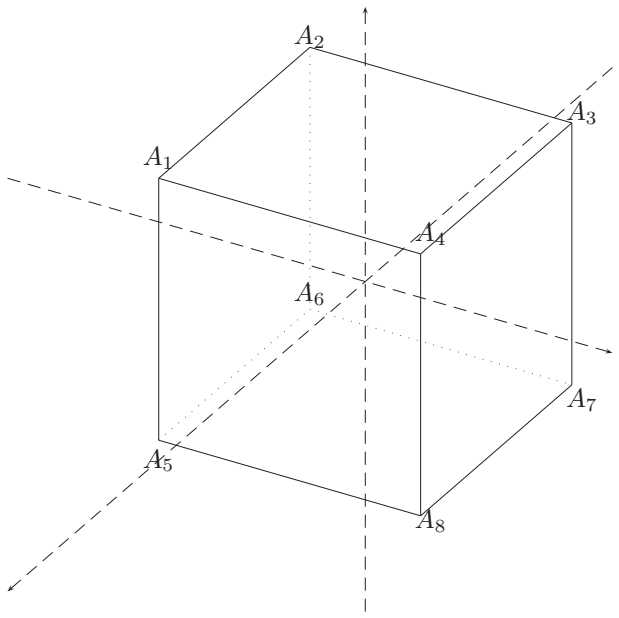

FIG. 4.1 –

On a donc :

$$A_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix},\ A_2 = \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix},\ A_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix},\ A_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

et :

$$A_5 = -A_3,\ A_6 = -A_4,\ A_7 = -A_1,\ A_8 = -A_2$$

De manière précise le cube $\mathcal{C}$ est l'enveloppe convexe de l'ensemble $\mathcal{S} = \{A_1, \cdots, A_8\}$ de ses sommets, c'est-à-dire l'ensemble des combinaisons linéaires convexes $M = \sum_{i=1}^{8} \lambda_i A_i$ avec $\lambda_i \geq 0$ pour tout i compris entre 1 et 8 et $\sum_{i=1}^{8} \lambda_i = 1$ (c'est aussi l'intersection de tous les convexes de $\mathbb{R}^3$ qui contiennent $\mathcal{S}$).

On désigne par $Is(\mathcal{C})$ le groupe des isométries de $\mathbb{R}^3$ qui conservent ce cube, soit :

$$Is(\mathcal{C}) = \left\{\varphi \in \mathcal{O}\left(\mathbb{R}^3\right) \mid \varphi(\mathcal{C}) = \mathcal{C}\right\}$$

par $Is^+(\mathcal{C}) = Is(\mathcal{C}) \cap \mathcal{O}^+(\mathbb{R}^3)$ le sous-groupe de $\mathcal{O}(\mathbb{R}^3)$ formé des rotations qui conservent $\mathcal{C}$ et par $Is^-(\mathcal{C}) = Is(\mathcal{C}) \cap \mathcal{O}^-(\mathbb{R}^3)$ le sous-ensemble de $\mathcal{O}(\mathbb{R}^3)$ formé des isométries indirectes qui conservent $\mathcal{C}$.

Théorème 4.7 *Le groupe $Is(\mathcal{C})$ des isométries qui conservent le cube $\mathcal{C}$ est aussi le groupe $Is(\mathcal{S})$ des isométries qui conservent l'ensemble $\mathcal{S}$ de ses sommets et c'est un groupe fini isomorphe à un sous groupe du groupe symétrique $\mathcal{S}_8$. La symétrie de centre 0, $\sigma_0 : x \mapsto -x$, est dans $Is^-(\mathcal{C})$, l'application $\rho \mapsto \rho \circ \sigma_0$ réalise une bijection de $Is^+(\mathcal{C})$ sur $Is^-(\mathcal{C})$ et :*

$$\operatorname{card}(Is(\mathcal{C})) = 2\operatorname{card}\left(Is^+(\mathcal{C})\right).$$

Démonstration. En écrivant que $\mathcal{S} = \mathcal{C} \cap S\left(0, \sqrt{3}\right)$, où $S\left(0, \sqrt{3}\right)$ est la sphère de centre 0 et de rayon $\|A_k\| = \sqrt{3}$ et en remarquant que cette sphère est conservée par toute isométrie, on déduit que pour toute isométrie $\varphi \in Is(\mathcal{C})$, on a :

$$\varphi(\mathcal{S}) = \varphi\left(\mathcal{C} \cap S\left(0, \sqrt{3}\right)\right) = \varphi(\mathcal{C}) \cap \varphi\left(S\left(0, \sqrt{3}\right)\right) = \mathcal{C} \cap S\left(0, \sqrt{3}\right) = \mathcal{S}$$

Réciproquement si φ est isométrie qui conserve $\mathcal{S}$, elle conserve $\mathcal{C}$. En effet, pour tout $M = \sum_{i=1}^{8} \lambda_i A_i \in \mathcal{C}$, on a :

$$\varphi(M) = \sum_{i=1}^{8} \lambda_i \varphi(A_i) = \sum_{i=1}^{8} \lambda_i A_{\sigma(i)} = \sum_{j=1}^{8} \lambda_{\sigma^{-1}(j)} A_j \in \mathcal{C}$$

et :

$$M = \varphi\left(\sum_{i=1}^{8} \lambda_i \varphi^{-1}(A_i)\right) = \varphi\left(\sum_{i=1}^{8} \lambda_i A_{\sigma^{-1}(i)}\right) = \varphi\left(\sum_{j=1}^{8} \lambda_{\sigma(j)} A_j\right) \in \varphi(\mathcal{C})$$

où $\sigma \in \mathcal{S}_8$.

On a donc :

$$Is(\mathcal{C}) = Is(\mathcal{S})$$

En associant à toute isométrie $\varphi \in Is(\mathcal{S})$, la permutation des sommets :

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5 & A_6 & A_7 & A_8 \\ \varphi(A_1) & \varphi(A_2) & \varphi(A_3) & \varphi(A_4) & \varphi(A_5) & \varphi(A_6) & \varphi(A_7) & \varphi(A_8) \end{pmatrix}$$

et en notant, pour k compris entre 1 et 8, $\varphi(A_k) = A_{\sigma_\varphi(k)}$ où $\sigma_\varphi \in \mathcal{S}_8$, l'application $\varphi \mapsto \sigma_\varphi$ réalise un morphisme de groupes injectif de $Is(\mathcal{C})$ dans $\mathcal{S}_8$. En effet, il est clair que cette application est un morphisme de groupes et si $\sigma_\varphi = Id$, on a alors $\varphi(A_k) = A_k$ pour $k = 1, 2, 3$ et $\varphi = Id_{\mathbb{R}^3}$ puisque (A_1, A_2, A_3) est une base de $\mathbb{R}^3$.

Il en résulte que $Is(\mathcal{C}) = Is(\mathcal{S})$ est un groupe fini isomorphe à un sous-groupe de $\mathcal{S}_8$.

Il est clair que $\sigma_0 \in Is(\mathcal{S})$ et avec $\det(\rho \circ \sigma_0) = \det(\rho)\det(\sigma_0) = -1$ pour tout $\rho \in Is^+(\mathcal{C})$, on déduit que l'application $\rho \mapsto \rho \circ \sigma_0$ va de $Is^+(\mathcal{C})$ dans $Is^-(\mathcal{C})$. Comme σ_0 est d'ordre 2, on en déduit que cette application est bijective. En effet $\rho \circ \sigma_0 = \rho' \circ \sigma_0$ donne $\rho = \delta \circ \sigma_0^2 = \rho' \circ \sigma_0^2 = \rho'$ et pour $\sigma \in Is^-(\mathcal{C})$, on a $\rho = \sigma \circ \sigma_0 \in Is^+(\mathcal{C})$ et $\rho \circ \sigma_0 = \sigma$. On a donc $\operatorname{card}(Is^+(\mathcal{C})) = \operatorname{card}(Is^-(\mathcal{C}))$ et avec la partition $Is(\mathcal{S}) = Is^+(\mathcal{C}) \cup Is^-(\mathcal{C})$, on en déduit que $\operatorname{card}(Is(\mathcal{C})) = 2\operatorname{card}(Is^+(\mathcal{C}))$. ■

La description de $Is(\mathcal{C}) = Is(\mathcal{S})$ passe donc par celle de $Is^+(\mathcal{C}) = Is^+(\mathcal{S})$.

Remarque 4.3 *Si on s'intéresse aux isométries qui conservent un cube dans un espace affine euclidien, en remarquant que le centre du cube, qui est l'isobarycentre des sommets, est un point fixe de toute isométrie $\varphi \in Is(\mathcal{C})$, on est ramené au cas vectoriel.*

En fait, de manière plus générale, on peut remarquer qu'une application affine qui conserve le cube est nécessairement une isométrie.

Exercice 4.6 *Soit $\mathcal{C}$ un cube dans l'espace affine euclidien $\mathbb{R}^3$.*

1. *Montrer que si φ est une application affine qui conserve le cube, c'est alors un automorphisme.*
2. *Montrer que le groupe $GA(\mathcal{C})$ des applications affines qui conservent le cube est contenu dans le groupe $Is(\mathbb{R}^3)$ des isométries de $\mathbb{R}^3$.*
   On a donc $GA(\mathcal{C}) = Is(\mathcal{C})$.

Solution 4.6

1. *De $\varphi(\mathcal{C}) = \mathcal{C}$, on déduit que $\varphi(\mathcal{C})$ contient un repère affine de $\mathbb{R}^3$, elle est donc surjective et c'est une bijection affine.*
2. *On utilise le repère orthonormé $\mathcal{R} = \left(A_1, \overrightarrow{A_1A_2'}, \overrightarrow{A_1A_4'}, \overrightarrow{A_1A_5'}\right)$, où $\overrightarrow{A_1A_k'} = \dfrac{1}{A_1A_k}\overrightarrow{A_1A_k}$ pour $k = 2, 4, 5$.*
   Si φ est une bijection affine qui conserve le cube, l'image du plan $\mathcal{P}$ qui contient la face $A_1A_2A_3A_4$ est un plan, $\varphi(\mathcal{C})$ est dans l'un des demi-espaces délimités par $\varphi(\mathcal{P})$ et comme $\varphi(\mathcal{C}) = \mathcal{C}$, il est aussi dans l'un des demi-espaces délimités par $\mathcal{P}$, donc une face de $\mathcal{C}$ est transformé en face et le repère $\mathcal{R}$ est transformé en un repère orthonormé. En définitive, φ est une isométrie.

L'application :

$$(\varphi, A_k) \in Is^+(\mathcal{S}) \times \mathcal{S} \mapsto \varphi(A_k)$$

définit une action du groupe $Is^+(\mathcal{S})$ sur $\mathcal{S}$. Pour calculer le cardinal de $Is^+(\mathcal{S})$ nous allons décrire le stabilisateur $Is^+(\mathcal{S})_{A_k}$ et l'orbite $Is^+(\mathcal{S}) \cdot A_k$ d'un sommet et utiliser la formule :

$$\operatorname{card}\left(Is^+(\mathcal{S})\right) = \operatorname{card}\left(Is^+(\mathcal{S})_{A_k}\right) \operatorname{card}\left(Is^+(\mathcal{S}) \cdot A_k\right)$$

Exercice 4.7 *Montrer que la rotation $\rho = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$ est dans le stabilisateur $Is^+(\mathcal{S})_{A_1}$.*

Solution 4.7 *Avec $\rho \neq Id_{\mathbb{R}^3}$, $\rho\ {}^t\rho = Id_{\mathbb{R}^3}$ et $\det(\rho) = 1$, on déduit que ρ est une rotation d'angle non nul (modulo 2π).*
L'axe de cette rotation est obtenu en résolvant le système linéaire $(\rho - Id_{\mathbb{R}^3})X = 0$, soit :

$$\begin{cases} -x + z = 0 \\ -x - y = 0 \\ -y - z = 0 \end{cases}$$

ce qui donne $x = -y = z$ et l'axe D de u est la droite dirigée par $A_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$.

Avec $\operatorname{Tr}(u) = 0 = 2\cos(\theta) + 1$, on déduit que $\cos(\theta) = -\dfrac{1}{2}$ et $\theta = \pm\dfrac{2\pi}{3}$.

Avec $\rho(A_1) = A_1$ et $\rho(A_k) = \begin{pmatrix} \pm 1 \\ \mp 1 \\ \mp 1 \end{pmatrix}$ pour $A_k = \begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix}$, on déduit que $\rho \in Is^+(\mathcal{S})_{A_1}$.

Précisément, on a :

$$\rho(A_2) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = A_4,\ \rho(A_3) = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} = A_8,\ \rho(A_4) = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} = A_5$$

et :

$$\rho(A_5) = -\rho(A_3) = A_2,\ \rho(A_6) = -\rho(A_4) = A_3,\ \rho(A_7) = -\rho(A_1) = A_7,\ \rho(A_8) = -\rho(A_2) = A_6$$

Sa représentation dans $\mathcal{S}_8$ étant :

$$\sigma = (2,4,5)(3,8,6)$$

Lemme 4.3 *Pour tout sommet A_k du cube $\mathcal{C}$ ($1 \leq k \leq 8$), l'orbite sous l'action de $Is^+(\mathcal{S})$ est :*

$$Is^+(\mathcal{S}) \cdot A_k = \mathcal{S}$$

Il y a donc une seule orbite et l'action de $Is^+(\mathcal{S})$ sur $\mathcal{S}$ est transitive.

Démonstration. On rappelle que :

$$Is^+(\mathcal{S}) \cdot A_k = \left\{\varphi(A_k) \mid \varphi \in Is^+(\mathcal{S})\right\} \subset \mathcal{S}$$

En désignant par $\rho_1 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ la rotation d'axe Oz et d'angle de mesure $-\frac{\pi}{2}$ et par $\rho_2 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ la rotation d'axe Oy et d'angle de mesure $\frac{\pi}{2}$, on a :

$$\rho_1(A_k) = A_{k+1} \text{ pour } k = 1,2,3,5,6,7 \text{ et } \rho_1(A_4) = A_1,\ \rho_1(A_8) = A_8$$

et :

$$\rho_2(A_1) = A_2,\ \rho(A_2) = A_6,\ \rho(A_6) = A_5,\ \rho(A_5) = A_1$$
$$\rho_2(A_4) = A_3,\ \rho(A_3) = A_7,\ \rho(A_7) = A_8,\ \rho(A_8) = A_4$$

ce qui se voit mieux en disant que ρ_1 et ρ_2 sont associées aux permutations :

$$\sigma_1 = (1,2,3,4)(5,6,7,8) \text{ et } \sigma_2 = (1,2,6,5)(4,3,7,8)$$

Utilisant ces rotations, on a :

$$A_1 = Id(A_1),\ A_2 = \rho_1(A_1),\ A_3 = \rho_1^2(A_1),\ A_4 = \rho_1^3(A_1)$$
$$A_5 = \rho_2^3(A_1),\ A_6 = \rho_2^2(A_1),\ A_7 = \rho_2\rho_1^2(A_1),\ A_8 = \rho_2^2\rho_1^2(A_1)$$

et donc $Is^+(\mathcal{C}) \cdot A_1 = \mathcal{S}$.

Comme ces orbites forment une partition de $\mathcal{S}$, on en déduit que $Is^+(\mathcal{S}) \cdot A_k = \mathcal{S}$ pour tout k. ∎

Lemme 4.4 *Une rotation $\varphi \in \mathcal{O}^+(\mathbb{R}^3)$ est uniquement déterminée par $\varphi(A_1)$ et $\varphi(A_2)$ (ou plus généralement par les images de deux sommets d'une même arête).*

Démonstration. Si $\varphi \in \mathcal{O}^+(\mathbb{R}^3)$ est telle que $\varphi(A_1) = A_1$ et $\varphi(A_2) = A_2$, sa restriction au plan engendré par A_1 et A_2 est l'identité et $\varphi = Id_{\mathbb{R}^3}$ du fait que l'ensemble des points fixes d'une rotation distincte de $Id_{\mathbb{R}^3}$ est une droite.

Si φ, ψ dans $\mathcal{O}^+(\mathbb{R}^3)$ sont telles que $\varphi(A_1) = \psi(A_1)$ et $\varphi(A_2) = \psi(A_2)$, on a alors $\varphi^{-1} \circ \psi(A_1) = A_1$ et $\varphi^{-1} \circ \psi(A_2) = A_2$ avec $\varphi^{-1} \circ \psi \in \mathcal{O}^+(\mathbb{R}^3)$, donc $\varphi^{-1} \circ \psi = Id_{\mathbb{R}^3}$ et $\varphi = \psi$. ∎

Lemme 4.5 *Pour tout sommet A_k du cube $\mathcal{C}$ ($1 \leq k \leq 8$), le stabilisateur de A_k sous l'action de $Is^+(\mathcal{S})$ est un sous-groupe d'ordre 3 de $Is^+(\mathcal{S})$.*

Démonstration. On peut supposer que $k = 1$ (quitte à réordonner les sommets).

Si $\varphi \in Is^+(\mathcal{S})_{A_1}$, elle uniquement déterminée par $\varphi(A_2)$ et avec $\left\|\overrightarrow{A_1\varphi(A_2)}\right\| \left\|\varphi\left(\overrightarrow{A_1A_2}\right)\right\| = \left\|\overrightarrow{A_1A_2}\right\| = \sqrt{2}$, on déduit que $\varphi(A_2) \in \{A_2, A_4, A_5\}$ (on a $\left\|\overrightarrow{A_1A_j}\right\| > \sqrt{2}$ pour $j \notin \{2,4,5\}$). Il en résulte que $\text{card}\left(Is^+(\mathcal{S})_{A_1}\right) \leq 3$.

La rotation $\rho = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$ d'axe dirigé par A_1 et d'angle $\frac{2\pi}{3}$ ou $-\frac{2\pi}{3}$ étant dans $Is^+(\mathcal{S})_{A_1}$ et d'ordre 3, on en déduit que $Is^+(\mathcal{S})_{A_1}$ est d'ordre 3 engendré par ρ. ∎

On en déduit alors le résultat suivant.

Théorème 4.8 *Le groupe $Is(\mathcal{S})$ agit de façon transitive sur $\mathcal{S}$ et a 48 éléments.*
Le groupe $Is^+(\mathcal{S})$ est isomorphe à $\mathcal{S}_4$ et le groupe $Is(\mathcal{S})$ est isomorphe à $\mathcal{S}_4 \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Démonstration. Comme $Is^+(\mathcal{S})$ agit de façon transitive sur $\mathcal{S}$, il en est de même de $Is(\mathcal{S})$.

On a :

$$\text{card}\left(Is^+(\mathcal{S})\right) = \text{card}\left(Is^+(\mathcal{S})_{A_1}\right) \text{card}\left(Is^+(\mathcal{S}) \cdot A_1\right) = 3 \times 8 = 24$$

et $\text{card}(Is(\mathcal{S})) = 2\,\text{card}(Is^+(\mathcal{S})) = 48$.

On vérifie ensuite que tout élément φ de $Is(\mathcal{S})$ induit une permutation de l'ensemble $\mathcal{D} = \{[A_1, A_7], [A_2, A_8], [A_3, A_5], [A_4, A_6]\}$ des grandes diagonales du cube, ce qui permet de définir un morphisme de groupes Φ de $Is(\mathcal{S})$ dans $\mathcal{S}(\mathcal{D})$.

Par conservation des normes par une isométrie, une diagonale est transformée en diagonale de même longueur, donc $\mathcal{D}$ est globalement invariant par tout élément de $Is(\mathcal{S})$ et l'application Φ qui associe à $\varphi \in Is(\mathcal{S})$ la permutation correspondante des grandes diagonales réalise un morphisme de groupes de $Is(\mathcal{S})$ dans $\mathcal{S}(\mathcal{D})$.

Si $\varphi \in \ker(\Phi)$, elle conserve alors chaque diagonale. On a donc $\varphi(A_1) = A_1$ ou $\varphi(A_1) = A_7$ et même chose pour les autres grandes diagonales.

Si $\varphi(A_1) = A_1$, on a alors $\varphi([A_1, A_2]) = [A_1, A_k]$ avec $k = 2, 4$ ou 5 puisque les arêtes sont conservées et $\varphi(A_2) = A_2$ puisque la diagonale $[A_2, A_8]$ est conservée. De même, on a $\varphi(A_4) = A_4$ et $\varphi = Id$ puisqu'elle laisse fixe la base (A_1, A_2, A_4).

Si $\varphi(A_1) = A_7$, on a alors $\varphi([A_1, A_2]) = [A_7, A_k]$ avec $k = 3, 6$ ou 8 puisque les arêtes sont conservées et $\varphi(A_2) = A_8$ puisque la diagonale $[A_2, A_8]$ est conservée. De même, on a $\varphi(A_4) = A_6$. Donc φ est la symétrie $\sigma_0 = -Id_{\mathbb{R}^3}$, puisque ces deux isométries coïncident sur la base (A_1, A_2, A_4).

En définitive, $\ker(\Phi) = \{Id_{\mathbb{R}^3}, -Id_{\mathbb{R}^3}\}$ et $\ker\left(\Phi_{|Is^+(\mathcal{S})}\right) = \{Id_{\mathbb{R}^3}\}$.

Il en résulte que $\Phi_{|Is^+(\mathcal{S})}$ est un morphisme injectif de $Is^+(\mathcal{S})$ dans $\mathcal{S}(\mathcal{D})$ et c'est un isomorphisme puisque ces deux groupes ont même cardinal. Le groupe $\mathcal{S}(\mathcal{D})$ étant isomorphe à $\mathcal{S}_4$, il en est de même pour $Is^+(\mathcal{S})$.

En désignant par θ un isomorphisme de groupes de $\mathcal{S}_4$ sur $Is^+(\mathcal{S})$, l'application :

$$\begin{array}{rccc} \Psi : & \{-1,1\} \times \mathcal{S}_4 & \to & Is(\mathcal{S}) \\ & (\varepsilon, \sigma) & \mapsto & \varepsilon\theta(\sigma) \end{array}$$

est un morphisme de groupes surjectif. En effet, pour (ε, σ) et (ε', σ') dans $\{-1,1\} \times \mathcal{S}_4$, on a

$$\Psi((\varepsilon, \sigma)(\varepsilon', \sigma')) = (\varepsilon\varepsilon', \sigma\sigma') = \varepsilon\varepsilon'\theta(\sigma\sigma') = \varepsilon\theta(\sigma)\varepsilon'\theta(\sigma')$$

et pour $\varphi \in Is^+(\mathcal{S})$ [resp. $\varphi \in Is^-(\mathcal{S})$], on a $\varphi = \Psi((1,\theta^{-1}(\varphi)))$ [resp. $-\varphi \in Is^+(\mathcal{S})$ et $\varphi = \Psi((-1,\theta^{-1}(-\varphi)))$]. Comme ces groupes ont même cardinal, Ψ est un isomorphisme. ■

En fait, en utilisant le fait qu'une isométrie qui conserve le cube va conserver les grandes diagonales, on en déduit facilement le cardinal de $Is(\mathcal{S})$ (voir l'exercice 3.42).

On peut donner la liste de tous les éléments de $Is^+(\mathcal{S})$ en fonction de leurs ordres.

Comme élément d'ordre 1, il n'y a que $Id_{\mathbb{R}^3}$.

Comme éléments d'ordre 2, on a les 3 rotations d'axes respectifs Ox, Oy et Oz (ce sont les axes qui passent par le milieu de deux faces opposées), d'angle de mesure π (retournements) :

$$\rho_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ \rho_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et les 6 rotations d'axes respectivement dirigés par les milieux des arêtes $[A_1,A_4]$, $[A_1,A_2]$, $[A_2,A_3]$, $[A_3,A_4]$, $[A_1,A_4]$, $[A_1,A_5]$, $[A_4,A_8]$, d'angle de mesure π.

Elles correspondent aux permutations :

$$(1,8)(2,7)(3,6)(4,5),\ \cdots$$

Comme éléments d'ordre 3, on à les 8 rotations d'axes respectifs les 4 grandes diagonales et d'angles de mesure $\pm\dfrac{2\pi}{3}$.

Comme éléments d'ordre 4, on a les 6 rotations d'axes respectifs Ox, Oy et Oz, d'angles de mesure $\pm\dfrac{\pi}{2}$.

Ce qui donne un total de $1+9+8+6=24$ et on les a toutes.

4.6 Sous groupes finis de $\mathcal{O}^+(E)$ pour $\dim(E)=2$ et $\dim(E)=3$

On désigne par $(E,\langle\cdot\mid\cdot\rangle)$ un espace euclidien de dimension $n\geq 2$, par $S=\{x\in E\mid \|x\|=1\}$ la sphère unité de E et par $\mathcal{O}(E)$ le groupe orthogonal de E (ou groupe des isométries de E). On rappelle que :

$$(u\in\mathcal{O}(E)) \Leftrightarrow (u\in GL(E) \text{ et } \forall x\in E,\ \|u(x)\|=\|x\|)$$

$\mathcal{O}^+(E)$ est le sous-groupe de $\mathcal{O}(E)$ formé des automorphismes orthogonaux positifs (ou rotations vectorielles).

Lemme 4.6 *L'application* $(u,x)\in\mathcal{O}^+(E)\times S\mapsto u\cdot x=u(x)$ *définit une action transitive de* $\mathcal{O}^+(E)$ *sur* S.

Démonstration. Comme $u\in\mathcal{O}^+(E)$ conserve la norme, on a $u(x)\in S$ pour tout $x\in S$ et il est clair qu'on a une action.

Dire que cette action est transitive revient à dire que pour tous x,y dans S, il existe une rotation $u\in\mathcal{O}^+(E)$ telle que $y=u(x)$.

Si $x=\pm y$, $u=\pm Id$ convient, sinon on désigne par H le plan vectoriel engendré par $\{x,y\}$. Comme (x,y) est lié, on a $|\langle x\mid y\rangle|<\|x\|\,\|y\|=1$ et il existe un unique réel $\theta\in\,]-\pi,\pi[$ tel que $\cos(\theta)=\langle x\mid y\rangle$. Une base orthonormée de H est donnée par le procédé de Gram-Schmidt :

$$e_1=x,\ e_2=\frac{\pm 1}{\|y-\langle x\mid y\rangle x\|}(y-\langle x\mid y\rangle x)=\frac{1}{\sin(\theta)}(y-\cos(\theta)x)$$

et on complète cette base en une base orthonormée $(e_i)_{1\leq i\leq n}$ de E. La rotation v du plan H ayant pour matrice :

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

dans la base (e_1, e_2) est telle que $v(x) = v(e_1) = \cos(\theta)\, e_1 + \sin(\theta)\, e_2 = y$ et la rotation $u \in \mathcal{O}^+(E)$ définie par $u(e_k) = v(e_k)$ pour $k = 1, 2$ et $u(e_k) = e_k$ pour $k = 3, \cdots, n$ convient. ■

Du lemme précédent, on déduit aussi que l'application $(u, x) \in \mathcal{O}(E) \times S \mapsto u \cdot x = u(x)$ définit une action transitive de $\mathcal{O}(E)$ sur S.

Comme l'action de $\mathcal{O}^+(E)$ sur S est transitive, S est l'unique orbite et pour tout $x \in S$, l'ensemble quotient $\mathcal{O}^+(E) / (\mathcal{O}^+(E))_x$ est en bijection avec S.

4.6.1 Le cas de la dimension 2

On suppose ici que $\dim(E) = 2$.

Lemme 4.7 *Pour tout $x \in S$, on a $(\mathcal{O}^+(E))_x = \{Id\}$ (on dit que l'action de $\mathcal{O}^+(E)$ sur S est simple) et en conséquence $\mathcal{O}^+(E)$ est en bijection avec S.*

Démonstration. Le vecteur nul est l'unique point fixe d'une rotation $u \neq Id$ d'un plan euclidien E (ce qui se vérifie facilement en utilisant la représentation matricielle d'une rotation du plan dans une base orthonormée). ■

Théorème 4.9 *Tout sous groupe d'ordre n de $\mathcal{O}^+(E)$ est cyclique, donc isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.*

Démonstration. $\mathcal{O}^+(E)$ est en bijection avec S lui même en bijection avec le groupe Γ des nombres complexes de module égal à 1 (une base orthonormée (e_1, e_2) de E étant choisie tout élément de S s'écrit $x = x_1 e_1 + x_2 e_2$ avec $x_1^2 + x_2^2 = 1$ et l'application $x \mapsto x_1 + i x_2$ est bijection de S sur Γ) et on connaît les sous-groupes finis de Γ (exercice 2.3). ■

4.6.2 Le cas de la dimension 3

On suppose ici que $\dim(E) = 3$.

Lemme 4.8 *Toute rotation $u \neq Id$ a exactement deux points fixes x et $-x$ dans S.*

Démonstration. Résulte du fait que, pour $\dim(E) = 3$, l'ensemble des points fixes de $u \in \mathcal{O}^+(E) \setminus \{Id\}$ est une droite $D = \mathbb{R}x$ avec $x \in S$ (voir la leçon sur les isométries d'un espace euclidien de dimension 2 ou 3 au chapitre 17) et $D \cap S = \{-x, x\}$. ■

Définition 4.7 *Les points fixes x et $-x$ dans S d'une rotation $u \neq Id$ d'un espace euclidien de dimension 3 sont appelés les pôles de u.*

On se donne un sous-groupe fini G de $\mathcal{O}^+(E)$ de cardinal $n \geq 2$ et on note P l'ensemble des pôles des éléments de $G \setminus \{Id\}$.

L'ensemble P est fini avec :

$$2 \leq \operatorname{card}(P) \leq 2(n-1).$$

L'action de $\mathcal{O}^+(E)$ sur S que nous avons considéré induit une action de G sur S.

Lemme 4.9 *L'application* $(u,x)\in G\times P\mapsto u\cdot x=u(x)$ *définit une action de* G *sur* P *et le nombre d'orbites pour cette action est* 2 *ou* 3.

Démonstration. Pour $(u,x)\in G\times P$, il existe une rotation $v\in G\setminus\{Id\}$ telle que $\{-x,x\}$ soit l'ensemble des points fixes de v dans S et on a :

$$\left(u\circ v\circ u^{-1}\right)(u(x))=u(v(x))=u(x)$$

c'est-à-dire que $u(x)$ est un pôle de $u\circ v\circ u^{-1}\in G\setminus\{Id\}$ ($u\circ v\circ u^{-1}=Id$ si, et seulement si, $v=Id$), donc $u(x)\in P$ et G agit sur P.

En notant, pour tout $u\in G$:

$$\mathrm{Fix}(u)=\{x\in P\mid u(x)=x\}$$

le théorème de Burnside nous dit que le nombre d'orbites pour cette action de G sur P est :

$$r=\frac{1}{\mathrm{card}(G)}\sum_{u\in G}\mathrm{card}(\mathrm{Fix}(u))=\frac{1}{n}(\mathrm{card}(P)+2(n-1))$$

(pour $u=Id$, $\mathrm{Fix}(u)=P$ et pour $u\neq Id$, $\mathrm{Fix}(u)$ a exactement deux éléments).

Tenant compte du fait que $2\leq\mathrm{card}(P)\leq 2(n-1)$, on a :

$$2\leq r\leq 4\left(1-\frac{1}{n}\right)<4$$

donc $r=2$ ou $r=3$. ∎

Définition 4.8 *L'ordre d'un pôle* $x\in P$ *sous l'action de* G *est le cardinal du stabilisateur* G_x.

Théorème 4.10 *Dans le cas où le nombre d'orbites, pour l'action de* G *sur* P, *est* $r=2$, *le groupe* G *est cyclique d'ordre* n, *donc isomorphe à* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration. Pour $r=2$, la formule de Burnside nous dit que :

$$\mathrm{card}(P)+2(n-1)=2n$$

et $\mathrm{card}(P)=2$, soit $P=\{-x,x\}$, ce qui signifie que toutes les rotations de $G\setminus\{Id\}$ ont le même axe $D=\mathbb{R}x$. Ces rotations laissent stable le plan $H=P^{\perp}$ et l'application qui associe à $u\in G$ sa restriction à H réalise un isomorphisme de G sur un sous groupe d'ordre n de $\mathcal{O}^+(H)$ qui est cyclique d'ordre n. ∎

On suppose maintenant que le nombre d'orbites, pour l'action de G sur P, est $r=3$.

Théorème 4.11 *Dans le cas où le nombre d'orbites, pour l'action de* G *sur* P, *est* $r=3$, *le groupe* G *est isomorphe soit à* $\mathcal{D}_n$ *(groupe diédral d'ordre* n*), soit à* $\mathcal{A}_4$, *soit à* $\mathcal{S}_4$, *soit à* $\mathcal{A}_5$.

Démonstration. La formule de Burnside nous dit que :

$$\mathrm{card}(P)+2(n-1)=3n$$

soit que $\mathrm{card}(P)=n+2$.

On note $G\cdot x_k$ ces orbites avec $x_k\in P$ pour $k=1,2,3$ et :

$$n_k=\mathrm{card}(G\cdot x_k),\ m_k=\mathrm{card}(G_{x_k})=\frac{\mathrm{card}(G)}{\mathrm{card}(G\cdot x_k)}=\frac{n}{n_k}.$$

Comme chaque $x_k \in P$ est point fixe de Id et d'une rotation de $G \setminus \{Id\}$, on a $2 \leq m_k \leq n$. La formule des classes nous donne :

$$\operatorname{card}(P) = n + 2 = \sum_{k=1}^{3} \operatorname{card}(G \cdot x_k) = \sum_{k=1}^{3} \frac{n}{m_k}$$

ou encore :

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

En ordonnant ces orbites de sorte que $m_1 \leq m_2 \leq m_3$, on a :

$$1 < 1 + \frac{2}{n} \leq \frac{3}{m_1}$$

donc $m_1 < 3$ et $m_1 = 2$. Il en résulte que :

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

donc $2 \leq m_2 < 4$ et $m_2 = 2$ ou 3.

Pour $m_2 = 2$, on a $m_3 = \dfrac{n}{2}$ (n est donc nécessairement pair) et pour $m_2 = 3$, on a $\dfrac{1}{m_3} = \dfrac{1}{6} + \dfrac{2}{n} > \dfrac{1}{6}$ avec $m_3 \geq m_2 = 3$ donc $m_3 = 3, 4$ ou 5.

En définitive, les seules possibilités sont :

$m_1 = 2$, $m_2 = 2$, $m_3 = \dfrac{n}{2} \geq 2$, donc $n \geq 4$;

$m_1 = 2$, $m_2 = 3$, $m_3 = 3$, $\dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{3} = 1 + \dfrac{2}{n}$, donc $n = 12$ et $n_1 = 6$, $n_2 = n_3 = 4$;

$m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $\dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{4} = 1 + \dfrac{2}{n}$, donc $n = 24$ et $n_1 = 12$, $n_2 = 8$, $n_3 = 6$;

$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $\dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{5} = 1 + \dfrac{2}{n}$, donc $n = 60$ et $n_1 = 30$, $n_2 = 20$, $n_3 = 12$.

1. Pour $m_1 = m_2 = 2$, on a :

$$n_3 = \operatorname{card}(P) - n_1 - n_2 = n + 2 - \frac{n}{2} - \frac{n}{2} = 2$$

soit $G \cdot x_3 = \{x_3, -x_3\}$ et les rotations $u \in G_{x_3}$ ont toutes le même axe $\mathbb{R}x_3$, donc G_{x_3} est cyclique d'ordre $m_3 = \dfrac{n}{2}$. Le groupe quotient G/G_{x_3} est alors d'ordre 2, il existe donc $\sigma \notin G_{x_3}$ tel que $G/G_{x_3} = \langle \overline{\sigma} \rangle = \{G_{x_3}, \sigma G_{x_3}\}$ et on a la partition $G = G_{x_3} \cup \sigma G_{x_3}$. Comme G_{x_3} est cyclique d'ordre m_3, on a $G_{x_3} = \langle \rho \rangle = \{Id, \rho, \cdots, \rho^{m_3 - 1}\}$ et :

$$G = \left\{Id, \rho, \cdots, \rho^{m_3-1}\right\} \cup \left\{\sigma, \sigma\rho, \cdots, \sigma\rho^{m_3-1}\right\}.$$

Pour toute rotation $u \in G \setminus G_{x_3}$ on a $u(x_3) \in G \cdot x_3 = \{x_3, -x_3\}$ avec $u(x_3) \neq x_3$, donc $u(x_3) = -x_3$ et si $x \in P \setminus \{x_3, -x_3\}$ est un pôle de u, on a $u^2(y) = y$ pour $y \in \{x_3, -x_3, x\}$, donc $u^2 = Id$ puisqu'il a au moins trois points fixes distincts dans S. On a donc $\sigma^2 = Id$ et $(\rho\sigma)^2 = Id$ ($\rho\sigma(x_3) = \rho(-x_3) = -x_3 \neq x_3$, donc $\rho\sigma \in G \setminus G_{x_3}$) et G est un groupe diédral d'ordre n.

2. Pour $m_1 = 2$, $m_2 = 3$, $m_3 = 3$, on a $n = 12$ et $n_1 = 6$, $n_2 = n_3 = 4$.
L'orbite $G \cdot x_2$ étant stable par toute rotation $u \in G$ (si $v(x_2) \in G \cdot x_2$, alors $u(v(x_2)) = (u \circ v)(x_2) \in G \cdot x_2$ puisque $u \circ v \in G$), chacune de ces rotation induit une permutation $\varphi(u)$ de $G \cdot x_2$ et l'application φ est un morphisme de groupes injectif de G sur le groupe

des permutations $\mathcal{S}(G\cdot x_2)$ (il est clair que φ est un morphisme de groupes et $u\in\ker(\varphi)$ entraîne que u a plus de deux points fixes dans S, c'est donc l'identité), donc G est un groupe d'ordre 12 isomorphe à un sous-groupe de $\mathcal{S}_4$, il est donc isomorphe à $\mathcal{A}_4$ qui est l'unique sous-groupe d'ordre 12 de $\mathcal{S}_4$.

3. Pour $m_1=2$, $m_2=3$, $m_3=4$, on a $n=24$ et $n_1=12$, $n_2=8$, $n_3=6$.
   Pour $x\in P$, on a $G_x=G_{-x}$, donc $\operatorname{card}(G\cdot x)=\dfrac{\operatorname{card}(G)}{\operatorname{card}(G_x)}=\operatorname{card}(G\cdot(-x))$ et comme les trois orbites sont de cardinal différent, on en déduit que :
   $$G\cdot x_2=\{\pm x_2,\pm y_2,\pm z_2,\pm t_2\}$$
   Cette orbite est stable par toute rotation $u\in G$ et chacune de ces rotation induit une permutation $\varphi(u)$ de l'ensemble $E=\{\mathbb{R}x_2,\mathbb{R}y_2,\mathbb{R}z_2,\mathbb{R}t_2\}$.
   Si $\varphi(u)=Id_E$, on a alors $u(x_2)=\pm x_2$, $u(y_2)=\pm y_2$, $u(z_2)=\pm z_2$, $u(t_2)=\pm t_2$. Si $u(x_2)=x_2$, on a alors $u\in G_{x_2}$ qui est d'ordre 3 et $y_2=u^3(y_2)=\pm y_2$ donne $u(y_2)=y_2$ et $u=Id$ puisqu'il a trois points fixes $x_2,-x_2$ et y_2 dans S. Si $u(x_2)=-x_2$, on a alors $u(y)=-y$ pour tout $y\in\{y_2,z_2,t_2\}$ puisque $u(y)=y$ entraîne $u\in G_y$ qui est d'ordre 3 (on a $G\cdot y=G\cdot x_2$, donc $\operatorname{card}(G_y)=\operatorname{card}(G_{x_2})=3$) et $u^3=Id$ est incompatible avec $u^3(x_2)=-x_2$. Mais l'espace vectoriel H engendré par $\{x_2,y_2,z_2,t_2\}$ est de dimension 3. En effet, sinon il est de dimension 2 stable par G ainsi que la droite $D=H^\perp$ et la restriction de $v\in G_{x_2}\setminus\{Id\}$ à D est $\pm Id_D$ et comme v est d'ordre 3, on a nécessairement $v_{|D}=Id_D$ et $v=Id$ du fait qu'elle a plus de 2 points fixes dans S (x_2, $-x_2$ et un vecteur directeur unitaire de D), ce qui contredit $v\neq Id$. Donc H est de dimension 3 et $u=-Id$, ce qui est incompatible avec $u\in\mathcal{O}^+(E)$.
   En définitive φ est injective de G dans $\mathcal{S}(E)$, ces deux groupes étant de même cardinal égal à 24, donc G est isomorphe à $\mathcal{S}_4$.
4. Enfin, dans le dernier cas, on montre de façon analogue que G est isomorphe à $\mathcal{A}_5$ (en réalité c'est un peu plus difficile et on peut consulter le livre de Nourdin pour les détails).

■