MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

Fiche 4: Actions de groupes

1. Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'on définit une G action de G sur $G/H = \{gH,\ g \in G\}$ par translation à gauche en posant $g \cdot C = gC = \{gx : x \in C\}$ pour tous $g \in G$ et $C \in G/H$.

(b) Montrer que cette action est transitive.

(c) Soit $a \in G$. Quel est le stabilisateur de aH ?

Solution.

(a) Comme $1_G \cdot gH = gH$ et

$$(g_1 g_2) \cdot gH = (g_1 g_2 g)H = g_1 \cdot (g_2 g)H = g_1 \cdot (g_2 \cdot gH),$$

alors l'application $G \times G/H \to G/H$ donnée par $g \cdot g'H = (gg')H$ est une action (à gauche).

(b) Étant donné $g, g' \in G$, on voit bien $g'g^{-1} \cdot gH = g'H$, ce qui implique que l'action est transitive.

(c) On voit bien que

$$\begin{aligned}\mathsf{Stab}(aH) &= \{g \in G : gaH = aH\} = \{g \in G : a^{-1}gaH = H\} = \{g \in G : a^{-1}ga \in H\} \\ &= aHa^{-1}.\end{aligned}$$

En particulier, $\mathsf{Stab}(H) = H$.

2. Soit G un groupe. On suppose que G possède un sous-groupe H d'indice fini m.

(a) Montrer que H contient un sous-groupe K distingué dans G, d'indice au plus $m!$ dans G.

(b) Qu'en déduit-on si G est d'ordre strictement plus grand que $m!$?

(c) Quel résultat retrouve-t-on si $m = 2$?

(d) On suppose que G est fini d'ordre n. Soit p le plus petit diviseur premier de n. Montrer que si H est d'indice p dans G, alors H est distingué dans G.

Solution.

(a) On considère le morphisme de groupes

$$\rho : G \to \mathsf{Aut}_{\mathsf{Ens}}(G/H)$$

qui associe à $g \in G$ la bijection $\rho(g) : G/H \to G/H$ donnée par $\rho(g)(g'H) = gg'H$, pour $g' \in G$. Soit $K = \mathsf{Ker}(\rho) \subseteq G$. Alors, K est un sous groupe normal et $K \subseteq H$, vu que $g \in K$ nous dit en particulier que $\rho(g)(H) = gH = H$, *i.e.* $g \in H$. Cette inclusion nous

dit que $m = [G : H][G : K]$. En plus, comme G/H a cardinal m, $\mathsf{Aut}_{\mathsf{Ens}}(G/H)$ a cardinal $m!$. L'application ρ induit un morphisme de groupes injectif $\bar{\rho} : G/K \to \mathsf{Aut}_{\mathsf{Ens}}(G/H)$, ce qui nous dit que $[G : K] = |G/K|$ divise $m!$. En conséquence,

$$m = [G : H][G : K] \text{ et } [G : K] | m! \tag{1}$$

et en particulier, $[G : K] \leq m!$.

(*b*) C'est clair que, si $|G| > m!$, alors $K \neq \{1_G\}$.

(*c*) Si $m = 2$, (1) nous dit que $[G : K] = [G : H] = 2$. L'inclusion $K \subseteq H$ implique alors que $H = K$ et en particulier H est normal.

(*d*) D'après (1), on voit que $p|[G : K]$ et $[G : K]|p!$. Comme $[G : K]||G| = p^m q$, avec $q, m \in \mathbb{N}^*$ tels que $\mathsf{PGCD}(p, q) = 1$, on conclut que $[G : K] | \mathsf{PGCD}(p^m q, p!) = p$. En conséquence, $[G : K] = p$. L'inclusion $K \subseteq H$ implique alors que $H = K$ et en particulier H est normal.

3. Soit G un groupe agissant sur un ensemble X. Soient $x \in X$, $S_x = \mathsf{Stab}(x)$ et p_x la projection canonique de G sur G/S_x.

(*a*) Soit $f_x : G \to \mathsf{Orb}(x)$ l'application définie par $f_x(g) = g.x$. Montrer qu'il existe une unique application $\bar{f}_x : G/S_x \to \mathsf{Orb}(x)$ telle que $f_x = \bar{f}_x \circ p_x$ et que cette application $\bar{f}_x$ est bijective.

(*b*) Le groupe G agit d'une part sur G/S_x et d'autre part sur $\mathsf{Orb}(x)$. Montrer que $\bar{f}_x(g \cdot C) = g \cdot \bar{f}_x(C)$ pour tous $g \in G$ et $C \in G/S_x$.

(*c*) En déduire que $S_{a\cdot x} = \mathsf{Stab}(aS_x) = aS_x a^{-1}$, pour tout $a \in G$.

(*d*) Quel est le noyau du morphisme $\phi_x : G \to \mathsf{Aut}_{\mathsf{Ens}}(\mathsf{Orb}(x))$ associé à l'action de G sur $\mathsf{Orb}(x)$?

Solution.

(*a*) On voit bien que $g \cdot x = f_x(g) = f_x(g') = g' \cdot x$ si et seulement si $(g^{-1}g') \cdot x = x$, *i.e.* $g^{-1}g' \in S_x$. En conséquence, f_x induit une application injective $\bar{f}_x : G/S_x \to \mathsf{Orb}(x)$ telle que $f_x = \bar{f}_x \circ p_x$. Comme f_x est surjective, $\bar{f}_x$ est surjective aussi. En conséquence, $\bar{f}_x$ est bijective.

(*b*) Comme $\bar{f}_x(gS_x) = g \cdot x$, pour $x \in X$ et $g \in G$, on voit bien que

$$\bar{f}_x\big(g \cdot (g'S_x)\big) = \bar{f}_x\big((gg')S_x\big) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot \bar{f}_x(g'S_x).$$

(*c*) C'est clair que $g \in S_{a\cdot x}$ si et seulement si $a \cdot x = g \cdot (a \cdot x) = (ga) \cdot x$, qui équivaut à $(a^{-1}ga) \cdot x = x$. Cette dernière condition est équivalente à $a^{-1}ga \in S_x$, *i.e.* $g \in aS_x a^{-1}$. En conclusion, $S_{a\cdot x} = aS_x a^{-1}$.

(*d*) C'est clair que $\mathsf{Ker}(\phi_x) = \cap_{a\in G} S_{a\cdot x} = \cap_{a\in G} aS_x a^{-1}$.

4. Soit G un groupe. On note $\mathsf{Subgr}(G)$ l'ensemble de ses sous-groupes.

(*a*) Montrer qu'on définit une action de G sur $\mathsf{Subgr}(G)$ par conjugaison en posant $g \cdot H = gHg^{-1}$, pour tous $g \in G$ et $H \in \mathsf{Subgr}(G)$.

(*b*) Cette action peut-elle être transitive ?

(*c*) Quels sont les points fixes pour cette action ?

Solution.

(*a*) Comme $1_G \cdot H = 1_G H 1_G^{-1} = H$ et

$$(g_1 g_2) \cdot H = (g_1 g_2) H (g_1 g_2)^{-1} = g_1 g_2 H g_2^{-1} g_1^{-1} = g_1 \cdot (g_2 H g_2^{-1}) = g_1 \cdot (g_2 \cdot H),$$

alors l'application $G \times \mathsf{Subgr}(G) \to \mathsf{Subgr}(G)$ donnée par $g \cdot H = gHg^{-1}$ est une action (à gauche).

(*b*) L'action ne peut pas être transitive, car $g \cdot \{1_G\} = \{1_G\}$ pour tout $g \in G$.

(*c*) On voit bien que $H = g \cdot H = gHg^{-1}$ pour tout $g \in G$ si et seulement si H est un sous-groupe normal.

5. Soient K un corps et E un K-espace vectoriel. On considère l'action naturelle de $\mathsf{GL}(E)$ sur E, définie par $g \cdot v = g(v)$, pour tous $g \in \mathsf{GL}(E)$ et $v \in E$.

(*a*) Quelles sont les orbites de cette action ?

(*b*) Montrer que cette action de groupe fournit un morphisme injectif de $\mathsf{GL}(E)$ dans $\mathsf{Aut}_{\mathsf{Ens}}(E \setminus \{\mathbf{0}_E\})$

(*c*) En prenant $E = (\mathbb{Z}/2\mathbb{Z})^2$, en déduire un isomorphisme entre $\mathsf{GL}_2(\mathbb{Z}/2\mathbb{Z})$ et $\mathbb{S}_3$.

Solution.

(*a*) Les orbites de l'action son $\{\mathbf{0}_E\}$ et $E \setminus \{\mathbf{0}_E\}$. En effet, toute application linéaire $\phi : E \to E$ satisfait que $\phi(\mathbf{0}_E) = \mathbf{0}_E$, et tout automorphisme linéaire ϕ de l'espace vectoriel E satisfait que, étant donné $e \in E \setminus \{\mathbf{0}_E\}$, $\phi(e) \in E \setminus \{\mathbf{0}_E\}$. En plus, étant donné $e, e' \in E \setminus \{\mathbf{0}_E\}$, il existe un automorphisme linéaire ϕ de l'espace vectoriel E tel que $\phi(e) = e'$. Pour le démontrer on remarque d'abord que les parties $\{e\}$ and $\{e'\}$ de E sont libres, ce qui implique qu'il existe deux bases $\mathscr{B}$ et $\mathscr{B}'$ de E telles que $e \in \mathscr{B}$ et $e' \in \mathscr{B}'$. En plus, comme $\mathscr{B}$ et $\mathscr{B}'$ sont deux bases du même espace vectoriel E, elles sont en bijection, ce qui implique que $\mathscr{B} \setminus \{e\}$ et $\mathscr{B}' \setminus \{e'\}$ sont en bijection aussi. Soit $\bar{f} : \mathscr{B} \setminus \{e\} \to \mathscr{B}' \setminus \{e'\}$ une telle bijection et soit $f : \mathscr{B} \to \mathscr{B}'$ l'application qui satisfait que $f(e) = e'$ et $f(v) = \bar{f}(v)$ pour tout $v \in \mathscr{B} \setminus \{e\}$. C'est clair que f est une bijection. Par conséquent, il existe une unique application linéaire bijective $F : E \to E$ telle que $F(v) = f(v)$ pour tout $v \in \mathscr{B}$, ce qui implique en particulier que $F(e) = e'$.

(*b*) Comme $\phi(E \setminus \{\mathbf{0}_E\}) \subseteq E \setminus \{\mathbf{0}_E\}$ pour tout $\phi \in \mathsf{GL}(E)$, on voit bien que l'application

$$\mathsf{res} : \mathsf{GL}(E) \to \mathsf{Aut}_{\mathsf{Ens}}(E \setminus \{\mathbf{0}_E\})$$

donnée par $\mathsf{res}(\phi) = \phi|_{E \setminus \{\mathbf{0}_E\}}$ est bien définie pour $\phi \in \mathsf{GL}(E)$. En plus, comme $\phi(\mathbf{0}_E) = \mathbf{0}_E$ pour toute application linéaire $\phi : E \to E$, l'application res est injective. Finalement, on note que $\mathsf{res}(\phi \circ \psi) = (\psi \circ \psi)|_{E \setminus \{\mathbf{0}_E\}} = \psi|_{E \setminus \{\mathbf{0}_E\}} \circ \psi|_{E \setminus \{\mathbf{0}_E\}} = \mathsf{res}(\phi) \circ \mathsf{res}(\psi)$, pour tous $\phi, \psi \in \mathsf{GL}(E)$, ce qui nous dit que res est un morphisme de groupes.

(*c*) Il suffit de démontrer que res est surjectif dans ce cas. Or, on note que les applications linéaires données dans la base canonique par les matrices

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

sont dans $\mathsf{GL}(E)$, où $E = (\mathbb{Z}/2\mathbb{Z})^2$. En conséquence, leurs images sous le morphisme injectif res donnent un ensemble S formé de 4 éléments différents dans $\mathsf{Aut}_{\mathsf{Ens}}(E \setminus \{\mathbf{0}_E\}) \simeq \mathbb{S}_3$. Soit H le sous-groupe engendré par S. L'inclusion évidente $S \subseteq H$, nous dit que $|H| \geq |S| = 4$. Comme $S \subseteq \mathsf{Img}(\mathsf{res})$ et $\mathsf{Img}(\mathsf{res})$ est un sous-groupe,

$H \subseteq \mathsf{Img}(\mathsf{res})$. Le théorème de Lagrange nous dit que l'ordre de H doit être un diviseur de l'ordre de $\mathbb{S}_3$, *i.e.* $|H| \in \{1,2,3,6\}$. La condition $|H| \geq 4$ implique alors $|H| = 6$, ce qui nous dit que $H = \mathbb{S}_3$ et *a fortiori* $\mathbb{S}_3 = \mathsf{Img}(\mathsf{res})$, vu que $\mathbb{S}_3 = H \subseteq \mathsf{Img}(\mathsf{res}) \subseteq \mathbb{S}_3$. En conséquence, res est un morphisme surjectif, comme on voulait montrer.

6. On munit $\mathbb{R}^3$ de sa structure euclidienne canonique et on considère l'action naturelle de $\mathsf{O}_3(\mathbb{R})$ sur $\mathbb{R}^3$. Soit $v \in \mathbb{R}^3 \setminus \{\mathbf{0}_{\mathbb{R}^3}\}$.

(*a*) Quelle est l'orbite de v ?

(*b*) Établir une bijection entre $\mathsf{SO}_3(\mathbb{R}) \cap \mathsf{Stab}(v)$ et $\mathsf{Stab}(v) \setminus \mathsf{SO}_3(\mathbb{R})$, et montrer que $\mathsf{Stab}(v) \setminus \mathsf{SO}_3(\mathbb{R})$ ne contient que des réflexions.

(*c*) Soit $P = (\mathbb{R}v)^\perp$. Montrer que les groupes $\mathsf{Stab}(v)$ et $\mathsf{O}(P)$ sont isomorphes.

(*d*) Soit H le sous-groupe de $\mathsf{O}_3(\mathbb{R})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \mathbf{0}_{\mathbb{R}^{1\times 2}} \\ \mathbf{0}_{\mathbb{R}^{2\times 1}} & A \end{pmatrix}$$

avec $A \in \mathsf{O}_2(\mathbb{R})$. Déduire des questions précédentes une bijection entre la sphère de centre $\mathbf{0}_{\mathbb{R}^3}$ et de rayon $\|v\|$, et l'ensemble quotient $\mathsf{O}_3(\mathbb{R})/H$.

Solution.

(*a*) On affirme que l'orbite de v est $S(\mathbf{0}_{\mathbb{R}^3}, \|v\|) = \{w \in \mathbb{R}^3 : \|w\| = \|v\|\}$. On note d'abord que $\|Aw\| = \|w\|$ pour tout $A \in \mathsf{O}_3(\mathbb{R})$ et $w \in \mathbb{R}^3$, ce qui nous dit que $Av \in S(\mathbf{0}_{\mathbb{R}^3}, \|v\|)$. Pour montrer l'autre inclusion, on peut supposer sans perte de généralité que $v = (r,0,0)$, où $r = \|v\|$. Si $r = 0$, c'est immédiat. On suppose désormais $r > 0$. Soit $w = (a,b,c) \in \mathbb{R}^3$ tel que $a^2 + b^2 + c^2 = r^2$. Si $b^2 + c^2 \neq 0$, on considère la matrice

$$M_w = \begin{pmatrix} \frac{a}{r} & \frac{\sqrt{b^2+c^2}}{r} & 0 \\ \frac{b}{r} & -\frac{ab}{r\sqrt{b^2+c^2}} & \frac{c}{\sqrt{b^2+c^2}} \\ \frac{c}{r} & -\frac{ac}{r\sqrt{b^2+c^2}} & -\frac{b}{\sqrt{b^2+c^2}} \end{pmatrix},$$

et si $b = c = 0$, alors $w = \pm v$, et on définit

$$M_w = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Alors, $M_w \in \mathsf{SO}_3(\mathbb{R})$ et $M_w v = w$.

(*b*) Soit $u \in \mathbb{R}^3 \setminus \{\mathbf{0}_{\mathbb{R}^3}\}$ un vecteur orthogonal à v et soit $\rho \in \mathsf{O}_3(\mathbb{R})$ la réflexion associé à l'hyperespace $H = \{u\}^\perp$. En conséquence, $\rho(v) = v$, vu que $v \in H$. On voit bien que l'application $\rho^* : \mathsf{O}_3(\mathbb{R}) \to \mathsf{O}_3(\mathbb{R})$ qui associe $\sigma\rho$ à $\sigma \in \mathsf{O}_3(\mathbb{R})$ est bijective, vu que $\rho^* \circ \rho^* = \mathsf{id}_{\mathsf{O}_3(\mathbb{R})}$. En plus, $\rho^*(\mathsf{SO}_3(\mathbb{R}) \cap \mathsf{Stab}(v)) = \mathsf{Stab}(v) \setminus \mathsf{SO}_3(\mathbb{R})$, ce qui implique que $\rho^*|_{\mathsf{SO}_3(\mathbb{R})\cap\mathsf{Stab}(v)}$ est donc une bijection entre $\mathsf{SO}_3(\mathbb{R}) \cap \mathsf{Stab}(v))$ et $\mathsf{Stab}(v) \setminus \mathsf{SO}_3(\mathbb{R})$.

Soit $\rho \in \mathsf{Stab}(v) \setminus \mathsf{SO}_3(\mathbb{R})$ et soit $P = (\mathbb{R}v)^\perp$. On choisit une base orthonormale $\{u, w\}$ de P. Alors, dans la base $\{v, u, w\}$ de $\mathbb{R}^3$ la représentation matricielle de ρ est

$$\begin{pmatrix} 1 & \mathbf{0}_{\mathbb{R}^{1\times 2}} \\ \mathbf{0}_{\mathbb{R}^{2\times 1}} & A \end{pmatrix}$$

avec $A \in \mathsf{O}_2(\mathbb{R})$. Comme déterminant de ρ est -1, $\det(A) = -1$. On rappelle l'identité immédiate

$$\mathsf{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}.$$

En particulier,

$$A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix},$$

qui possède valeurs propres ± 1, avec vecteurs propres $v_\pm = (-b, a \pm 1)$. En conséquence, ρ est la réflexion associée à l'hyperplan engendré par v et $-bu + (a-1)w$.

(*c*) Soient $\rho \in \mathsf{Stab}(v)$ et $u \in P = (\mathbb{R}v)^\perp$. On note d'abord que $0 = \langle v, u \rangle = \langle \rho(v), \rho(u) \rangle = \langle v, \rho(u) \rangle$ nous dit que $\rho(u) \in P$, *i.e.* $\rho(P) \subseteq P$. En employant ρ^{-1} au lieu de ρ, on conclut que $\rho(P) = P$. On note d'abord que le produit scalaire euclidien de $\mathbb{R}^3$ induit un produit scalaire sur P, que l'on va aussi noter $\langle , \rangle$. En conséquence, si $\rho \in \mathsf{Stab}(v)$, on voit que $\rho|_P : P \to P$ est aussi une application orthogonale pour le produit scalaire induit. On considère alors l'application

$$\mathsf{res}_P : \mathsf{Stab}(v) \to \mathsf{O}(P)$$

qui associe $\rho|_P : P \to P$ à $\rho \in \mathsf{Stab}(v)$. C'est clair que res_P est un morphisme de groupes, vu que $\mathsf{res}_P(\rho \circ \rho') = (\rho \circ \rho')|_P = \rho|_P \circ \rho'|_P = \mathsf{res}_P(\rho) \circ \mathsf{res}_P(\rho')$, pour tous $\rho, \rho' \in \mathsf{Stab}(v)$. En plus, res_P est injectif, vu que $\mathsf{res}_P(\rho) = \mathsf{res}_P(\rho')$ implique $\rho|_P = \rho'|_P$, et comme $\rho(v) = v = \rho'(v)$ et $\mathbb{R}^3 = \mathbb{R}v \oplus P$, on conclut que $\rho = \rho'$. Finalement, res_P est surjectif. En effet, étant donné $\sigma \in \mathsf{O}(P)$, la seule application linéaire $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ donnée par $\rho|_P = \sigma$ et $\rho(v) = v$ est orthogonale et satisfait que $\mathsf{res}_P(\rho) = \sigma$.

(*d*) On va supposer sans perte de généralité que $v = (\|v\|, 0, 0)$, vu que l'action de $\mathsf{O}_3(\mathbb{R})$ est transitive. Alors, $H = \mathsf{Stab}(v)$ est formé des matrices de la forme

$$\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$$

avec $A \in \mathsf{O}_2(\mathbb{R})$. Comme l'application $\mathsf{O}_3(\mathbb{R}) \to \partial B(\mathbf{0}_{\mathbb{R}^3}, \|v\|)$ est surjective, l'application induite $\mathsf{O}_3(\mathbb{R})/H \to \partial B(\mathbf{0}_{\mathbb{R}^3}, \|v\|)$ est une bijection, d'après l'exercice **3**.

7. Dans $\mathbb{R}^3$, on considère l'ensemble S des 8 sommets d'un cube centré en $\mathbf{0}_{\mathbb{R}^3}$ (pour fixer les idées, on peut prendre les points de coordonnées ± 1). On note G le sous-groupe de $\mathsf{O}(\mathbb{R}^3)$ des isométries de $\mathbb{R}^3$ qui laissent l'ensemble S globalement invariant, $G^+ = G \cap \mathsf{SO}(\mathbb{R}^3)$ et $G^- = G \setminus \mathsf{SO}(\mathbb{R}^3)$.

(*a*) Utiliser l'action naturelle du groupe G sur S pour montrer que G est fini.

(*b*) En utilisant la symétrie centrale de centre $\mathbf{0}_{\mathbb{R}^3}$, montrer que $|G^-| = |G^+|$.

(*c*) On cherche à compter les éléments de G^+.

(i) Donner des exemples d'isométries qui appartiennent à G^+.

(ii) Le groupe G^+ agit sur l'ensemble des sommets du cube. Montrer que cette action est transitive, déterminer le stabilisateur d'un sommet et en déduire que G^+ contient exactement 24 isométries.

(iii) Faire la liste de toutes les isométries de G^+.

(*d*) Puisque G^+ est un groupe d'ordre 24 on peut se demander s'il est isomorphe à

$\mathbb{S}_4$. Pour cela on cherche à faire agir G^+ sur un ensemble de 4 éléments attenant au cube. Soit D l'ensemble des 4 grandes diagonales du cube. L'action naturelle de G sur D fournit un morphisme $\phi : G^+ \to \mathsf{Aut}_{\mathsf{Ens}}(D)$.

(i) Montrer que chaque transposition de $\mathsf{Aut}_{\mathsf{Ens}}(D)$ a un antécédent par ϕ.

(ii) En déduire que le morphisme ϕ est surjectif, et enfin qu'il est bijectif.

(*e*) Construire un isomorphisme de groupe de $G^+ \times \{\pm \mathsf{id}_{\mathbb{R}^3}\}$ sur G.

(*f*) Soient S_1 l'ensemble des sommets d'un parallélépipède centré en $\mathbf{0}_{\mathbb{R}^3}$ et G_1 le sous-groupe de $\mathsf{GL}(\mathbb{R}^3)$ des isomorphismes de $\mathbb{R}^3$ qui laissent l'ensemble S_1 globalement invariant. Montrer que les groupes G et G_1 sont conjugués dans $\mathsf{GL}(\mathbb{R}^3)$.

Solution.

(*a*) On considère le morphisme de groupes

$$\mathsf{res}_S : G \to \mathsf{Aut}_{\mathsf{Ens}}(S)$$

qui associe $\rho|_S : S \to S$ à $\rho \in G$. L'application précédente est bien définie, car l'inverse de $\rho|_S : S \to S$ est $\rho^{-1}|_S : S \to S$. On affirme que res_S est un morphisme injectif. En effet, $\mathsf{res}_S(\rho) = \mathsf{res}_S(\rho')$ nous dit que $\rho(s) = \rho'(s)$ pour tout $s \in S$. Comme l'ensemble S est un ensemble de générateurs de l'espace vectoriel $\mathbb{R}^3$, on conclut que $\rho = \rho'$. Comme $\mathsf{Aut}_{\mathsf{Ens}}(S)$ est fini, alors G est aussi fini.

(*b*) On considère l'application

$$\iota : G \to G$$

qui associe $-\rho$ à $\rho \in G$. C'est clair que ι est bijective, vu qu'elle est sa propre réciproque. On voit bien que $\iota(G^\pm) \subset G^\mp$, ce qui implique en plus que $\iota(G^\pm) = G^\mp$. En conséquence, $|G^-| = |G^+|$.

(*c*) (i) On voit bien que $\mathsf{id}_{\mathbb{R}^3} \in G^+$.

(ii) On montre d'abord que si $v, w \in S$ se trouvent dans la même face du cube, alors il existe $\rho \in G^+$ tel que $\rho v = w$. En effet, sans perte de généralité on peut supposer que $v = (1,1,1)$ et $w = (a,b,1)$, où $a, b \in \{\pm 1\}$, se trouvent dans une face horizontale, *i.e.* orthogonal au vecteur $(0,0,1)$. On considère la matrice

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

de rotation d'angle θ autour de l'axe formé par le vecteur $(0,0,1)$. Noter que $R_{n\pi/2} \in G^+$ pour tout $n \in \mathbb{Z}$, et que $R_{\pi/2}v = (-1,1,1)$, $R_\pi v = (-1,-1,1)$ et $R_{3\pi/2}v = (1,-1,1)$, ce qui montre l'affirmation. Comme chaque élément de $S \setminus \{-v\}$ se trouvent dans un même face du cube que v, on conclut que $S \setminus \{-v\}$ est inclus dans l'orbite de v. En outre, comme $R_\pi v$ et $-v$ se trouvent dans une même face du cube, par le résultat précédent il existe $\rho \in G^+$ tel que $\rho R_\pi v = -v$. En conséquence, on conclut que l'orbite de v sous l'action de G^+ est S.

Par ailleurs, on affirme que le groupe d'isotropie $\mathsf{Stab}_G(v) = \{g \in G : gv = v\}$ a cardinalité 6. En effet, comme $\mathsf{Stab}_G(v) \subseteq G \subseteq \mathsf{O}_3(\mathbb{R})$, la distance $\|v - w\|$ est préservée pour tout $w \in S$. On considère l'ensemble $S_v = \{w \in S : \|w - v\| = 1\}$. C'est clair que $\#(S_v) = 3$ et que S_v est un ensemble de générateurs de l'espace

vectoriel $\mathbb{R}^3$, ce qui implique que S_v est une base de $\mathbb{R}^3$. On considère le morphisme de groupes

$$\mathsf{res}_v : \mathsf{Stab}_G(v) \to \mathsf{Aut}_{\mathsf{Ens}}(S_v)$$

qui associe $\rho|_{S_v} : S_v \to S_v$ à $\rho \in \mathsf{Stab}_G(v)$. L'application précédente est bien définie, car l'inverse de $\rho|_{S_v} : S_v \to S_v$ est $\rho^{-1}|_{S_v} : S_v \to S_v$. On affirme que res_v est un morphisme bijectif. En effet, le morphisme est injectif car $\mathsf{res}_v(\rho) = \mathsf{res}_v(\rho')$ nous dit que $\rho(s) = \rho'(s)$ pour tout $s \in S_v$. Comme l'ensemble S_v est un ensemble de générateurs de l'espace vectoriel $\mathbb{R}^3$, on conclut que $\rho = \rho'$. En outre, le morphisme est surjectif, car, étant donné $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(S_v)$, on définit $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ comme la seule application linéaire qui satisfait que $\rho(w) = \sigma(w)$ pour tout $w \in \S_v$. C'est clair que ρ est une isométrie, *i.e.* $\rho \in \mathsf{O}_3(\mathbb{R})$, car $\langle \rho(w), \rho(w') \rangle = \langle w, w' \rangle$ pour tous $w, w' \in S_v$, que $\rho(S) = S$ et $\rho \in \mathsf{Stab}_G(v)$, car $S = S_v \cup (-S_v) \cup \{\pm v\}$, $\rho(-S_v) = -S_v$, $v = \sum_{w \in S_v} w$ et $\rho(v) = \sum_{w \in S_v} \rho(w) = \sum_{w \in S_v} w = v$, et que $\rho|_{S_v} = \sigma$. On conclut que $|\mathsf{Stab}_G(v)| = 6$.

Comme l'orbite de v sous l'action de G coïncide avec l'orbite sous l'action de G^+, l'exercice **3** nous dit que $8 = |S| = |G/\mathsf{Stab}_G(v)| = |G|/6$, ce qui implique que $|G| = 48$ et donc $|G^+| = 24$.

(iii) On laisse à la lectrice/au lecteur la vérification élémentaire suivante.

$$\begin{aligned} G^+ = \Bigg\{ & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \\ & \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \Bigg\}. \end{aligned}$$

Si l'on note e_i le i-ème vecteur de la base canonique de $\mathbb{R}^3$, alors dans la liste précédente :

(G^+.1) le premier élément est l'identité ;

(G^+.2) les 9 éléments qui suivent sont formés de 3 groupes, dont le i-ème est formé des 3 rotations d'angle $n\pi/2$ autour de l'axe donné par e_i pour $n \in [\![1, 3]\!]$;

(G^+.3) les 8 éléments qui suivent sont formés de 4 groupes, chacun indéxé par $\bar{i} = (i_1, i_2) \in \{\pm 1\}^2$ et que l'on a ordonné avec l'ordre $(1,1) < (1,-1) < (-1,1) < (-1,-1)$, dont le $\bar{i}$-ème est formé des 2 rotations d'angle $2n\pi/3$ autour de l'axe donné par $i_1 e_1 + i_2 e_2 + e_3$, pour $n \in [\![1, 2]\!]$;

(G^+.4) les 6 derniers éléments sont formés de 3 groupes, dont le i-ème est formé des 2 rotations d'angle π autour de l'axe donné par $e_j \pm e_k$ où $\{i,j,k\} = [\![1,3]\!]$;

(*d*) Pour tout $v \in S$, on va identifier la diagonale déterminée par v avec la partie $d_v = \{v,-v\} \subseteq S$. On pose $D = \{d_v : v \in S\}$. C'est clair que $d_v = d_w$ si et seulement si $v = w$ ou $v = -w$. Noter que, étant donné $\rho \in G$ et $v \in S$, il existe $w \in S$ tel que $\rho(d_v) = d_w$, ce qui nous dit qu'il existe une application $G \times D \to D$ qui associe $\rho(d_v)$ à $d_v \in D$. C'est clair que cette application est une action (à gauche).

(i) Or, étant donné deux diagonales $d, d' \in D$ différentes, on voit bien qu'il existe un seul plan $\Pi_{d,d'} \subseteq \mathbb{R}^3$ tel que $d'' \subseteq \Pi_{d,d'}$ pour $d'' \in D \setminus \{d,d'\}$. On considère la rotation $r_{d,d'} \in \mathsf{SO}_3(\mathbb{R})$ d'angle π autour de l'axe donné par $\Pi_{d,d'}^{\perp}$ Alors, $r_{d,d'} \in G^+$, $\phi(r_{d,d'})(d) = d'$, $\phi(r_{d,d'})(d') = d$ et $\phi(r_{d,d'})(d'') = d''$ pour $d'' \in D \setminus \{d,d'\}$.

(ii) Comme les transpositions engendrent le groupe $\mathsf{Aut}_{\mathsf{Ens}}(D)$ et $\mathsf{Img}(\phi)$ inclut toutes les transpositions par l'item précédent, on conclut que ϕ est surjectif. En plus, comme le domaine et codomaine de ϕ ont la même cardinalité finie, ϕ est bijectif.

(*e*) C'est clair que l'application $\psi : G^+ \times \{\pm \mathsf{id}_{\mathbb{R}^3}\} \to G$ donnée par $\psi(g,h) = g \circ h$, pour $g \in G^+$ et $h \in \{\pm \mathsf{id}_{\mathbb{R}^3}\}$ est un morphisme de groupes, vu que $\{\pm \mathsf{id}_{\mathbb{R}^3}\} \subseteq \mathscr{Z}(G)$. En plus, d'après les commentaires dans l'item (b), ψ est surjectif. Comme le domaine et codomaine de ψ ont la même cardinalité finie, ψ est bijectif.

(*f*) Soient $v \in S$ et $v' \in S_1$ deux points fixes. On considère $S_{1,v'}$ l'ensemble formé des éléments w' de S_1 telles que $\{w', v'\}$ est un arête du parallélépipède. Soit $\rho : \mathbb{R}^3 \to \mathbb{R}^3$ une application linéaire qui satisfait que $\rho(S_v) = S_{1,v'}$. C'est clair que $\rho \in \mathsf{GL}(\mathbb{R}^3)$. En plus, on voit bien que l'application $\mathsf{Ad}_\rho : G \to G_1$ qui associe $\rho g \rho^{-1}$ à $g \in G$ est bien définie. En conséquence, les groupes G et G_1 sont conjugués dans $\mathsf{GL}(\mathbb{R}^3)$.

⋆ **8.** *Isométries d'un tétraèdre régulier.* Soient E un espace euclidien orienté de dimension 3 et $\mathscr{B} = (e_1, e_2, e_3)$ une base orthonormée directe de E. On considère les vecteurs v_1, v_2, v_3, v_4 donnés par

$$\mathsf{Mat}_{\mathscr{B}}(v_1, v_2, v_3, v_4) = \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}.$$

(*a*) Calculer les produits scalaires $\langle v_i, v_j \rangle$. Que vaut $v_1 + v_2 + v_3 + v_4$?

(*b*) Soit $\sigma \in \mathbb{S}_4$. Montrer qu'il existe une unique application linéaire $u_\sigma \in \mathsf{L}(E)$, telle que $u_\sigma(v_j) = v_{\sigma(j)}$ pour tout $j \in [\![1,4]\!]$. Montrer que $u_\sigma \in \mathsf{O}(E)$.

(*c*) Montrer que l'application $\sigma \mapsto u_\sigma$ est un isomorphisme entre $\mathbb{S}_4$ et le groupe des isométries vectorielles préservant $\{v_1, v_2, v_3, v_4\}$.

(*d*) Donner la nature de u_σ en fonction de la structure de σ. Que vaut $\det u_\sigma$?

Solution.

(*a*) On voit bien que $\langle v_i, v_i \rangle = 3$ pour $i \in [\![1,4]\!]$ et $\langle v_i, v_j \rangle = -1$ pour $i, j \in [\![1,4]\!]$ avec $i \neq j$. En plus, $v_1 + v_2 + v_3 + v_4 = \mathbf{0}_{\mathbb{R}^3}$.

(*b*) C'est clair que $\{v_1, v_2, v_3\}$ est un ensemble libre de E et en conséquence une base. En effet, le déterminant des premières 3 colonnes de $\mathsf{Mat}_{\mathscr{B}}(v_1, v_2, v_3, v_4)$ est $-4 \neq 0$. De façon plus générale, $\{v_i, v_j, v_k\}$ est une base de E pour $i, j, k \in [\![1,4]\!]$ tels que

$\#\{i,j,k\} = 3$. On définit la seule application linéaire $u_\sigma : E \to E$ telle que $u_\sigma(v_j) = v_{\sigma(j)}$ pour tout $j \in [\![1,3]\!]$. On voit bien que

$$u_\sigma(v_4) = u_\sigma(-v_1 - v_2 - v_3) = -v_{\sigma(1)} - v_{\sigma(2)} - v_{\sigma(3)} = v_{\sigma(4)}.$$

En conséquence, $u_\sigma(v_j) = v_{\sigma(j)}$ pour tout $j \in [\![1,4]\!]$. En plus,

$$\langle u_\sigma(v_i), u_\sigma(v_j)\rangle = \langle v_{\sigma(i)}, v_{\sigma(j)}\rangle = \langle v_i, v_j\rangle$$

pour tous $i,j \in [\![1,3]\!]$, d'après le premier item. Cela nous dit que $u_\sigma \in \mathsf{O}(E)$, vu que, étant donné $v = \sum_{i=1}^3 c_i v_i$ et $v' = \sum_{i'=1}^3 c'_{i'} v_{i'}$, on a

$$\langle u_\sigma(v), u_\sigma(v')\rangle = \sum_{i'=1}^3\sum_{i=1}^3 \langle u_\sigma(v_i), u_\sigma(v_{i'})\rangle = \sum_{i'=1}^3\sum_{i=1}^3 \langle v_i, v_{i'}\rangle = \langle v, v'\rangle.$$

(*c*) C'est clair que l'application $\mathbb{S}_4 \to \mathsf{O}(E)$ donnée par $\sigma \mapsto u_\sigma$ est un morphisme de groupes. En plus, cette application est injective, car, si $u_\sigma = \mathsf{id}_E$, alors $v_{\sigma(i)} = u_\sigma(v_i) = v_i$ pour tout $i \in [\![1,4]\!]$, ce qui implique que $\sigma = \mathsf{id}_{[\![1,4]\!]}$. Finalement, l'image du morphisme de groupes précédent est formé des isométries vectorielles préservant $\{v_1, v_2, v_3, v_4\}$. En effet, étant donné $\rho \in \mathsf{O}(E)$ préservant $\{v_1, v_2, v_3, v_4\}$, alors il existe une permutation $\sigma \in \mathbb{S}_4$ telle que $\rho(v_i) = v_{\sigma(i)}$, vu que $\rho \in \mathsf{O}(E) \subseteq \mathsf{GL}(E)$. C'est clair que $\rho = u_\sigma$.

(*d*) Un calcul élémentaire montre que $\det(u_\sigma) = -1$ pour toute transposition $\sigma \in \mathbb{S}_4$. En effet, si $\sigma = (i\ j)$, on considère $k \in [\![1,4]\!]$ tel que $\#\{i,j,k\} = 3$. Alors, la matrice de u_σ dans la base $\{v_i, v_j, v_k\}$ est de la forme

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ce qui nous dit que $\det(u_\sigma) = -1$. En conséquence, $\det(u_\sigma) = \epsilon(\sigma)$. En effet, si $\sigma = \tau_1 \dots \tau_n$, avec $\tau_1, \dots, \tau_n$ transpositions, alors

$$\det(u_\sigma) = \det(\tau_1)\dots\det(\tau_n) = (-1)^n = \epsilon(\sigma).$$

Avant de continuer, on rappelle que, étant donné une isométrie A de l'espace euclidien $\mathbb{R}^n$ (ou, de façon équivalente, une matrice orthogonale), ses valeurs propres ont valeur absolue 1. Pour le montrer, on note d'abord que, si $\langle\,,\rangle_{\mathbb{C}} : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ note la forme sesquilinéaire canonique de $\mathbb{C}^n$, alors $\langle v, w\rangle_{\mathbb{C}} = \langle Av, Aw\rangle_{\mathbb{C}}$ pour tous $v, w \in \mathbb{C}^n$. En outre, si $v \in \mathbb{C}^n$ est un vecteur propre de A avec valeur propre $\lambda \in \mathbb{C}$ alors

$$\langle v, v\rangle_{\mathbb{C}} = \langle Av, Av\rangle_{\mathbb{C}} = \langle \lambda v, \lambda v\rangle_{\mathbb{C}} = |\lambda|^2 \langle v, v\rangle_{\mathbb{C}},$$

ce qui implique que $|\lambda| = 1$. En outre, c'est clair aussi que les vecteurs propres de valeurs propres différentes sont orthogonaux, car si $v \in \mathbb{C}^n$ et $w \in \mathbb{C}^n$ sont des vecteurs propres de A de valeurs propres $\lambda_v \in \mathbb{C}$ et $\lambda_w \in \mathbb{C}$, respectivement, avec $\lambda_v \neq \lambda_w$, alors

$$\langle v, w\rangle_{\mathbb{C}} = \langle Av, Aw\rangle_{\mathbb{C}} = \langle \lambda_v v, \lambda_w w\rangle_{\mathbb{C}} = \bar{\lambda}_v \lambda_w \langle v, w\rangle_{\mathbb{C}},$$

ce qui implique $\langle v, w\rangle_{\mathbb{C}} = 0$. Par induction sur n, on montre alors que l'extension $\mathbb{C}$-linéaire $A_{\mathbb{C}} : \mathbb{C}^n \to \mathbb{C}^n$ de toute isométrie A est diagonalisable. En effet, cela suit immédiatement du fait que $A_{\mathbb{C}}$ possède au moins un vecteur propre $v \in \mathbb{C}^n$, l'espace orthogonal $V = \{v\}^\perp \subseteq \mathbb{C}^{n-1}$ pour la forme sesquilinéaire $\langle\,,\rangle_{\mathbb{C}}$ est invariant pour A et $A|_V : V \to V$ est une isométrie pour la restriction de $\langle\,,\rangle_{\mathbb{C}}$ à V.

Par ailleurs, on rappelle qu'une **rotation** A est un élément $\mathsf{SO}_3(\mathbb{R})$. On note que toute rotation A possède une seule valeur propre réelle, 1, qui a multiplicité 1. En effet,

comme $A_{\mathbb{C}}$ est diagonalisable et son polynôme caractéristique appartient à $\mathbb{R}[X]$ et est de degré 3, il possède deux racines complexes non réelles λ et $\bar{\lambda}$, ce qui implique que la racine réelle est $\det(A_{\mathbb{C}})/|\lambda|^2 = \det(A)/|\lambda|^2 = \det(A) = 1$. L'angle de rotation θ de A est donné par $\mathrm{Tr}(A) = 1 + 2\cos(\theta)$ et l'axe de rotation est déterminé par le vecteur propre v de valeur propre 1. Noter que si A est une rotation avec vecteur propre v de valeur propre 1, alors l'image de l'application $\{v\}^{\perp} \to \mathbb{R}$ qui associe $\langle u \wedge Au, v\rangle$ à $u \in \{v\}^{\perp}$ est incluse dans $\mathbb{R}_{\geq 0}$ ou $\mathbb{R}_{\leq 0}$, où $u \wedge Au$ dénote le produit vectoriel. Dans le premier cas on dit que A est une **rotation d'angle** θ **autour de** v et dans le deuxième que A est une **rotation d'angle** $-\theta$ **autour de** v (ou A est une rotation d'angle θ autour de $-v$). En outre, c'est facile à démontrer qu'un élément $A \in \mathsf{O}_3(\mathbb{R}) \setminus \mathsf{SO}_3(\mathbb{R})$ (resp. $A \in \mathsf{SO}_3(\mathbb{R})$) est une réflexion (resp., renversement) si et seulement si ses valeurs propres sont 1 (resp., -1) avec multiplicité 2 et -1 (resp., 1) avec multiplicité 1. Le plan de réflexion (resp., l'axe de renversement) de A est le sous-espace propre de valeur propre 1.

On laisse à la lectrice/au lecteur la vérification des affirmations élémentaires suivantes :

(A.1) si $\sigma = \mathsf{id}_{[\![1,4]\!]}$, alors $u_\sigma = \mathsf{id}_{\mathbb{R}^3}$;

(A.2) si $\sigma = (i\ j) \in \mathbb{S}_4$, alors u_σ est la réflexion associée au plan engendré par v_k et v_ℓ, où $\{i, j, k, \ell\} = [\![1, 4]\!]$;

(A.3) si $\sigma = (i\ j\ k) \in \mathbb{S}_4$, alors u_σ est la rotation d'angle $2\pi/3$ et d'axe de rotation donné par v_ℓ, où $\{i, j, k, \ell\} = [\![1, 4]\!]$;

(A.4) si $\sigma = (i\ j)(k\ \ell) \in \mathbb{S}_4$, alors u_σ est le renversement d'axe donné par $v_i + v_j$ (ou $v_k + v_\ell$) ;

(A.5) si $\sigma = (i\ j\ k\ \ell) = (i\ j)(j\ k\ \ell) \in \mathbb{S}_4$, alors u_σ est la composition d'une rotation d'angle $2\pi/3$ autour de v_i et d'une réflexion associée au plan engendré par v_k et v_ℓ.

9. Soit G un groupe fini qui agit sur un ensemble fini X. On note X/G l'ensemble des orbites sous cette action. Pour $g \in G$ on note $\mathsf{Fix}(g)$ l'ensemble des éléments de X qui sont fixés par g. En calculant de deux façons différentes le cardinal de l'ensemble $S = \{(g, x) \in G \times X : g.x = x\}$, montrer la formule de Burnside

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\,\mathsf{Fix}(g)|.$$

Solution. C'est clair que

$$\sum_{x \in X} |\,\mathsf{Stab}(x)| = \#(S) = \sum_{g \in G} |\,\mathsf{Fix}(g)|,$$

car

$$S = \bigsqcup_{x \in X} \mathsf{Stab}(x) \times \{x\} = \bigsqcup_{g \in G} \{g\} \times \mathsf{Fix}(g).$$

On rappelle que $|\,\mathsf{Stab}(x)| = |G|/|\,\mathsf{Orb}(x)|$, pour $x \in X$, d'après l'exercice **3**. Alors,

$$\begin{aligned}\sum_{x \in X} |\,\mathsf{Stab}(x)| &= \sum_{\bar{x} \in X/G} \sum_{x \in \bar{x}} |\,\mathsf{Stab}(x)| = \sum_{\bar{x} \in X/G} \sum_{x \in \bar{x}} \frac{|G|}{|\bar{x}|} = \sum_{\bar{x} \in X/G} |\bar{x}|.\frac{|G|}{|\bar{x}|} \\ &= \sum_{\bar{x} \in X/G} |G| = |G|.|X/G|.\end{aligned}$$

En conséquence,

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |\mathsf{Fix}(g)|.$$

10. Soient X et Y deux ensembles, G un groupe agissant sur X au moyen du morphisme de groupes $\phi : G \to \mathsf{Aut}_{\mathsf{Ens}}(X)$.

(*a*) Montrer qu'on définit une action de $\mathsf{Aut}_{\mathsf{Ens}}(X)$ sur Y^X par $\sigma \cdot f = f \circ \sigma^{-1}$, pour tous $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(X)$ et $f \in Y^X$.

(*b*) Montrer que l'on définit une action de G sur Y^X par $g \bullet f = f \circ \phi(g)^{-1}$, pour tous $g \in G$ et $f \in Y^X$.

(*c*) Soient $g \in G$ et $f \in Y^X$. Montrer que $g \bullet f = f$ si et seulement si f est constante sur chaque orbite de $\phi(g)$.

Solution.

(*a*) On voit bien que $\mathsf{id}_X \cdot f = f \circ \mathsf{id}_X^{-1} = f$ et que

$$\sigma \cdot (\sigma' \cdot f) = \sigma \cdot (f \circ \sigma'^{-1}) = (f \circ \sigma'^{-1}) \circ \sigma^{-1} = f \circ (\sigma \circ \sigma')^{-1} = (\sigma \circ \sigma') \cdot f,$$

pour $\sigma, \sigma' \in \mathsf{Aut}_{\mathsf{Ens}}(X)$ et $f \in Y^X$. On rappelle que cette action est déterminée de façon équivalente par un morphisme de groupes $\rho : \mathsf{Aut}_{\mathsf{Ens}}(X) \to \mathsf{Aut}_{\mathsf{Ens}}(Y^X)$ donné par $\rho(\sigma)(f) = \sigma \cdot f$, pour $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(X)$ et $f \in Y^X$.

(*b*) Si $\rho : G' \to \mathsf{Aut}_{\mathsf{Ens}}(S)$ est un morphisme de groupes, qui détermine une action (à gauche) de G' sur S, et $\phi : G \to G'$ est un morphisme de groupes, alors c'est clair que $\rho \circ \phi : G \to \mathsf{Aut}_{\mathsf{Ens}}(S)$ est aussi un morphisme de groupes, qui détermine une action (à gauche) de G sur S. Dans ce cas, l'action dans l'item précédent nous donne un morphisme de groupes $\rho : \mathsf{Aut}_{\mathsf{Ens}}(X) \to \mathsf{Aut}_{\mathsf{Ens}}(Y^X)$, dont la composition $\rho \circ \phi$ avec $\phi : G \to \mathsf{Aut}_{\mathsf{Ens}}(X)$ est aussi un morphisme de groupes, qui détermine une action (à gauche) de G' sur Y^X. De façon explicite, cette action est de la forme $g \cdot f = (\rho \circ \phi)(g)(f) = \rho(\phi(g))(f) = \phi(g) \cdot f = f \circ \phi(g)^{-1}$, pour $g \in G$ et $f \in Y^X$.

(*c*) C'est clair que $g \bullet f = f$ si et seulement si $f \circ \phi(g)^{-1} = f$, si et seulement si $f \circ \phi(g) = f$. Un argument simple par récurrence sur k nous dit que cela équivaut à $f(\phi(g)^k(x)) = f(x)$ pour tout $k \in \mathbb{Z}$ et $x \in X$, *i.e.* f est constante sur chaque orbite de $\phi(g)$.

11. Dans $\mathbb{R}^3$, on fixe un cube centré en $\mathbf{0}_{\mathbb{R}^3}$. Soit S l'ensemble des sommets et X l'ensemble des faces du cube. On fixe un ensemble Y de $n \in \mathbb{N}^*$ couleurs. On note G le sous-groupe de $\mathsf{O}(\mathbb{R}^3)$ des isométries de $\mathbb{R}^3$ qui laissent l'ensemble S globalement invariant.

(*a*) Montrer que le groupe G agit sur l'ensemble X.

(*b*) On appelle coloriage du cube toute application de X dans Y. Montrer que G agit sur l'ensemble des coloriages du cube.

(*c*) En utilisant la formule de Burnside, on va compter le nombre de coloriages possibles du cubes à rotation du cube près, c'est-à dire le nombre des orbites de l'action de $G^+ = G \cap \mathsf{SO}(\mathbb{R}^3)$ sur l'ensemble des coloriages.

(i) Déterminer $|\mathsf{Fix}(r)|$ pour chaque rotation r appartenant à G^+.

(ii) Conclure en utilisant la formule de Burnside.

Solution.

(*a*) On remarque d'abord que, si $\{e_1, e_2, e_3\}$ est la base canonique de $\mathbb{R}^3$, alors $g(e_i) \in \{\pm e_1, \pm e_2, \pm e_3\}$ pour tout $g \in G$. Pour le démontrer il suffit de vérifier l'affirmation précédente pour chaque élément de G, à partir de la description des éléments de $G = G^+ \sqcup G^-$ de l'exercice **7**. On définit une **face** du cube comme une partie $F \subseteq S$ de cardinal 4 telle que $\sum_{v\in F} v \in \{\pm 4e_1, \pm 4e_2, \pm 4e_3\}$. La lectrice/le lecteur pourra vérifier que cette définition est équivalente à la définition usuelle de face. Alors, c'est clair que $g(F) \in X$ pour tout $F \in X$, car $g(F) \subseteq S$ a cardinal 4 et

$$\sum_{v\in F} g(v) = g\Big(\sum_{v\in F} v\Big) \in \big\{\pm 4g(e_1), \pm 4g(e_2), \pm 4g(e_3)\big\} = \big\{\pm 4e_1, \pm 4e_2, \pm 4e_3\big\}.$$

On voit bien que l'application $G \times X \to X$ qui associe $g(F)$ à $(g, F) \in G \times X$ est bien définie et elle est une action (à gauche) de G sur X, car $1_G(F) = F$ et $(gg')(F) = g(g'(F))$ pour tous $g, g' \in G$ et $F \in X$.

(*b*) L'action de G sur Y^X est celle donnée dans l'exercice **10**, *i.e.* $g \cdot f = f \circ g^{-1}$, pour $g \in G$ et $f \in Y^X$.

(*c*) On veut compter la cardinalité de l'ensemble X^Y/G^+, car on veut identifier deux coloriages s'ils se trouvent dans la même orbite.

(i) D'après le dernier item de l'exercice **10**, on a que

$$\mathsf{Fix}(r) = \{f \in Y^X : f \text{ est constante sur les orbites de } r \text{ sur } F\}.$$

En conséquence, $|\mathsf{Fix}(r)|$ coïncide avec $n^{o(r)}$, où $o(r)$ est la quantité d'orbites de l'action de $\langle r\rangle \subseteq G^+$ sur F. On va utiliser la classification des éléments de G^+ de l'item (c) de l'exercice **7**. C'est clair que $r = \mathsf{id}_{\mathbb{R}^3}$ a $\#(F) = 6$ orbites, ce qui nous dit que $|\mathsf{Fix}(r)| = n^6$ dans ce cas. Si r est l'une des 6 rotations dans $(G^+.2)$ avec angle $\theta \in \{\pi/2, 3\pi/2\}$, alors r a 3 orbites, ce qui nous dit que $|\mathsf{Fix}(r)| = n^3$ dans ce cas. Si r est l'une des 3 rotations dans $(G^+.2)$ avec angle $\theta = \pi$, alors r a 4 orbites, ce qui nous dit que $|\mathsf{Fix}(r)| = n^4$ dans ce cas. Si r est l'une des 8 rotations dans $(G^+.3)$ avec angle $\theta \in \{2\pi/3, 4\pi/3\}$, alors r a 2 orbites, ce qui nous dit que $|\mathsf{Fix}(r)| = n^2$ dans ce cas. Finalement, si r est l'une des 6 rotations dans $(G^+.4)$ avec angle $\theta = \pi$, alors r a 3 orbites, ce qui nous dit que $|\mathsf{Fix}(r)| = n^3$ dans ce cas.

(ii) La formule de Burnside dans l'exercice **9** nous dit que

$$|Y^X/G^+| = \frac{1}{24}\big(n^6 + 6n^3 + 3n^4 + 8n^2 + 6n^3\big) = \frac{n^2}{24}\big(n^4 + 3n^2 + 12n + 8\big).$$

La lectrice minutieuse/le lecteur minutieux vérifiera que le nombre précédent est toujours un entier pour tout $n \in \mathbb{N}^*$.

12. Soient E un K-espace vectoriel de dimension finie et G un groupe fini agissant linéairement sur E, *i.e.* pour tout $g \in G$, l'application $\rho_g : E \to E$ donnée par $v \mapsto g \cdot v$ est linéaire. On obtient ainsi un morphisme de groupes $\rho : G \to \mathsf{GL}(E)$. Soient

$$F = \{v \in E : g \cdot v = v, \text{ pour tout } g \in G\} \text{ et } \pi = \frac{1}{|G|}\sum_{g\in G} \rho(g).$$

Montrer que F est un sous-espace vectoriel de E et que π est un projecteur sur F. En déduire que $\mathsf{Tr}(\pi) = \dim(F)$.

Solution. C'est clair que $g \cdot \mathbf{0}_E = \mathbf{0}_E$ vu que l'action est linéaire. En plus, si $v, w \in F$, alors $v+w \in F$, ce qui nous dit en particulier que $g \cdot (v+w) = g \cdot v + g \cdot w = v+w$ pour tout $g \in G$. En conséquence, F est un sous-espace vectoriel de E.

Par ailleurs, on voit bien que $\pi(v) \in F$ pour tout $v \in E$, car

$$g' \cdot \pi(v) = \frac{1}{|G|} \sum_{g \in G} g' \cdot (g \cdot v) = \frac{1}{|G|} \sum_{g \in G} (g'g) \cdot v = \frac{1}{|G|} \sum_{g \in G} g \cdot v = \pi(v),$$

pour tout $g' \in G$, où l'on a utilisé que l'application $G \to G$ qui associe $g'g$ à $g \in G$ est une bijection. En outre, si $v \in F$,

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v = \frac{1}{|G|} \sum_{g \in G} v = v,$$

ce qui implique que $\pi \circ \pi = \pi$ et que $\mathsf{Img}(\pi) = F$. Cela nous dit que $\mathsf{Ker}(\pi) \oplus \mathsf{Img}(\pi) = E$, vu que $v = (v - \pi(v)) + \pi(v)$ pour tout $v \in E$ nous dit que $\mathsf{Ker}(\pi) + \mathsf{Img}(\pi) = E$ car $\pi(v - \pi(v)) = \pi(v) - \pi(v) = \mathbf{0}_E$, et si $v \in \mathsf{Ker}(\pi) \cap \mathsf{Img}(\pi)$, alors $v = \pi(w)$ et $\pi(v) = \mathbf{0}_E$ impliquent $\mathbf{0}_E = \pi(v) = \pi(\pi(w)) = \pi(w) = v$. En conséquence $\mathsf{Tr}(\pi) = \dim(F)$. En effet, si l'on prend une base $\mathscr{B}'$ de $\mathsf{Img}(\pi)$ et une base $\mathscr{B}''$ de $\mathsf{Ker}(\pi)$, $\mathscr{B} = \mathscr{B}' \cup \mathscr{B}''$ est une base de E. On note que $\pi(v') = v'$ pour tout $v' \in \mathscr{B}'$ et $\pi(v'') = \mathbf{0}_E$ pour tout $v'' \in \mathscr{B}''$. En conséquence, la représentation matricielle de π relative à la base $\mathscr{B}$ est donnée par

$$[\pi]_{\mathscr{B}} = \begin{array}{c} \\ \#(\mathscr{B}') \\ \\ \\ \\ \\ \#(\mathscr{B}'') \\ \\ \\ \end{array} \overbrace{\phantom{\begin{matrix}1&0&0&\cdots&0\end{matrix}}}^{\#(\mathscr{B}')} \overbrace{\phantom{\begin{matrix}0&0&0&\cdots&0\end{matrix}}}^{\#(\mathscr{B}'')} \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

ce qui implique que $\mathsf{Tr}(\pi) = \#(\mathscr{B}') = \dim(F)$.

13. Soit n un entier supérieur ou égal à 2. À tout $\sigma \in \mathbb{S}_n$ on associe l'endomorphisme $u_\sigma \in \mathsf{L}(\mathbb{R}^n)$ défini par

$$u_\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

On note $\mathscr{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$ et P_σ la matrice de u_σ dans $\mathscr{B}$.

(*a*) Calculer $u_\sigma(e_j)$ pour $j \in [\![1, n]\!]$. En déduire les coefficients de P_σ et montrer que u_σ est inversible.

(*b*) Montrer que l'application $\sigma \mapsto u_\sigma$ est un morphisme de $\mathbb{S}_n$ dans $\mathsf{GL}(\mathbb{R}^n)$.

(*c*) Calculer $\det(u_\sigma)$.

(*d*) Quels sont les vecteurs fixes de l'action correspondante de $\mathbb{S}_n$ sur $\mathbb{R}^n$?

(*e*) Déterminer le polynôme caractéristique de u_σ en fonction du type de σ. On se ramènera au cas où chaque orbite de σ est constituée d'entiers consécutifs.

Solution.

(*a*) On voit bien que $u_\sigma(e_j) = e_{\sigma(j)}$, pour $j \in [\![1,n]\!]$. En particulier, $(P_\sigma)_{ij} = \delta_{i,\sigma(j)}$ pour $i,j \in [\![1,n]\!]$. Cela nous dit que $\det(u_\sigma) = \epsilon(\sigma)$, car $\det(v_{\sigma(1)},\dots,v_{\sigma(n)}) = \epsilon(\sigma)\det(v_1,\dots,v_n)$ pour tous $v_1,\dots,v_n \in \mathbb{R}^n$ et $\det(u_\sigma) = \det(e_{\sigma(1)},\dots,e_{\sigma(n)})$. En particulier, u_σ est inversible.

(*b*) On voit bien que

$$\begin{aligned}(u_\sigma \circ u_{\sigma'})(x_1,\dots,x_n) &= u_\sigma(x_{\sigma'^{-1}(1)},\dots,x_{\sigma'^{-1}(n)}) = (x_{\sigma'^{-1}(\sigma^{-1}(1))},\dots,x_{\sigma'^{-1}(\sigma^{-1}(n))})\\ &= (x_{(\sigma\circ\sigma')^{-1}(1)},\dots,x_{(\sigma\circ\sigma')^{-1}(n)}) = u_{\sigma\circ\sigma'}(x_1,\dots,x_n).\end{aligned}$$

En conséquence, l'application $\sigma \mapsto u_\sigma$ est un morphisme de $\mathbb{S}_n$ dans $\mathsf{GL}(\mathbb{R}^n)$.

(*c*) On a montré que $\det(u_\sigma) = \epsilon(\sigma)$.

(*d*) C'est clair que $\bar{x} = (x_1,\dots,x_n)$ satisfait que $u_\sigma \bar{x} = \bar{x}$ si et seulement s'il existe $\lambda \in \mathbb{R}$ tel que $\bar{x} = \lambda(e_1 + \cdots + e_n)$. En effet, $u_\sigma \lambda(e_1+\cdots+e_n) = \lambda(e_1+\cdots+e_n)$. En outre, s'il existe $i,j \in [\![1,n]\!]$ tels que $x_i \neq x_j$, alors $u_{(i\ j)}\bar{x} \neq \bar{x}$.

(*e*) Comme le polynôme caractéristique d'un morphisme u coïncide avec le polynôme caractéristique du conjugué vuv^{-1} pour tout v automorphisme, on peut supposer sans perte de généralité que la matrice u_σ est formée de blocs $u_1 \in M_{n_1}(\mathbb{R})$, …, $u_r \in M_{n_r}(\mathbb{R})$. Plus précisément, on pose $n_1 \leq \cdots \leq n_r \in \mathbb{N}^*$ tels que $\#(\{i : n_i = d\}) = \mathsf{type}(\sigma)(d)$ pour tout $d \in \mathbb{N}^*$. Noter que $n_1 + \cdots + n_r = n$. Alors, il existe des matrices $u_1 \in M_{n_1}(\mathbb{R})$, …, $u_r \in M_{n_r}(\mathbb{R})$ telles que

$$u_i = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1\\ 1 & 0 & 0 & \dots & 0 & 0\\ 0 & 1 & 0 & \dots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & 0 & 0\\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

pour tout $i \in [\![1,r]\!]$ et

$$u = \begin{pmatrix} u_1 & 0 & \dots & 0\\ 0 & u_2 & \dots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & u_r \end{pmatrix}.$$

Or, c'est facile à vérifier que $\chi_i = \det(u_i - \lambda\,\mathrm{id}_{\mathbb{R}^{n_i}}) = (-\lambda)^{n_i} - (-1)^{n_i}$, pour tout $i \in [\![1,r]\!]$. En conséquence, le polynôme caractéristique χ de u_σ est

$$\chi = \prod_{i=1}^{r} \chi_i = (-1)^n \prod_{i=1}^{r} (\lambda^{n_i} - 1).$$

⋆ **14.** *Sous-groupes finis du groupe spécial orthogonal en dimension* 3. Soient E un espace euclidien orienté de dimension 3 et G un sous-groupe fini de $\mathsf{SO}(E)$ d'ordre $n \neq 1$. Pour tout $g \in G \setminus \{\mathrm{id}_E\}$, on note $D_g = \mathsf{Ker}(g - \mathrm{id}_E)$ l'axe de la rotation g. On

note S la sphère unité de E et

$$F = \bigcup_{g \in G \setminus \{\mathrm{id}_E\}} (D_g \cap S).$$

(a) Montrer que F est fini et que tout élément de G induit une permutation de F.

(b) Soient $O_1, \dots, O_s$ les orbites de l'action de G sur F rangées par cardinaux croissants. Pour $x \in F$, on note S_x le stabilisateur de x. Montrer que l'ordre de S_x est constant sur chaque orbite O_k. Dans la suite, on note n_k cette constante.

(c) En calculant le cardinal de $D = \{(g,x) \in (G \setminus \{\mathrm{id}_E\}) \times F : g(x) = x\}$ de deux manières différentes, montrer que

$$2n - 2 = ns - \sum_{k=1}^{s} |O_k| \text{ et } 2 - \frac{2}{n} = \sum_{k=1}^{s} \Big(1 - \frac{1}{n_k}\Big).$$

(d) Montrer que l'on est dans l'un des cinq cas suivants :

(C.1) $s = 2$ et $n_1 = n_2 = n$;

(C.2) $s = 3$, n pair et $(n_1, n_2, n_3) = (n/2, 2, 2)$;

(C.3) $s = 3$, $n = 12$ et $(n_1, n_2, n_3) = (3, 3, 2)$;

(C.4) $s = 3$, $n = 24$ et $(n_1, n_2, n_3) = (4, 3, 2)$;

(C.5) $s = 3$, $n = 60$ et $(n_1, n_2, n_3) = (5, 3, 2)$.

Indication : montrer que $s \in \{2, 3\}$ et lorsque $s = 3$ montrer que $n_3 = 2$ et $n_2 \in \{2, 3\}$.

(e) Dans les deux premiers cas, montrer l'existence d'une droite stable par tous les éléments de G.

Remarque : on peut montrer que G est l'ensemble des rotations préservant un polygone régulier à n sommets dans le premier cas, et l'ensemble des isométries préservant un polygone régulier à $n/2$ sommets dans le deuxième. Les trois derniers cas sont plus difficiles. On peut montrer que dans ces cas, G est l'ensemble des rotations de E préservant un polyèdre régulier et que G est isomorphe à $\mathbb{A}_4$, $\mathbb{S}_4$ ou $\mathbb{A}_5$.

Solution.

(a) On remarque d'abord que pour tout $g \in G \setminus \{\mathrm{id}_E\}$ il existe $v_g \in E$ de norme 1 tel que $D_g = \mathsf{Ker}(g - \mathrm{id}_E) = \langle v_g \rangle$, ce qui implique que $D_g \cap S = \{\pm v_g\}$. En conséquence, F, vu que c'est une réunion finie d'ensembles finis.

Par ailleurs, étant donné $g, g' \in G$ et $v_{g'}$ tel que $D_{g'} \cap S = \{\pm v_{g'}\}$, on note que $(gg'g^{-1})(g(v_{g'})) = g((g'(v_{g'}))) = g(v_{g'})$, *i.e.* $g(v_{g'}) \in D_{gg'g^{-1}}$. En plus, comme $G \subseteq \mathsf{SO}(E)$, alors $g(v_{g'}) \in S$, *i.e.* $g(v_{g'}) \in D_{gg'g^{-1}} \cap S \subseteq F$. En conséquence, $g(v) \in F$ pour tout $v \in F$. Cela implique que l'application $G \times F \to F$ donnée par $(g, v) \mapsto g(v)$ détermine une action (à gauche) de G sur F, vu $1_G(v) = v$ et $g(g'(v)) = (gg')(v)$ pour tous $g, g' \in G$ et $v \in F$.

(b) On sait que les stabilisateurs de deux points dans la même orbite sont conjugués, d'après l'exercice **3**, (c). En conséquence, $|S_v| = |S_{v'}|$ pour tous $v, v' \in O_k$ et $k \in [\![1, s]\!]$.

(c) On note d'abord que les deux identités demandées sont équivalentes, car

$$2n - 2 = ns - \sum_{k=1}^{s} |O_k|$$

est équivalent à

$$2-\frac{2}{n}=s-\sum_{k=1}^{s}\frac{|O_k|}{n}=\sum_{k=1}^{s}1-\sum_{k=1}^{s}\frac{1}{n_k}=\sum_{k=1}^{s}\Big(1-\frac{1}{n_k}\Big),$$

en divisant par n, où l'on a utilisé que $n_k = n/|O_k|$ pour tout $k \in [\![1,s]\!]$.

Pour montrer l'égalité demandée, on remarque d'abord que

$$D=\bigsqcup_{v\in F}\big(\mathsf{Stab}(v)\setminus\{\mathsf{id}_E\}\big)\times\{v\}=\bigsqcup_{k=1}^{s}\bigsqcup_{v\in O_k}\big(\mathsf{Stab}(v)\setminus\{\mathsf{id}_E\}\big)\times\{v\}.$$

On choisit $v_k \in O_k$ pour $k \in [\![1,s]\!]$. C'est clair qu'il existe une bijection entre $(\mathsf{Stab}(v)\setminus\{\mathsf{id}_E\})\times\{v\}$ et $\mathsf{Stab}(v_k)\setminus\{\mathsf{id}_E\}$ pour tout $v \in O_k$ et $k \in [\![1,s]\!]$. En conséquence,

$$\#(D)=\sum_{k=1}^{s}\sum_{v\in O_k}(n_k-1)=\sum_{k=1}^{s}\frac{n}{n_k}(n_k-1)=n\sum_{k=1}^{s}\Big(1-\frac{1}{n_k}\Big),$$

où l'on a utilisé que le cardinal de $\mathsf{Stab}(v_k)\setminus\{\mathsf{id}_E\}$ est n_k-1 et $n_k = n/|O_k|$ pour tout $k \in [\![1,s]\!]$. Par ailleurs,

$$D=\bigsqcup_{g\in G\setminus\{\mathsf{id}_E\}}\{\pm v_g\}$$

nous dit que $\#(D) = (n-1)2$. En conséquence,

$$2(n-1)=\#(D)=n\sum_{k=1}^{s}\Big(1-\frac{1}{n_k}\Big),$$

qui nous donne la deuxième identité dans l'énoncé si l'on divise par n.

(*d*) On note d'abord que $1 \le 2-2/n < 2$ pour $n \ge 2$. En particulier, si $s = 1$, l'identité dans l'item précédent nous dit que

$$1\le 2-\frac{2}{n}=1-\frac{1}{n_1}<1,$$

ce qui est impossible. On considère désormais que $s \ge 2$.

Par ailleurs, on note que $\#(F)=\sum_{k=1}^{s}|O_k|$. La première identité dans l'item précédent est donc équivalente à $2n-2 = ns-\#(F)$, *i.e.* $\#(F) = n(s-2)+2$. En outre, la définition de F nous dit que $\#(F) \le 2n-2$. En conséquence, on trouve que $n(s-2)+2 \le 2n-2$. Si $s \ge 4$, alors on conclut que $2n+2 \le n(s-2)+2 \le 2n-2$, ce qui est impossible. En conséquence, $s \in \{2,3\}$.

Si $s = 2$, alors $\#(F) = n(2-2)+2 = 2$ et donc $|O_1| = |O_2| = 1$, car $|O_1|+|O_2| = \#(F) = 2$ et $|O_1|, |O_2| \ge 1$. En conséquence, $n_1 = n_2 = n$, car $n_k = n/|O_k|$ pour $k \in \{1,2\}$, ce qui nous donne le cas (C.1).

On suppose maintenant que $s = 3$. On remarque que la définition de F nous dit que $\#(F)$ est pair, vu que l'application $v \mapsto -v$ induit une involution sans points fixes de F. Comme $\#(F) = n(3-2)+2 = n+2$, n est aussi pair. En outre, la première identité dans l'item précédent est équivalente à

$$\sum_{k=1}^{3}\frac{1}{n_k}=1+\frac{2}{n}. \tag{2}$$

On remarque aussi que, par hypothèse, $n_1 \ge n_2 \ge n_3$. Si $n_3 \ge 3$, alors $n_1 \ge n_2 \ge n_3 \ge 3$ et (2) donne

$$1<1+\frac{2}{n}=\sum_{k=1}^{3}\frac{1}{n_k}\le\frac{1}{3}+\frac{1}{3}+\frac{1}{3}=1,$$

ce qui est absurde.

En conséquence, $n_3 \in \{1,2\}$. Si $n_3 = 1$, alors (2) devient

$$\sum_{k=1}^{2} \frac{n}{n_k} = 2, \tag{3}$$

dont la seule solution est $n_1 = n_2 = n$, car n_1 et n_2 divisent n. Dans ce cas, on a précisément deux éléments différents $v, w \in F$ tels que $g(v) = v$ et $g(w) = w$ pour tout $g \in G$. Par définition, $-v \in F$ car $g(-v) = -g(v) = -v$, ce qui implique que $w = -v$. Or, comme $g(v) = v$ pour tout $g \in G\,\mathsf{SO}_3(\mathbb{R})$, on conclut que G est formé de rotations autour de l'axe déterminé par v, ce qui implique que $F = \{\pm v\}$, par définition de F. Comme dans ce $\#(F) = n+2$, on conclut que $n = 0$, ce qui est absurde.

En outre, on note que si $n_3 = 2$, alors (2) devient

$$\sum_{k=1}^{2} \frac{1}{n_k} = \frac{2}{n} + \frac{1}{2}. \tag{4}$$

Si $n_2 \geq 4$, alors $n_1 \geq n_2 \geq 4$, ce qui nous dit que

$$\frac{1}{2} < \frac{1}{2} + \frac{2}{n} = \sum_{k=1}^{2} \frac{1}{n_k} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$

ce qui est absurde. En conséquence, si $n_3 = 2$, alors $n_2 \in \{2,3\}$. Si $n_2 = n_3 = 2$, (4) équivaut à $n_1 = n/2$, ce qui donne le cas (C.2). Si $n_2 = 3$ et $n_3 = 2$, (4) devient l'identité de nombres entiers donnée par

$$n + 12 = 6\frac{n}{n_1}. \tag{5}$$

Soit $n_1' = n/n_1$. Comme n_1' est un diviseur de n, alors l'identité précédente nous dit que $n_1' | 12$, *i.e.* $n_1' \in \{1,2,3,4,6,12\}$. Si l'on remplace les valeurs précédentes de n_1' dans (5), on utilise que $n \geq 2$ et $n_1 \geq n_2 = 3$, on trouve que $(n_1, n) \in \{(3,12),(4,24),(5,60)\}$, ce qui nous donne les cas (C.3), (C.4) et (C.5).

(*e*) On suppose d'abord que $s = 2$. Comme on a vu dans l'item précédent, $\#(F) = 2$ dans ce cas, et on a donc $F = \{\pm v\}$. Par définition $g(v) = v$ pour tout $g \in G$, car sinon on devrait avoir $v_g \in D_g \cap S$ avec $v_g \neq \pm v$, ce qui est absurde. La droite engendré par v est donc stable par l'action de tout élément de G.

On suppose maintenant que $s = 3$, $n_1 = n/2$ et $n_2 = n_3 = 2$. Comme on a vu dans l'item précédent, $\#(F) = n+2$ dans ce cas. Comme $n_1 = n/2$, il existe une orbite $\{v, w\}$ de F à 2 éléments. Si l'on considère la droite engendrée par v et w, on conclut qu'elle est stable par l'action de G.

15. Soient X un ensemble fini et K un corps. Pour tout $x \in X$, on note δ_x l'application de X dans K qui associe 1 à x et 0 à tous les autres éléments de X.

(*a*) Montrer que $(\delta_x)_{x \in X}$ est une base du K-espace vectoriel K^X.

(*b*) Soient G un groupe agissant sur l'ensemble X et $\phi : G \to \mathsf{Aut}_{\mathsf{Ens}}(X)$ le morphisme de groupes associé. Montrer que l'action du groupe G sur K^X définie par $g \cdot f = f \circ \phi(g)^{-1}$, pour tous $g \in G$ et $f \in K^X$, est linéaire. On notera $\rho : G \to \mathsf{GL}(K^X)$ le morphisme de groupes associé.

(*c*) Pour tout $g \in G$, on note $\mathsf{Fix}(g)$ l'ensemble des points fixes de $\phi(g)$. Montrer que $|\mathsf{Fix}(g)| = \mathsf{Tr}(\rho(g))$.

(*d*) Soit $F = \{v \in K^X : g \cdot v = v \text{ pour tout } g \in G\}$. Montrer qu'une application $f : X \to K$ appartient à F si et seulement si elle est constante sur chaque orbite de l'action de G sur X.

(*e*) En déduire que la dimension de F est $|X/G|$, où X/G désigne l'ensemble des orbites de l'action de G sur X.

(*f*) Retrouver la formule de Burnside, *i.e.*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |\,\mathsf{Fix}(g)|.$$

Solution.

(*a*) C'est clair que $(\delta_x)_{x\in X}$ est un ensemble libre car, si $\sum_{x\in X} c_x\delta_x$ est la fonction nulle, où $c_x \in K$ pour tout $x \in X$, alors

$$0 = \sum_{x\in X} c_x\delta_x(y) = c_y$$

pour tout $y \in X$, ce qui implique que $c_x = 0$ pour tout $x \in X$. En outre, si $f \in K^X$, c'est clair que $f = \sum_{x\in X} f(x)\delta_x$, ce qui implique que $(\delta_x)_{x\in X}$ est une famille génératrice de K^X. On conclut que $(\delta_x)_{x\in X}$ est une base de K^X.

(*b*) On voit bien que

$$g \cdot (f_1 + \lambda f_2) = (f_1 + \lambda f_2) \circ \phi(g)^{-1} = f_1 \circ \phi(g)^{-1} + \lambda f_2 \circ \phi(g)^{-1} = g \cdot f_1 + \lambda g \cdot f_2,$$

pour tous $f_1, f_2 \in K^X$, $\lambda \in K$ et $g \in G$. En conséquence, l'action du groupe G sur K^X est linéaire. Noter que $g \cdot \delta_x = \delta_{\phi(g)(x)}$ pour tout $x \in X$.

(*c*) On rappelle que $\mathsf{Fix}(g) = \{x \in X : \phi(g)(x) = x\}$. On considère les ensemble $D_g = \{\delta_x : x \in \mathsf{Fix}(g)\}$ et $C_g = \{\delta_x : x \notin \mathsf{Fix}(g)\}$. C'est clair que $g \cdot \delta_x = \delta_x$ pour tout $x \in D_g$ et $g \cdot \delta_x = \delta_{\phi(g)(x)} \neq \delta_x$ pour tout $x \in C_g$, d'après la dernière identité dans l'item précédent. On fixe un ordre total sur X avec $x < y$ si $x \in \mathsf{Fix}(g)$ et $y \notin \mathsf{Fix}(g)$. Alors, la représentation matricielle de $\rho(g)$ dans la base $(\delta_x)_{x\in X}$ est donnée par une matrice $(A_{x,y})_{x,y\in X}$ qui satisfait que $A_{x,x} = 1$ pour $x \in \mathsf{Fix}(g)$ et $A_{x,x} = 0$ pour $x \notin \mathsf{Fix}(g)$. Cela nous dit en particulier que $\mathsf{Tr}(\rho(g)) = |\,\mathsf{Fix}(g)|$.

(*d*) On voit bien que $f \in F$ si et seulement si $g \cdot f = f$ pour tout $g \in G$, ce qui équivaut à $f(x) = f(\phi(g)(x))$ pour tout $x \in X$ et $g \in G$, *i.e.* f est constante sur chaque orbite de l'action de G sur X.

(*e*) C'est facile à vérifier que $\{\hat{\delta}_{\bar{x}} : \bar{x} \in X/G\}$ forme une base de F, où $\hat{\delta}_{\bar{x}} = \sum_{x\in\bar{x}} \delta_x$ pour tout $\hat{x} \in X/G$. En effet, si $\sum_{\bar{x}\in X/G} c_{\bar{x}}\hat{\delta}_{\bar{x}}$ est la fonction nulle, alors

$$0 = \sum_{\bar{x}\in X/G} c_{\bar{x}}\hat{\delta}_{\bar{x}}(y) = c_{\bar{y}}\Big(\sum_{y'\in\bar{y}} \delta_{y'}\Big)$$

pour tout $y \in X$, où $y \in \bar{y}$, ce qui implique que $c_{\bar{y}} = 0$, vu que $(\delta_x)_{x\in X}$ est un ensemble libre. En outre, $\{\hat{\delta}_{\bar{x}} : \bar{x} \in X/G\}$ est une famille génératrice, car, si $f \in F$, on a que

$$f = \sum_{\bar{x}\in X/G}\sum_{x\in\bar{x}} c_{\bar{x}}\delta_x = \sum_{\bar{x}\in X/G} c_{\bar{x}}\hat{\delta}_{\bar{x}},$$

d'après l'item précédent. On conclut que $\mathsf{dim}(F) = \#(X/G)$.

(*f*) Comme

$$\pi = \frac{1}{|G|}\sum_{g\in G}\rho(g) : K^X \to K^X$$

est un projecteur d'image F d'après l'exercice **12**, on conclut que

$$\#(X/G) = \dim(F) = \dim\big(\mathrm{Img}(\pi)\big) = \mathrm{Tr}(\pi) = \mathrm{Tr}\Big(\frac{1}{|G|}\sum_{g\in G}\rho(g)\Big)$$
$$= \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\big(\rho(g)\big) = \frac{1}{|G|}\sum_{g\in G}|\,\mathrm{Fix}(g)|,$$

où l'on a utilisé les items précédents dans la première et la dernière identités.

16. On considère l'espace vectoriel $\mathbb{C}^n$ et l'espace vectoriel A_n des applications polynomiales de $\mathbb{C}^n$ dans $\mathbb{C}$.

(*a*) Définir une action linéaire non triviale du groupe $\mathsf{GL}_n(\mathbb{C})$ sur A_n.

(*b*) Soient G un sous-groupe de $\mathsf{GL}_n(\mathbb{C})$ et $F = \{v \in A_n : g\cdot v = v \text{ pour tout } g \in G\}$. Montrer qu'une application polynomiale $f : \mathbb{C}^n \to \mathbb{C}$ appartient à F si et seulement si elle est constante sur chaque orbite de l'action de G sur $\mathbb{C}^n$.

(*c*) Lorsque $G = \{\pm \mathrm{id}_{\mathbb{C}^n}\}$, déterminer F.

Solution.

(*a*) On affirme d'abord que $P \circ g^{-1} \in A_n$ pour tout $P \in A_n$ et $g \in \mathsf{GL}_n(\mathbb{C})$. En effet, $P = \sum_{\bar{i}\in\mathbb{N}^n} c_{\bar{i}} X^{\bar{i}}$, où $X^{\bar{i}} = X_1^{i_1}\dots X_n^{i_n}$, $c_{\bar{i}} \in \mathbb{C}$ et la somme précédente a support fini, *i.e.* $\{\bar{i} \in \mathbb{N}^n : c_{\bar{i}} \neq 0\}$ est fini, et g^{-1} est donné par la matrice $(A_{i,j})_{1\le i,j\le n}$, alors

$$P \circ g^{-1} = \sum_{\bar{i}\in\mathbb{N}^i} c_{\bar{i}} \prod_{j=1}^{n}\Big(\sum_{k=1}^{n} A_{j,k}X_k\Big)^{i_j} \in A_n.$$

On considère alors l'application $\rho : \mathsf{GL}_n(\mathbb{C}) \times A_n \to A_n$ qui associe $P \circ g^{-1}$ à $(g,P) \in \mathsf{GL}_n(\mathbb{C}) \times A_n$. C'est clair que $\rho(\mathsf{I}_n, P) = P \circ \mathsf{I}_n^{-1} = P$ et

$$\rho\big(g, \rho(h,P)\big) = \rho(g, P\circ h^{-1}) = P \circ h^{-1} \circ g^{-1} = P \circ (gh)^{-1} = \rho(gh, P)$$

pour tous $P \in A_n$ et $g,h \in \mathsf{GL}_n(\mathbb{C})$. On écrira aussi $\rho(g,P) = g\cdot P$, pour $P \in A_n$ et $g \in \mathsf{GL}_n(\mathbb{C})$.

(*b*) On voit bien que $f \in F$ si et seulement si $g \cdot f = f$ pour tout $g \in G$, ce qui équivaut à $f(x) = f(g(x))$ pour tout $x \in \mathbb{C}^n$ et $g \in G$, *i.e.* f est constante sur chaque orbite de l'action de G sur $\mathbb{C}^n$.

(*c*) C'est clair que $F = \{P \in A_n : P(-\bar{X}) = P(\bar{X})\}$. En plus, on voit bien que $P \in A_n$ satisfait $P(-\bar{X}) = P(\bar{X})$ si et seulement si

$$P = \sum_{\substack{\bar{i}\in\mathbb{N}^n \\ |\bar{i}|\in 2\mathbb{Z}}} c_{\bar{i}} X^{\bar{i}},$$

où $|\bar{i}| = i_1 + \dots + i_n$.

17. Soit p un entier premier. On se propose de faire la liste des groupes d'ordre p^2 à isomorphisme près.

(*a*) Soit G un groupe. On suppose que le quotient de G par son centre est un groupe cyclique. Montrer que le groupe G est abélien.

(*b*) Soit G un groupe d'ordre p^2.

(i) En utilisant l'action de G sur lui-même par conjugaison, montrer que le centre de G n'est pas réduit à l'élément neutre.

(ii) Montrer que le groupe G est abélien.

(iii) Montrer que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Solution.

(*a*) Comme $G/\mathscr{Z}(G)$ est cyclique, il existe $g \in G$ tel que $g\mathscr{Z}(G)$ est le générateur de $G/\mathscr{Z}(G)$. En conséquence, étant donné $x, y \in G$ il existe $n, m \in \mathbb{Z}$ et $x', y' \in \mathscr{Z}(G)$ tels que $x = g^n x'$ et $y = g^m y'$. En conséquence, $xy = g^n x' g^m y' = g^{n+m} x' y' = g^{n+m} y' x' = g^m y' g^n x' = yx$, *i.e.* G est abélien.

Noter que ce résultat n'est pas valide si l'on remplace cyclique par abélien, vu que le centre du groupe non abélien $G = \mathscr{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ des quaternions est $\mathscr{Z}(\mathscr{H}) = \{\pm 1\}$ et le quotient $\mathscr{H}/\mathscr{Z}(\mathscr{H})$ est un groupe d'ordre 4, donc *a fortiori* abélien.

(*b*) (i) Pour un groupe G d'ordre p^n avec $n \in \mathbb{N}^*$, l'équation de classes (pour l'action donnée par conjugaison) nous dit que l'on peut écrire

$$|G| = |\mathscr{Z}(G)| + \sum_{i=1}^{s} [G : \mathsf{Stab}(x_i)],$$

où $\{x_1, \dots, x_s\} \subseteq G \setminus \mathscr{Z}(G)$ satisfait que $\{\mathsf{cl}(x_1), \dots, \mathsf{cl}(x_s)\}$ est une famille disjointe dont la réunion est $G \setminus \mathscr{Z}(G)$. Comme $\mathsf{Stab}(x_i)$ est un sous-groupe de G différent de G, son ordre est de la forme $p^m < |G|$ avec $m \in \mathbb{N}^*$, ce qui implique $p | [G : \mathsf{Stab}(x_i)]$ pour tout $i \in [\![1, s]\!]$. Comme $p || G|$, on conclut que $p || \mathscr{Z}(G)|$ et en particulier $\mathscr{Z}(G)$ n'est pas trivial.

(ii) Comme $p || \mathscr{Z}(G)|$ et $|G| = p^2$, on voit que $G/\mathscr{Z}(G)$ a ordre 1 ou p, ce qui nous dit que $G/\mathscr{Z}(G)$ est cyclique. D'après le premier item on conclut que G est abélien.

(iii) S'il existe $g \in G$ tel que $G = \langle g \rangle$, alors le morphisme de groupes surjectif $\mathbb{Z} \to G$ donné par $n \mapsto g^n$ pour $n \in \mathbb{Z}$ induit un isomorphisme $\mathbb{Z}/p^2\mathbb{Z} \to G$. On suppose que pour tout $g \in G$, le sous-groupe engendré par g est différent de G. Cela équivaut à dire que $\langle g \rangle$ a ordre p pour tout $g \in G \setminus \{1_G\}$. On fixe donc $g \in G \setminus \{1_G\}$ et on prend $h \in G \setminus \langle g \rangle$. Noter que $\langle g \rangle \cap \langle h \rangle = \{1_G\}$, car $\langle g \rangle \cap \langle h \rangle$ est un sous-groupe de $\langle g \rangle$ et en conséquence a ordre 1 ou p, et le dernier cas équivaut à $\langle g \rangle = \langle h \rangle$, ce qui est impossible car $h \notin \langle g \rangle$. On considère le morphisme de groupes $f : \mathbb{Z}^2 \to G$ donné par $(n, m) \mapsto g^n h^m$ pour $n, m \in \mathbb{Z}$. Comme $\langle g \rangle \cap \langle h \rangle = \{1_G\}$, on conclut que l'ordre de l'image de f est strictement supérieur à p, ce qui implique que f est surjectif. En outre, comme g et h ont ordre p, f induit un morphisme de groupes surjectif $\bar{f} : (\mathbb{Z}/p\mathbb{Z})^2 \to G$. Comme les deux groupes ont la même cardinalité finie, $\bar{f}$ est un isomorphisme de groupes.

18. *Petit théorème de Fermat.* Soient p un nombre premier et $a \in \mathbb{N}^*$. Soient A un ensemble à a éléments et $E = A^p$. On note $\gamma = (1 \quad 2 \quad \cdots \quad p) \in \mathbb{S}_p$.

(*a*) Montrer que la formule $\sigma \cdot (x_1, \dots, x_p) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(p)})$ définit une action de $\langle \gamma \rangle$ sur E.

(*b*) Décrire l'orbite d'un élément $(x_1, \dots, x_p) \in E$.

(*c*) À l'aide de l'équation aux orbites, en déduire que $a^p \equiv a \pmod{p}$.

Solution.

(*a*) C'est clair que la formule $\sigma \cdot (x_1, \dots, x_p) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(p)})$ définit une action de $\mathbb{S}_p$ sur E, car $\mathsf{id}_{[\![1,p]\!]} \cdot (x_1, \dots, x_p) = (x_1, \dots, x_p)$ et

$$\begin{aligned}\rho \cdot \big(\sigma \cdot (x_1, \dots, x_p)\big) &= \rho \cdot (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(p)}) = (x_{\sigma^{-1}(\rho^{-1}(1))}, \dots, x_{\sigma^{-1}(\rho^{-1}(p))}) \\ &= (x_{(\rho\sigma)^{-1}(1)}, \dots, x_{(\rho\sigma)^{-1}(p)}) = (\rho\sigma) \cdot (x_1, \dots, x_p),\end{aligned}$$

pour tous $\rho, \sigma \in \mathbb{S}_p$ et $(x_1, \dots, x_p) \in E$. On conclut que cela définit *a fortiori* une action de $\langle\gamma\rangle$ sur E.

(*b*) C'est clair que

$$\mathsf{Orb}(x_1, \dots, x_p) = \big\{(x_i, \dots, x_p, x_1, \dots, x_{i-1}) : i \in [\![1, p]\!]\big\}.$$

En particulier, noter que $\#(\mathsf{Orb}(x_1, \dots, x_p)) = 1$ si et seulement si $(x_1, \dots, x_p) = (x, \dots, x)$ pour $x \in A$. On conclut qu'il existe précisément a orbites de cardinalité 1. En outre, si $\#(\mathsf{Orb}(x_1, \dots, x_p)) > 1$, alors $\#(\mathsf{Orb}(x_1, \dots, x_p)) = p$, car $\#(\mathsf{Orb}(x_1, \dots, x_p))$ est le cardinal du quotient de $|\langle\gamma\rangle| = p$ par le cardinal du groupe d'isotropie de $(x_1, \dots, x_p)$.

(*c*) On sait que

$$a^p = \#(E) = \sum_{\bar{x} \in E/\langle\gamma\rangle} \#(\bar{x}) = \sum_{\substack{\bar{x} \in E/\langle\gamma\rangle \\ \#(\bar{x}) = 1}} \#(\bar{x}) + \sum_{\substack{\bar{x} \in E/\langle\gamma\rangle \\ \#(\bar{x}) = p}} \#(\bar{x}) = a + \sum_{\substack{\bar{x} \in E/\langle\gamma\rangle \\ \#(\bar{x}) = p}} \#(\bar{x}),$$

ce qui implique que $a^p \equiv a \pmod p$, car la dernière somme est un multiple de p.

19. *Lemme de Cauchy.* Soit G un groupe fini d'ordre n et soit p un diviseur premier de n. On note $E = \{(x_1, \dots, x_p) \in G^p : x_1 \cdots x_p = 1_G\}$ et $\gamma = (1 \quad 2 \quad \cdots \quad p) \in \mathbb{S}_p$.

(*a*) Montrer que la formule $\sigma \cdot (x_1, \dots, x_p) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(p)})$ définit une action de $\langle\gamma\rangle$ sur E.

(*b*) Décrire l'orbite d'un élément $(x_1, \dots, x_p) \in E$.

(*c*) À l'aide de l'équation aux orbites, montrer que p divise le nombre de solutions de l'équation $x^p = 1_G$ dans G.

(*d*) En déduire que G possède au moins un sous-groupe d'ordre p.

Solution.

(*a*) On affirme d'abord que $\gamma \cdot (x_1, \dots, x_p) = (x_p, x_1 \dots, x_{p-1}) \in E$ si $(x_1, \dots, x_p) \in E$. En effet, $x_p x_1 \dots, x_{p-1} = x_p x_1 \dots, x_{p-1} x_p x_p^{-1} = x_p x_p^{-1} = 1_G$. En conséquence, $\gamma^k \cdot (x_1, \dots, x_p) = (x_p, x_1 \dots, x_{p-1}) \in E$ si $(x_1, \dots, x_p) \in E$ et $k \in \mathbb{N}$, ce qui implique que $\sigma \cdot (x_1, \dots, x_p) = (x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(p)}) \in E$ si $\sigma \in \langle\gamma\rangle$. On a montré dans le premier item de l'exercice **18** que l'expression précédente satisfait les conditions dans la définition d'action à gauche et en conséquence définit une action de $\langle\gamma\rangle$ sur E.

Pour $g \in G$, on définit $E_g = \{(x_1, \dots, x_p) \in G^p : x_1 \cdots x_p = g\}$. Alors, $E_{1_G} = E$ et l'application $f_{g,h} : E_g \to E_h$ donnée par $(x_1, \dots, x_p) \mapsto (hg^{-1}x_1, \dots, x_p)$ est bijective, car $f_{g,h} \circ f_{h,g} = \mathsf{id}_{E_h}$ pour tous $g, h \in G$. On conclut que $n^p = \#(G^p) = n\#(E)$, car $G^p = \sqcup_{g \in G} E_g$, ce qui nous dit que $\#(E) = n^{p-1}$. Comme $p \geq 2$ et $p | n$, on conclut que $p | \#(E)$.

(*b*) C'est clair que

$$\mathsf{Orb}(x_1,\dots,x_p)=\big\{(x_i,\dots,x_p,x_1,\dots,x_{i-1}) : i\in[\![1,p]\!]\big\}.$$

En particulier, on remarque que $\#(\mathsf{Orb}(x_1,\dots,x_p)) = 1$ si et seulement si $(x_1,\dots,x_p) = (x,\dots,x)$ pour $x \in G$. En outre, si $\#(\mathsf{Orb}(x_1,\dots,x_p)) > 1$, alors $\#(\mathsf{Orb}(x_1,\dots,x_p)) = p$, car $\#(\mathsf{Orb}(x_1,\dots,x_p))$ est le cardinal du quotient de $|\langle\gamma\rangle| = p$ par le cardinal du groupe d'isotropie de $(x_1,\dots,x_p)$.

(*c*) On sait que

$$\#(E)=\sum_{\bar{x}\in E/\langle\gamma\rangle}\#(\bar{x})=\sum_{\substack{\bar{x}\in E/\langle\gamma\rangle\\ \#(\bar{x})=1}}\#(\bar{x})+\sum_{\substack{\bar{x}\in E/\langle\gamma\rangle\\ \#(\bar{x})=p}}\#(\bar{x})=\#\big(\{x\in G : x^p=1_G\}\big)+\sum_{\substack{\bar{x}\in E/\langle\gamma\rangle\\ \#(\bar{x})=p}}\#(\bar{x}).$$

En plus, c'est clair que la dernière somme est un multiple de p. Comme $p|\#(E)$, p divise $\#(\{x \in G : x^p = 1_G\})$.

(*d*) Comme p divise $\#(\{x \in G : x^p = 1_G\})$, il existe $x \in G \setminus \{1_G\}$ tel que $x^p = 1_G$. Cela nous dit que le sous groupe $\langle x\rangle$ a ordre p.