Exercices du chapitre 5

Exercice 5.2. (i) On a $\varphi > 1$. Pour voir que les 12 faces sont équilatérales il suffit de montrer que la largeur commune des trois rectangles, à savoir 2, coïncide avec celle du segment AB avec $A = (\varphi, 0, 1)$ (un sommet du rectangle vert foncé) et $B = (0, 1, \varphi)$ (un sommet du rectangle violet). Mais on a $AB^2 = \varphi^2 + 1 + (\varphi - 1)^2 = 2 - 2\varphi + 2\varphi^2$, et donc $AB = 2$ si, et seulement si, $\varphi^2 = \varphi + 1$. L'unique solution > 1 de cette équation est bien le nombre d'or $\frac{1+\sqrt{5}}{2}$.

(ii) Le centre d'une face (un triangle équilatéral) est l'isobarycentre de ses sommets. Le centre de la face F supérieure est donc

$$\frac{1}{3}((\varphi, 0, 1) + (0, 1, \varphi) + (0, -1, \varphi)) = \frac{1}{3}(\varphi, 0, \varphi^3)$$

en notant $\varphi^3 = \varphi(1+\varphi) = 1+2\varphi$. De même le centre de la face adjacente à F et contenant $(1, \varphi, 0)$ est $\frac{1}{3}((\varphi, 0, 1)+(1, \varphi, 0)+(0, 1, \varphi)) = \frac{1}{3}(\varphi^2, \varphi^2, \varphi^2)$ Par construction, le sous-groupe $G \subset \mathrm{O}(3)$ constitué des permutations circulaires (ou triviales) des coordonnées et des changements de signes (qui est d'ordre 24) est un sous-groupe du groupe des isométries de I. Il permute donc ses 20 faces, et donc leurs centres. L'orbite par G de $\frac{1}{3}(\varphi, 0, \varphi^3)$ a clairement $3 \cdot 4 = 12$ points, et celle de $\frac{1}{3}(\varphi^2, \varphi^2, \varphi^2)$ en a $2^3 = 8$. On conclut par $8+12 = 20$.

Exercice 5.3. (i) L'angle au sommet d'un polygone régulier à $n \geqslant 3$ côtés est $\pi - 2\pi/n$. La somme des angles entre les f demi-droites consécutives est 2π. On a donc $2\pi > (\pi - 2\pi/n)f$ puis $1/2 < 1/f + 1/n$.

(ii) Comme on a $f \geqslant 3$ et $1/3 + 1/6 = 9/18 = 1/2$, on a $3 \leqslant n \leqslant 5$, et de même $3 \leqslant f \leqslant 5$, et aussi $f = 3$ ou $n = 3$ car $1/4 + 1/4 = 1/2$. Les seules solutions sont donc $(n, f) = (3, 3), (3, 4), (4, 3), (3, 5), (5, 3)$. Soit P un polyèdre convexe possédant un sommet S appartenant à exactement f faces que l'on suppose être des polygones réguliers à n côtés. Soit H un plan affine avec $H \cap P = \{S\}$. Considérons la projection orthogonale $p : \mathbb{R}^3 \to H$. Les n arêtes de P de sommets S, et dans l'une des f faces contenant P, sont envoyés sur des segments de H satisfaisant les hypothèses de l'exercice. On est donc dans l'un des 5 cas de couples (n, f) ci-dessus. Si P est régulier, c'est donc manifestement (?) un tétraèdre, un octaèdre, un cube, un dodécaèdre ou un icosaèdre.

Exercice 5.5. Le groupe $\mathbb{Z}/2\mathbb{Z}$ est le groupe de symétries d'un parallélogramme centré en 0 non losange, et le groupe trivial est le groupe de symétries de tout quadrilatère suffisamment quelconque. On suppose donc $n \geqslant 3$.

Soient $\mathscr{P}_n \subset E$ un polygone régulier à n côtés de centre 0, S_n l'ensemble des sommets de $\mathscr{P}_n$, S'_n une petite rotation non triviale de S_n et $r > 1$ un réel assez proche de 1. Soit P_n l'enveloppe convexe de $\Sigma_n = S_n \cup rS'_n$. C'est un polygone régulier à $2n$ côtés de sommets Σ_n. Le groupe $G \simeq \mathbb{Z}/n\mathbb{Z}$ des rotations d'angle dans $\frac{2\pi}{n}\mathbb{Z}$ préserve clairement P_n. Réciproquement, une isométrie de P_n préserve ses sommets Σ_n ainsi que S_n et rS'_n, car pour $x \in S_n$ et $y \in rS'_n$ on a $||x|| \neq ||y||$. Mais on sait que $\mathrm{Iso}(\mathscr{P}_n)$ est un groupe diédral d'ordre $2n$, constitué de G et de n réflexions orthogonales fixant soit le milieu d'une arête de $\mathscr{P}_n$, soit deux sommets opposés de $\mathscr{P}_n$. Mais par choix de S'_n, une telle réflexion ne préserve pas S_n. On a donc bien $\mathrm{Iso}(P_n) = G$.

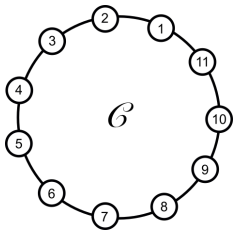
Exercice 5.6. Les éléments non triviaux de A_5 sont soit des 3-cycles, soit des 5-cycles, soit des doubles transpositions. Les sous-groupes cycliques de A_5 sont donc $\simeq \mathbb{Z}/n\mathbb{Z}$ avec $n = 1, 2, 3, 5$. Un sous-groupe fini G de A_5 se plonge dans $\mathrm{SO}(3)$. Il est donc dans la liste du théorème de Klein. S'il est réductible, il est soit cyclique, et ce cas vient d'être traité, soit diédral, soit $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si on a $G \simeq \mathrm{D}_{2m}$, avec donc $m \geqslant 3$, on a $m = 3$ ou 5 car G contient un élément d'ordre $m \geqslant 3$. Réciproquement, on constate que D_{10} est dans A_5 (et plus généralement, D_{2n} est dans A_n pour $n \equiv 0, 1 \bmod 4$). De plus, le sous-groupe

de A_5 préservant $\{1,2,3\}$ est isomorphe à $\mathrm{S}_3 \simeq \mathrm{D}_6$, et le groupe A_4 se plonge clairement dans A_5, ainsi donc au passage que son sous-groupe K_4. On peut donc supposer que G est irréductible, et isomorphe à S_4. Mais c'est impossible par Lagrange car 24 ne divise pas 60.

Exercice 5.7. (i) Le groupe G a $2m$ éléments, dont m rotations, et donc m réflexions. Si m est pair, on a $\mathscr{P}_m = -\mathscr{P}_m$, et les $m/2$ réflexions d'axe passant par deux sommets opposés sont conjuguées par la formule $gs_Hg^{-1} = s_{g(H)}$, car G agit transitivement sur les sommets. Les $m/2$ autres réflexions ont un axe reliant les milieux de deux côtés opposés. Pour la même raison, elles sont conjuguées entre elles, mais pas aux $m/2$ précédentes car aucune isométrie de $\mathscr{P}_m$ n'envoie un sommet sur le milieu d'un côté. Enfin si m est impair, il y a m droites reliant un sommet de $\mathscr{P}_m$ au milieu du côté opposé, permutées transitivement par G. Les m réflexions associées forment donc une unique classe de conjugaison de G.

(ii) Il suffit de prendre pour s la réflexion fixant un sommet S et t celle fixant le milieu d'une arête contenant S. L'angle entre les axes de ces deux réflexions est $\frac{1}{2}\frac{2\pi}{m}$, donc st est la rotation d'angle $\pm\frac{2\pi}{m}$. Comme G est d'ordre $2m$, on a bien $G = \langle s, t\rangle$.

Exercice 5.8. Supposons fixé un collier $\mathscr{C}$ possédant $2+3+6=11$ emplacements de perles numérotés circulairement de 1 à 11.



Notons X l'ensemble de tous les remplissages possibles de ces 11 emplacements avec en tout 2 perles violettes, 3 rouges et 6 bleues. On peut définir rigoureusement X comme un sous-ensemble de l'ensemble des 3^{11} fonctions $\{1,2,\ldots,11\} \to \{\text{bleu}, \text{rouge}, \text{violet}\}$. On a $|X| = \binom{11}{2}\binom{9}{3} = 4620$. Le groupe S_{11} agit naturellement sur X par précomposition à la source des fonctions. On sait que le groupe des rotations spatiales de $\mathscr{C}$ s'identifie au sous-groupe diédral D_{22} du groupe S_{11} des permutations des 11 emplacements. Il agit donc aussi naturellement sur X, et la question de l'énoncé est de déterminer le nombre N d'orbites de cette action. D'après Burnside-Frobenius, N est le nombre moyen de points fixes d'un élément de D_{22} agissant sur X. Le groupe D_{22} a trois types d'éléments :

– Le neutre 1. Il agit bien sûr sur X avec $|X|$ points fixes.

– 10 éléments d'ordre 11 (les c^i avec $0 < i < 11$). Un éléments d'ordre 11 de S_{11} est un 11-cycle. Un remplissage de $\mathscr{C}$ fixé par un 11-cycle doit donc avoir toutes ses perles de couleurs identiques, et un tel remplissage n'est pas dans X. Ainsi, les 10 éléments d'ordre 11 de D_{22} n'ont aucun point fixe dans X.

– 11 éléments d'ordre 2 possédant un unique point fixe dans $\{1,2,\ldots,11\}$ (les conjugués de τ). Fixons $s \in \mathrm{S}_{11}$ d'ordre 2 et possèdant un unique point fixe. Déterminons le nombre de remplissages de $\mathscr{C}$ dans X et invariants par s. La seule couleur présente en nombre impaire (en l'occurence, 3) étant le rouge, la perle fixée par s doit être rouge, et toutes les autres viennent par paires monochromes préservées par s. Parmi ces 5 paires, une est violette, une est rouge et les 3 autres sont bleues. Il y a donc exactement $5\cdot 4 = 20$ éléments de X fixés par s.

On a donc $N = \frac{1}{|\mathrm{D}_{22}|}(|X| + 10\cdot 0 + 11\cdot 20) = \frac{1}{22}(4620+220) = 220$ colliers possibles.

Exercice 5.9. (i) L'action de G sur X ayant une seule orbite, on a $1 = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}\, g|$ par Burnside-Frobenius. Mais $g = 1$ a $|X| \geqslant 2$ points fixes. Ainsi, si les éléments non triviaux de G ont tous au moins un point fixe on aurait $1 \geqslant \frac{1}{|G|}(2 + |G| - 1) > 1$, une contradiction.

(ii) On applique la question précédente à $X = G/H$, pour l'action (transitive) par translations. On a bien $|X| \geqslant 2$ par l'hypothèse $H \neq G$. Il existe donc $\gamma \in G$ qui ne stabilise aucun gH avec $g \in G$. Mais le stabilisateur de gH pour l'action par translations est gHg^{-1}, on a donc $\gamma \in G \smallsetminus \cup_{g\in G} gHg^{-1}$.

(iii) Si H contient un représentant de chaque classe de conjugaison de G, on a $G \subset \cup_{g\in G} gHg^{-1}$, et donc $H = G$ par la question (ii).

(iv) Le groupe infini $G = \mathrm{SO}(3)$ agit transitivement sur la sphère S^2. Par Euler, tout $g \in G$ admet deux points fixes dans S^2. Fixons $x_0 \in \mathrm{S}^2$, de stabilisateur $T := G_{x_0}$ (un sous-groupe isomorphe à S^1). Pour $g \in G$, le stabilisateur du point gx_0 est gTg^{-1}, et on a donc $G = \cup_{g\in G} gTg^{-1}$. Ainsi le sous-groupe T (commutatif !) contient un représentant de chaque classe de conjugaison de G. On a bien sûr $T \neq G$.

Exercice 5.10. Écrivons $X = \coprod_{i=1}^{r} \Omega_i$ comme réunion disjointe des orbites Ω_i sous l'action de G. Par la formule de Burnside-Frobenius et l'hypothèse (b), on a

$$r = \frac{1}{|G|}(|X| + h), \tag{82}$$

où h est le nombre d'éléments de G distincts de 1 et ayant exactement 1 point fixe dans X. On a bien sûr $h < |G|$. De plus, comme on a $|G_x| \geqslant 2$ pour tout $x \in X$ par l'hypoth ese (a), on a aussi $|\Omega_i| \leqslant |G|/2$ pour tout i par la formule orbite-stabilisateur, puis $|X| \leqslant r|G|/2$. L'égalité (82) montre donc $r < r/2 + 1$, puis $r < 2$ et $r = 1$.

Exercice 5.11. On se place dans l'espace euclidien standard $E = \mathbb{R}^n$, et on identifie $\mathrm{O}(E)$ à $\mathrm{O}(n)$ comme d'habitude (matrice dans la base canonique).

(i) Un élément g du centre de $\mathrm{O}(E)$ commute avec toutes les réflexions de E. On a donc $g\,\mathrm{s}_H\,g^{-1} = \mathrm{s}_{g(H)} = \mathrm{s}_H$, puis $g(H) = H$ (car on a $\mathrm{s}_H = \mathrm{s}_{H'} \iff H = H'$) pour tout hyperplan $H \in E$. On en déduit que g préserve toutes les droites de E (orthogonaux des hyperplans). Il est classique (et vu en cours) qu'alors g est une homothétie, puis $g = \pm\mathrm{id}_E$ car g est dans $\mathrm{O}(E)$. On en déduit $\mathrm{Z}(\mathrm{O}(n)) = \{\pm 1_n\}$.

(ii) Le morphisme det de $\mathrm{O}(E)$ vers le groupe abélien $\{\pm 1\}$ montre $\mathrm{D}(\mathrm{O}(E)) \subset \mathrm{SO}(E)$. Montrons l'inclusion réciproque. Pour $g \in \mathrm{O}(E)$ et $H \subset E$ un hyperplan on a $[g, s_H] = s_{g(H)}s_H$. Mais $\mathrm{O}(E)$ permute transitivement les hyperplans de E, car il permute transitivement les vecteurs de norme 1. On en déduit que le produit de deux réflexions est dans $\mathrm{D}(\mathrm{O}(E))$. Comme les produits de deux réflexions engendrent $\mathrm{SO}(E)$ par Cartan-Dieudonné, on a montré $\mathrm{SO}(E) = \mathrm{D}(\mathrm{O}(E))$.

(iii) Considérons l'application $f : \mathrm{O}(E) \to \mathrm{O}(E) \times \{\pm 1\}, g \mapsto ((\det g)g, \det g)$. On constate que c'est un morphisme de groupes injectif et d'image contenant $\mathrm{SO}(E) \times \{1\}$. Si n est impair on a $\det -\mathrm{id}_E = -1$ et donc f induit un isomorphisme $\mathrm{O}(E) \xrightarrow{\sim} \mathrm{SO}(E) \times \{\pm 1\}$. Si n est pair, on n'a pas $\mathrm{O}(n) \simeq \mathrm{SO}(n) \times \{\pm 1\}$, car le centre de $\mathrm{SO}(n) \times \{\pm 1\}$ contient les 4 éléments $(\pm 1_n, \pm 1)$, et celui de $\mathrm{O}(n)$ est d'ordre 2 par le (i).

Exercice 5.12. On pose $E = \mathbb{R}^n$ et on identifie encore $\mathrm{O}(E)$ à $\mathrm{O}(n)$ comme dans l'exercice précédent.

(i) Pour tout plan P de E il existe un unique élément $r_P \in \mathrm{O}(E)$. qui vaut l'identité sur P et $-\mathrm{id}$ sur $P^\perp$. C'est l'unique retournement fixant $P^\perp$. On a $r_P \in \mathrm{SO}(E)$, et pour $g \in \mathrm{O}(E)$ on a $gr_Pg^{-1} = r_{g(P)}$. On notera $R(E) \subset \mathrm{SO}(E)$ le sous-ensemble des retournements de E, *i.e.* des r_P avec P un plan de E. Pour voir $\langle R(E)\rangle = \mathrm{SO}(E)$, il suffit de voir que le

groupe de gauche contient les produits de deux réflexions par Cartan-Dieudonné. Soient s_1 et s_2 deux réflexions de E d'hyperplans H_1 et H_2. Supposons d'abord $\dim E = 3$. Pour tout plan P de E on a alors $-r_P = \mathrm{s}_P$ (une réflexion). On a donc $s_1 s_2 = (-s_1)(-s_2) \in \langle R(E)\rangle$. Retournons au cas général $\dim E \geqslant 3$. Le cas $\dim E = 3$ appliqué à tous les sous-espaces de dimension 3 de E montre que $\langle R(E)\rangle$ contient tous les éléments $g \in \mathrm{SO}(E)$ dont les points fixes sont de codimension $\leqslant 3$. On conclut car $s_1 s_2$ fixe $H_1 \cap H_2$ qui est de codimension $\leqslant 2$.

(ii) Pour $n \leqslant 2$ alors $\mathrm{SO}(E)$ est commutatif. On a donc $\mathrm{Z}(\mathrm{SO}(E)) = \mathrm{SO}(E)$ et $\mathrm{D}(\mathrm{SO}(E)) = \{1\}$. On suppose donc $n \geqslant 3$. Un élément $g \in \mathrm{Z}(\mathrm{SO}(E))$ commute à tous les r_P, et donc stabilise tous les plans P de E. Comme on a $\dim E > 2$, toute droite de E est intersection de deux plans. Ainsi, g préserve toutes les droites, puis g est une homothétie, $g = \pm \mathrm{id}_E$, puis $g = \mathrm{id}_E$ si n est impair. On a donc $\mathrm{Z}(\mathrm{SO}(E)) = 1$ pour n impair, $\mathrm{Z}(\mathrm{SO}(E)) = \{\pm \mathrm{id}_E\}$ pour n pair.

Montrons enfin $\mathrm{D}(\mathrm{SO}(E)) = \mathrm{SO}(E)$. Le même argument qu'au (i) montre que l'on peut supposer $n = \dim E = 3$. Mais pour $g \in \mathrm{SO}(E)$ et $r_P \in R(E)$ on a $[g, r_P] = r_{g(P)} r_P = (-r_{g(P)})(-r_P) = s_{g(P)} s_P \in \mathrm{D}(\mathrm{SO}(E))$. Comme $\mathrm{SO}(E)$ agit transitivement sur les plans de E, on en déduit que $\mathrm{D}(\mathrm{SO}(E))$ contient tous les produits de deux réflexions, puis $\mathrm{SO}(E)$.

Exercice 5.13. Soit G un sous-groupe de $\mathrm{SO}(2)$ et $h \in \mathrm{O}(2)$. Si h est dans $\mathrm{SO}(2)$ on a $hGh^{-1} = G$ car $\mathrm{SO}(2)$ est commutatif. Si non, h est une réflexion et on a $hrh^{-1} = r^{-1}$ pour tout $r \in \mathrm{SO}(2)$. On a donc encore $hGh^{-1} = G^{-1} = G$. On a montré que tout sous-groupe de $\mathrm{SO}(2)$ est distingué dans $\mathrm{O}(2)$.

Il reste à voir que si un sous-groupe $G \subset \mathrm{O}(2)$ est distingué et contient une réflexion s, alors on a $G = \mathrm{O}(2)$. Mais alors G contient les rsr^{-1} avec $r \in \mathrm{SO}(2)$, et donc toutes les réflexions, puis toutes les rotations (produits de deux réflexions).

Exercice 5.14. (i) La matrice d'une rotation plane d'angle θ est

$$\mathrm{R}_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

dans une base orthonormée, de sorte que sa trace est $2\cos\theta$. Par Euler, toute rotation g de $\mathrm{SO}(3)$ fixe une droite, et donc induit une rotation d'un certain angle θ dans le plan orthogonal. Ainsi, g est conjuguée à

$$\mathrm{m}(\theta) := \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{R}_\theta \end{bmatrix}.$$

dans $\mathrm{O}(3)$, et même dans $\mathrm{SO}(3)$ car $\det -1_3 = -1$, et sa trace est $1 + 2\cos\theta$.

(ii) La trace est invariante par conjugaison. Réciproquement, on a $\mathrm{tr}\,\mathrm{m}(\theta) = \mathrm{tr}\,\mathrm{m}(\theta')$ si, et seulement si, $\theta \equiv \pm\theta' \bmod 2\mathbb{Z}$. On conclut car $\mathrm{m}(\theta)$ est conjuguée à $\mathrm{m}(-\theta)$ dans $\mathrm{SO}(3)$ (conjuguer par la matrice diagonale $\mathrm{diag}(-1,-1,1)$).

(iii) On a $\mathrm{tr}\,\mathrm{m}(\theta) = 3$ si et seulement si $\theta \in 2\pi\mathbb{Z}$, *i.e.* $\mathrm{m}(\theta) = 1_3$. On peut aussi utiliser le (ii).

(iv) Comme H est distingué dans G, on sait par le (ii) et l'hypothèse que H contient tous les $\mathrm{m}(\theta)$ avec $|\theta| < \epsilon$ pour un certain $\epsilon > 0$ (par exemple vérifiant $1 + 2\cos\epsilon > x$), et il faut voir par le (ii) encore qu'il contient tous les $\mathrm{m}(\theta)$ avec $\theta \in \mathbb{R}$. Pour tout entier $n \geqslant 1$ et $|\theta| < \epsilon$, le sous-groupe H contient $\mathrm{m}(\theta)^n = \mathrm{m}(n\theta)$, et on conclut car on a $\cup_{n\geqslant 1}]-n\epsilon, n\epsilon[= \mathbb{R}$.

(iv) Fixons $h \in H \smallsetminus \{1\}$. Pour tout $g \in \mathrm{SO}(3)$, on a $[g,h] = (ghg^{-1})h^{-1} \in H$ car H est distingué. Considérons l'application $f : \mathrm{SO}(3) \to [-1,3], g \mapsto \mathrm{tr}[g,h]$, est continue. Comme $\mathrm{SO}(3)$ est connexe son image est un connexe de $[-1,3]$, donc un intervalle. Elle contient $f(1) = 3$. Mieux, $[g,h]$ est de trace 3 si, et seulement si, on a $[g,h] = 1$ par le

(iii), *i.e.* si g commute avec h. Comme le centre de SO(3) est 1, h est $\neq 1$ par hypothèse, on a $]x,3] \subset \mathrm{Im} f$ pour un certain $x < 3$. On a montré $\mathrm{tr}\, H \supset]x,3]$, et on conclut par le (iii).

Exercice 5.15. (i) Montrons que les seuls sous-groupes distingués de Sp(1) sont 1, $\{\pm 1\}$ et Sp(1) (ces sous-groupes le sont clairement). On sait qu'il existe un morphisme $\pi : \mathrm{Sp}(1) \to \mathrm{SO}(3)$ qui est surjectif de noyau $\{\pm 1\}$. Si G est un sous-groupe distingué de Sp(1), alors $\pi(G)$ est distingué dans SO(3). C'est donc $\{1\}$ ou SO(3) par l'Exercice 5.14. Mais $\pi(G) = \{1\}$ entraîne bien $G \subset \{\pm 1\}$. Sinon il existe $q \in G$ tel que $\pi(q)$ est d'ordre 2 dans SO(3). On a donc $q^2 = \pm 1$. Mais $q^2 = 1$ implique $q = \pm 1$ dans le corps gauche $\mathbb{H}$, et donc $\pi(q) = 1$. On a donc $q^2 = -1$, et donc $-1 \in G$, puis $G = \mathrm{Sp}(1)$ car $\pi(G) = \mathrm{SO}(3)$.

(ii) Posons $\Gamma = \mathrm{Sp}(1) \times \mathrm{Sp}(1)$. Ce groupe a deux sous-groupes distingués naturels $\simeq \mathrm{Sp}(1)$ qui sont $\Gamma_1 = \mathrm{Sp}(1) \times \{1\}$ et $\Gamma_2 = \{1\} \times \mathrm{Sp}(1)$. On sait qu'il existe un morphisme $\pi : \Gamma \to \mathrm{SO}(4)$ surjectif et de noyau $\{(1,1),(-1,-1)\}$. Nous allons voir que les sous-groupes distingués de SO(4) sont $1, \{\pm 1\}, \pi(\Gamma_1), \pi(\Gamma_2)$ et SO(4). Mais les sous-groupes distingués de SO(4) sont exactement les $\pi(G)$ avec G un sous-groupe distingué de Γ contenant $(-1,-1)$. Soit G un tel sous-groupe. Il suffit donc de voir que l'on a soit $G \subset Z$ (et donc $\pi(G) \subset \pi(Z) = \{\pm 1\}$), soit $G = Z\Gamma_i$ (et donc $\pi(G) = \pi(\Gamma_i)$ car $\pi(Z) \subset \pi(\Gamma_i)$), soit $G = \Gamma$ (et donc $\pi(G) = \mathrm{SO}(4)$). Mais $G_i := G \cap \Gamma_i$ est distingué dans Γ_i. Par le (i) on a donc $G_i \subset \{\pm 1\}$ ou $G_i = \Gamma_i$. Supposons $G_1 = \Gamma_1$, le cas $G_2 = \Gamma_2$ est similaire. La relation $\Gamma = \Gamma_1\Gamma_2$ entraîne alors $G = \Gamma_1 G_2$, puis soit $G = \Gamma_1 Z$ car $(-1,-1) \in G$ (cas $G_2 \subset \{\pm 1\}$) soit $G = \Gamma$ (cas $G_2 = \Gamma_2$). Dans le cas restant, on a G_1 et G_2 inclus dans $\{\pm 1\}$ et donc $G \subset Z$.

Exercice 5.16. Cet exercice est à comparer à la preuve du cours montrant la simplicité de A_n à partir de celle de A_5.

(i) On pose $E = \mathbb{R}^{2n+1}$ et on identifie $\mathrm{SO}(2n+1)$ à $\mathrm{SO}(E)$ comme d'habitude. Soit G un sous-groupe distingué non trivial de $\mathrm{SO}(E)$. On va montrer $G = \mathrm{SO}(E)$. Par l'Exercice 5.12, il suffit de voir que G contient un retournement. Soit F un sous-espace de E de dimension k. On a $\mathrm{S}(F) \simeq \mathrm{SO}(k)$ et $G \cap \mathrm{S}(F)$ est distingué dans $\mathrm{S}(F)$. Comme SO(3) est simple, il suffit de trouver F de dimension 3 tel que $G \cap \mathrm{S}(F)$ est non trivial. Cela impliquera $G \cap \mathrm{S}(F) = \mathrm{S}(F)$, et donc que G contient un retournement.

Soit $g \in G \smallsetminus \{1\}$ (et donc aussi $g \neq -1$ car $-1 \notin \mathrm{SO}(2n+1)$). Alors on a g n'est pas dans le centre de $\mathrm{O}(E)$ par l'Exercice 5.11. Ainsi, il existe une doite $D \subset E$ avec $s(D) \neq D$. Posant $H = D^\perp$, on a donc $g\mathrm{s}_H \neq \mathrm{s}_H g$. Le commutateur $[g, \mathrm{s}_H] = [g, -\mathrm{s}_H]$ est donc non trivial. Mais comme $\dim E$ est impaire, on a $-\mathrm{s}_H \in \mathrm{SO}(E)$, et comme G est distingué dans $\mathrm{SO}(E)$, on a donc $[g, \mathrm{s}_H] \in G$. Mais on a aussi $[g, \mathrm{s}_H] = g\mathrm{s}_H g^{-1}\mathrm{s}_H = \mathrm{s}_{g(H)}\mathrm{s}_H$. C'est un élément non trivial de $\mathrm{S}(F)$ pour $F = g(D) + D$, qui est de dimension 2. Il est donc aussi dans $\mathrm{S}(F)$ pour tout sous-espace F contenant $g(D) + D$. Il suffit donc de considérer un tel F de dimension 3.

(ii) On suppose maintenant $E = \mathbb{R}^{2n+2}$ avec $n > 1$, et G distingué dans $\mathrm{SO}(E)$ non trivial. Soit g dans G différent de ± 1. Il existe donc un plan P de E avec $[g, r_P] \neq 1$ par l'Exercice 5.12. Mais on a d'une part $[g, r_P] = g(r_P g^{-1} r_P^{-1}) \in G$ car G est distingué, et aussi $[g, r_P] = r_{g(P)} r_P \in \mathrm{S}(F)$ avec $F = P + g(P^\perp)$, qui est de dimension $\geqslant 4$. Considérant un sous-espace F' de dimension 5 arbitraire contenant F, on a alors $[g, r_P] \in G \cap \mathrm{S}(F')$ et donc $G \cap \mathrm{S}(F') \neq \{1\}$. Mais on a $\mathrm{S}(F') \simeq \mathrm{SO}(5)$ et $G \cap \mathrm{S}(F')$ distingué non trivial dans $\mathrm{S}(F')$, donc $G \cap \mathrm{S}(F') = \mathrm{S}(F')$. En particulier, G contient des retournements, et donc $G = \mathrm{SO}(E)$ par l'Exercice 5.12 (i).

Exercice 5.18. (i) Si B est un bloc, alors B est non vide, ainsi donc que les $g(B)$. Si on a $g(B) \cap g'(B) \neq \varnothing$ pour $g, g' \in G$ alors $g^{-1}g'(B) \cap B$ est non vide. On a donc $g^{-1}g'(B) = B$ car B est un bloc, puis $g(B) = g'(B)$. Comme l'action de G sur X est transitive, on a

aussi $X = \cup_{g\in G} g(B)$. On a bien montré que les $g(B)$, avec $g \in G$, forment une partition de X. La réciproque est triviale.

(ii) Soit B un bloc et $b \in B$. Pour $g \in G_b$ on a $g(b) = b$ et donc $b \in g(B) \cap B$, puis $g(B) = B$ car B est un bloc.

(iii) Observer que si l'action de G sur X est libre, on a $G_x = \{1\}$ pour tout $x \in X$. Ainsi, tous les sous-ensembles non vide $B \subset X$ sont trivialement équilibrés. Considérons $X = G$ pour l'action de Cayley pour fixer les idées. Notons B un bloc contenant 1, fixons $g, h \in B$. On a $g^{-1}.g = 1 \in B \cap g^{-1}(B)$ donc $g^{-1}(B) = B$ puis $g^{-1}.1 = g^{-1} \in B$. On a aussi $hg.g^{-1} = h \in B \cap hg(B)$ donc $B = hg(B)$ puis $gh.1 = hg \in B$. Ainsi, B est un sous-groupe de G. On obtient donc un contre-exemple en choisisant pour B une partie de G contenant 1 mais qui n'est pas un sous-groupe. C'est possible dès que $|G| > 2$.

(iv) Soient N un sous-groupe distingué de G, $x \in G$ et $B = Nx$ l'orbite de x sous N. Soit $g \in G$. On constate $gNx = gNg^{-1}gx = Ngx$ car N est distingué dans G, et Ngx est l'orbite de $gx \in X$ sous N. On conclut car on sait que les orbites de X sous l'action de N forment une partition de X.

Exercice 5.19. (i) Supposons $n = 3$ pour commencer. Soit $B \subset \mathrm{S}^2$ une partie équilibée possédant deux éléments x, y avec $y \notin \{x, -x\}$. Si $r_\theta \in \mathrm{SO}(3)$ est désigne rotation d'axe y et d'angle $\pm\theta$, on a $r_\theta(x) \in B$ par hypothèse. Nous en déduisons deux choses.

(a) il existe des éléments de $B \smallsetminus \{x\}$ aussi proches que l'on veut de x (prendre des θ très petits).

(b) le cercle de S^2 passant par y et orthogonal à x est inclus dans B.

Ceci étant dit, notons $\mathscr{C}_z$ le grand cercle (ou *équateur*) de S^2 orthogonal à $z \in \mathrm{S}^2$. Ainsi, si on a $B \cap \mathscr{C}_x \neq \varnothing$, on en déduit $\mathscr{C}_x \subset B$ par (b), puis $\mathscr{C}_z \subset B$ pour tout $z \in \mathscr{C}_x$ encore par (b) car $\mathscr{C}_x \cap \mathscr{C}_z$ est non vide, et on conclut car on a alors

$$\mathrm{S}^2 = \cup_{z\in\mathscr{C}_x} \mathscr{C}_z \subset B.$$

Posons $x_0 = x$. Il suffit donc de montrer $B \cap \mathscr{C}_{x_0} \neq \varnothing$. Par (a), il existe $x_1 \in B \smallsetminus \{x_0\}$ assez proche de x_0 de sorte que la longueur ℓ de l'arc (x_0x_1) soit $< \pi/2$ (cette condition sera suffisante mais il sera plus clair d'imaginer ℓ très petite). Soit $\mathscr{C} \subset \mathrm{S}^2$ le grand cercle passant par x_0 et x_1. Le cercle de S^2 de centre x_1 et passant par x_0 est inclus dans B par (b), et il coupe $\mathscr{C}$ en deux points x_0, x_2. On construit ainsi de proche en proche une suite de points $x_0, x_1, x_2, \ldots, x_n$ de $B \cap \mathscr{C}$, avec $(x_0x_n) \subset \mathscr{C}$ de longueur $n\ell$ et (x_ix_{i+1}) de longueur ℓ. Soit $n > 0$ le plus petit entier tel que la longueur de $(x\, x_{n+1})$ est $\geqslant \pi/2$. Alors $(x_nx_{n+1}) \cap \mathscr{C}_x$ est non vide. On peut supposer $x_n, x_{n+1} \notin \mathscr{C}_x$ (sinon on a gagné). Mais alors le cercle de centre x_n et de rayon ℓ rencontre $\mathscr{C}_x$ car $\ell < \pi/2$, puis $B \cap \mathscr{C}_x \neq \varnothing$ par (b).

(ii) Pour $n \geqslant 1$ on note $C_n \subset \mathrm{SO}(2)$ le sous-groupe cyclique d'ordre n. C'est un sous-groupe distingué de $\mathrm{SO}(2)$ car ce dernier est abélien. Ses orbites dans S^1 sont donc des blocs pour l'action de $\mathrm{SO}(2)$ sur S^1 par l'Exercice 5.18 (iv). Une telle orbite a n éléments (sommets d'un polygone régulier du plan à n côtés).

Exercice 5.20. (i) D'après l'Exercice 5.18 (iv), les orbites de S^2 sous H sont des blocs pour l'action de $\mathrm{SO}(3)$. Par ce même exercice assertion (ii), ce sont des parties équilibrées. Par l'Exercice 5.19, chaque orbite de S^2 sous H est donc soit de la forme $\{x\}$, soit de la forme $\{x, -x\}$, soit S^2. Dans ce dernier cas on conclut, et sinon pour tout $h \in H$ on a $h(x) = \pm x$ pour tout $x \in \mathrm{S}^2$. On sait qu'un tel h est une homothétie, puis $h = \pm\mathrm{id}$, et donc $h = 1$ car $\det -1_3 = -1$. C'est une contradiction car H est non trivial.

(ii) Soit s_P la réflexion orthogonal d'hyperplan $P \subset \mathbb{R}^3$. On a $-\mathrm{s}_P \in \mathrm{SO}(3)$, puis

$$[h, -\mathrm{s}_P] = g\mathrm{s}_P g^{-1}\mathrm{s}_P = \mathrm{s}_{h(P)}\mathrm{s}_P$$

pour tout $h \in H$. Comme H est distingué dans $\mathrm{SO}(3)$ on a $[h, -\mathrm{s}_P] \in H$ pour tout plan P et $h \in H$. Mais H agit transitivement sur S^2 par le (i), donc sur les plans de $\mathbb{R}^3$ (considérer un vecteur orthogonal). La formule ci-dessus montre que H contient tous les produits de deux réflexions. On a donc $H = \mathrm{SO}(3)$ par Cartan-Dieudonné.

Exercice 5.28. On voit $\mathbb{H}$ comme espace euclidien muni de n. On a vu en cours $q \in \mathscr{I} \iff q \in \mathbb{H}^0$ et $\mathrm{n}(q) = 1$. (i) Soient q et q' deux éléments de $\mathscr{I}$, *i.e.* de la sphère unité de $\mathbb{H}^0$, il existe $u \in \mathrm{SO}(\mathbb{H}^0)$ avec $u(q) = q'$. D'après le cours, u est de la forme $h \mapsto xhx^{-1}$ pour un certain $x \in \mathrm{Sp}(1)$. On a donc $q' = xqx^{-1}$, comme demandé. (Voir l'exercice suivant pour une généralisation de cet argument).

(ii) Comme indiqué, $\mathbb{C}_q$ est un sous-corps de $\mathbb{H}$ de dimension 2 sur $\mathbb{R}$ (isomorphe à $\mathbb{C}$!). (En particulier, il est commutatif). On peut donc voir $\mathbb{H}$ comme $\mathbb{C}_q$-espace vectoriel. On constate que si $a, b \in \mathbb{H}$ est $\mathbb{C}_q$-libre, alors a, qa, b, qb est $\mathbb{R}$-libre, donc $\mathbb{H}$ est un $\mathbb{C}_q$-espace vectoriel de dimension 2. Écrivons $\mathbb{H} = \mathbb{C}_q + \mathbb{C}_q h$ pour un certain $h \in \mathbb{H}$, en complément la famille libre $\{1\}$. Si $A \subset \mathbb{H}$ contient strictement $\mathbb{C}_q$, il va contenir qh pour un certain $q \in \mathbb{C}_q$ non nul, donc inversible, puis $h \in A$ et $\mathbb{C}_q + \mathbb{C}_q = \mathbb{H} \subset A$.

(iii) On a $q^2 - aq + b = 0$ avec $a, b \in \mathbb{R}$ par Cayley-Hamilton. On a donc $(q - a/2)^2 = -b + a^2/4$. Si $-b + a^2/4$ est $\geqslant 0$, on a $(q - a/2)^2 = u^2$ avec $u \in \mathbb{R}$, puis $(q - a/2 - u)(q - a/2 + u) = 0$ dans $\mathbb{H}$ et donc $q = a/2 \pm u \in \mathbb{R}$, en contradiction avec l'énoncé. On a donc $(q - a/2)^2 = -u^2$ avec $u \in \mathbb{R}^\times$, et donc $q' = \frac{1}{u}(q - a/2) \in \mathbb{C}_q$ vérifiant $q'^2 = -1$, puis évidemment $\mathbb{C}_{q'} = \mathbb{R} + \mathbb{R}q' = \mathbb{R} + \mathbb{R}q$.

(v) Si A est une sous-algèbre de $\mathbb{H}$, on a $\mathbb{R} \subset A$ par définition. Si $\mathbb{R} \subsetneq A$, il existe $q \in \mathscr{I}$ avec $\mathbb{C}_q \subset A$ par le (iii). Par le (ii) on a soit $A = \mathbb{H}$, soit $A = \mathbb{C}_q$. Les $\mathbb{C}_q$ sont conjuguées par le (i).

Exercice 5.29. D'abord, on a $\mathrm{t}(xqx^{-1}) = \mathrm{t}(x^{-1}xq) = \mathrm{t}(q)$ car on a $\mathrm{trace}AB = \mathrm{trace}\, BA$ pour A, B dans $\mathrm{M}_2(\mathbb{C})$. Réciproquement, supposons $q, q' \in \mathrm{Sp}(1)$ et $\mathrm{t}(q) = \mathrm{t}(q')$. Dans l'espace euclidien $(\mathbb{H}, \mathrm{n})$, de produit scalaire $x.y = \mathrm{tr}(x^*y)$, on a donc $1.q = 1.q'$. Ainsi, il existe $u \in \mathrm{O}(\mathbb{H})$ vérifiant $u(1) = 1$ et $u(q) = q'$. Quitte à modifier u par un élément de $\mathrm{O}(\mathbb{H})$ fixant 1, q et de déterminant -1, on peut supposer $u \in \mathrm{SO}(\mathbb{H})$). Mais alors on a$u(x) = axb^{-1}$ pour certains $a, b \in \mathrm{Sp}(1)$ par le cours, puis $u(1) = ab^{-1} = 1$ donc $a = b$, et donc $u(q) = aqa^{-1} = q'$.

Exercice 5.30. Pour $1 \leqslant k \leqslant m/2$, on considère le polynôme suivant dans $\mathbb{R}[X]$

$$P_{k/m}(X) = (X - e^{2ik\pi/m})(X - e^{-2ik\pi/m}) = X^2 - 2\cos(2k\pi/m)X + 1.$$

Le polynôme $X^m - 1$ est produit de $X - 1$ et des $P_{k/m}$ dans $\mathbb{R}[X]$, avec $1 \leqslant k < m/2$, ainsi que de $X + 1$ si m est pair. Ainsi, pour $q \neq \pm 1$, on a $q^m = 1$ si, et seulement si, il existe $0 < k/m < 1/2$ avec $P_{k/m}(q) = 0$, car $\mathbb{H}$ est un corps gauche.

Soit $q \in \mathrm{Sp}(1)$, de polynôme caractéristique $\chi_q = X^2 - \mathrm{t}(q)\, X + 1$. Sous l'hypothèse de l'énoncé, on a $\chi_q = P_{k/m}$, et donc le théorème de Cayley-Hamilton montre $P_{k/m}(q) = 0$, et q est d'ordre m. Réciproquement, si on a $P_{k/m}(q) = 0$ le polynôme minimal de q dans $\mathbb{R}[X]$ divise $P_{k/m}$, et est donc égal à $P_{k/m}$ car ce dernier est irréductible. Mais il divise aussi χ_q par Cayley-Hamilton, et on a donc $\chi_q = P_{k/m}$. (Une démonstration alternative aurait été d'utiliser l'exercice précédent).

Exercice 5.35. Il est évident que G_B est un sous-groupe de G.

(i) Si B est un bloc, on a vu que B est équilibré à l'Exercice 5.18, ce qui signifie $G_x \subset G_B$ pour tout $x \in B$. Soient $b, b' \in B$. Par transitivité de l'action de G sur X, il existe $g \in G$ avec $gb = b'$. Mais alors $gB \cap B$ est non vide, et donc $g(B) = B$ car B est un bloc, puis $g \in G_B$. On a montré que G_B agit transitivement sur B.

(ii) Montrons que $B = Hx$ est un bloc pour l'action de G sur X. Si on a $ghx = h'x$ pour $g \in G$ et $h, h' \in H$, alors constate que l'on a $(h')^{-1}gh \in G_x$, puis $g \in h'G_xh^{-1} \in H$ car G_x est inclus dans H. On en déduit $gB = gHx = Hx = B$: on a montré que B est un bloc. L'inclusion $H \subset G_B$ est évidente, et l'analyse juste faite montre $G_B \subset H$.

(iii) Notons $\mathscr{B}_x$ l'ensemble des blocs de X contenant x et $\mathscr{G}_x$ l'ensemble des sous-groupes de G contenant G_x. D'après le (ii), on a une application bien définie $\beta : \mathscr{G}_x \to \mathscr{B}_x,\ H \mapsto Hx$. D'après le (i), on a une application bien définie $\gamma : \mathscr{B}_x \mapsto \mathscr{G}_x, B \mapsto G_B$. Ces applications sont manifestement croissantes pour l'inclusion. Pour $H \in \mathscr{G}_x$ on a $\gamma \circ \beta(H) = G_{Hx} = H$, par le (ii). On a aussi $\beta \circ \gamma(B) = G_Bx = B$ car G_B agit transitivement sur B par le (i). Ainsi, β et γ sont inverses l'une de l'autre.

Exercice 5.36. (i) Soit B un bloc et $b \in B$. On a vu $G_b \subset G_B$. Mais G_b agit transitivement sur $X \setminus \{b\}$ par l'hypothèse de 2-transitivité. Ainsi, on a soit $B = \{b\}$, soit $B = X$: l'action est primitive.

(ii) Comme N agit non trivialement, il existe $x \in X$ avec $|Nx| > 1$. Mais Nx est un bloc par la question (iv) de l'Exercice 5.18. On a donc $Nx = X$ par primitivité, et donc N agit transitivement sur X.

(iii) C'est verbatim la démonstration du cours à ceci près qu'on utilise le (ii) au lieu de la 2-transitivité pour assurer que si N agit non trivialement sur X alors il agit transitivement.

(iv) Supposons que G agit transitivement sur X et fixons $x \in X$. D'après la dernière question de l'Exercice 5.35, G_x est un sous-groupe maximal si et seulement si les deux seuls blocs de X contenant x sont $\{x\}$ (cas $H = G_x$) et X (cas $H = G$). Si l'action est primitive, on en déduit donc que G_x est maximal. Réciproquement supposons G_x maximal. Soit B un bloc de X. Alors les $g(B)$ avec $g \in G$ sont clairement aussi des blocs de X. Comme l'action est transitive l'un deux contient x. On a donc $g(B) = \{x\}$ ou $g(B) = X$. Dans le second cas on a $B = X$, et dans le premier on a $B = \{g^{-1}x\}$: l'action est primitive.

(v) Soient $x \in X$, $Y = X \setminus \{x\}$ et $g \in G \setminus G_x$. On a $g(x) \neq x$, et donc $g(x) \in Y$. On sait que G agit 2-transitivement sur X, si et seulement si G_x agit transitivement sur Y (Exercice 4.23 (i)). Supposons que G_x agit transitivement sur Y. Pour $h \in G \setminus G_x$, l'élément $h(x) \in Y$ est de la forme $kg(x)$ pour un certain $k \in G_x$. On a donc $g^{-1}k^{-1}h(x) = x$ puis $g^{-1}k^{-1}h \in G_x$ et donc $h \in G_xgG_x$. On a montré $G = G_x \cup G_xgG_x$. Supposons réciproquement $G = G_x \cup G_xgG_x$. Comme G agit transitivement sur X, on a

$$X = Gx = G_x\, x \cup G_x\, g\, G_x\, x = \{x\} \cup G_x\, g(x).$$

Noter qu'un élément de la forme $hg(x)$ avec $h \in G_x$ ne peut être égal à x, sinon on aurait $g(x) = h^{-1}(x) = x$, absurde. On en déduit $Y = G_xg(x)$, et donc que G_x agit transitivement sur Y.

Exercice 5.37. On rappelle $n \geqslant 3$.

(i) Notons $\mathscr{C}_n$ l'ensemble des couples (I, J) constitués de deux parties $I, J \subset \{1, \ldots, n\}$ avec $|I| = |J| = 2$ et $I \neq J$. Le groupe S_n agit sur $\mathscr{C}_n$ via $(\sigma, (I, J)) \mapsto (\sigma(I), \sigma(J))$. Dire que S_n agit 2-transitivement sur X_n est équivalent à dire qu'il agit transitivement sur $\mathscr{C}_n$. Mais il y a deux "types" d'éléments de $\mathscr{C}_n$: les couples (I, J) avec $I \cap J = \varnothing$ et ceux avec $|I \cap J| = 1$. Le premier type n'existe que pour $n \geqslant 4$ car on doit avoir $4 = |I| + |J| \leqslant n$, et le second existe pour tout $n \geqslant 3$. Si (I, J) et d'un type, et pour $\sigma \in \mathrm{S}_n$, alors $(\sigma(I), \sigma(J))$ est clairement du même type. Ainsi, pour que S_n agisse 2-transitivement sur X_n il faut que l'on ait $n = 3$. Pour $n = 3$, X_3 est en bijection avec $\{1, 2, 3\}$ par passage au complémentaire, et l'action de S_3 sur X_3 est équivalente à celle sur $\{1, 2, 3\}$, qui est 3-transitive comme on le sait.

(ii) Pour $n = 4$, observons que les parties à deux éléments de X_4 de la forme $\{I, I^c\}$, avec I^c le complémentaire de I dans $\{1, 2, 3, 4\}$, sont des blocs non triviaux. En effet, ces parties sont deux à deux disjointes dans X_4, et permutées par S_4. Ainsi, l'action n'est pas primitive pour $n = 4$. Elle est 2-transitive donc primitive pour $n = 3$.

Supposons $n > 4$. Soit $B \subset X_4$ une partie équilibrée de cardinal > 1. Pour $\{i, j\} \in B$, alors B est stable par le stabilisateur de $\{i, j\}$ dans S_n, qui est un groupe $\simeq \mathrm{S}_2 \times \mathrm{S}_{n-2}$ agissant à la fois transitivement sur $\{i, j\}$ et $n-2$ transitivement sur son complémentaire (et ce indépendamment). Ainsi, si B contient un élément I avec $|I| = 2$ et $I \cap \{i, j\} = \varnothing$ (resp. $|I \cap \{i, j\}| = 1$), il contient toutes les telles parties. Mais pour $n \geqslant 5$, le complémentaire d'une partie à 2 éléments de $\{1, \ldots, n\}$ contient deux parties à deux éléments distinctes et d'intersection non triviale. Ainsi, B contient toujours deux parties à 2 éléments de $\{1, \ldots, n\}$ qui sont distinctes d'intersection non triviale, disons $\{1, 2\}$ et $\{2, 3\}$ quitte à renuméroter. Il contient ensuite $\{1, 3\}$, les $\{1, i\}$ avec $i > 1$, les $\{2, i\}$ avec $i > 2$, puis tous les $\{i, j\}$ avec $i \neq j$. On a montré $B = X_n$: l'action est primitive.

(iii) On suppose $n > 4$. On a vu que S_n agit primitivement sur X_n. Le stabilisateur dans S_n de l'élément $\{1, 2\} \in X_n$ est $\mathrm{S}_2 \times \mathrm{S}_{n-2}$. Il contient $A := \mathrm{S}_2 \times 1$ comme sous-groupe abélien distingué, engendré par la transposition $(1\,2)$, et on sait que les conjugués de $(1\,2)$ dans S_n engendent S_n. D'après le critère d'Iwasawa (version du (iii) de l'Exercice 5.36), un sous-groupe distingué de S_n contient soit $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$ (ce point était facile dans le cours), soit est inclus dans le noyau de l'action de S_n sur X_n. Mais cette action est fidèle, car un $\sigma \in \mathrm{S}_n$ stabilisant $\{i, j\}$ et $\{i, k\}$ pour tous i, j, k distincts fixe tout $i \in \{1, \ldots, n\}$.

Exercice 5.43. (i) On a $|\mathrm{A}_8| = 8!/2$. D'autre part, si k est un corps à q éléments on a $|\mathrm{SL}_3(k)| = q^3(q^3 - 1)(q^2 - 1)$ et $|\mu_3(k)| = (3, q - 1)$. Pour $q = 4$ on a donc

$$|\mathrm{PSL}_3(\mathbb{F}_4)| = \frac{1}{3} \cdot 4^3 \cdot (4^3 - 1) \cdot (4^2 - 1) = 4^4 \cdot 7 \cdot 9 \cdot 5 = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = \frac{8!}{2}.$$

(ii) Soit $g \in \mathrm{SL}_3(\mathbb{F}_4)$ avec $g^2 = 1$. On a $(g-1)^2 = 0$ dans $\mathrm{M}_3(\mathbb{F}_4)$ car on a $2g = 0$. On en déduit $\{0\} \subsetneq \mathrm{Im}(g-1) \subset \ker g - 1$, puis par le théorème du rang que l'on a $\dim \ker(g-1) = 2$. Ainsi g est une transvection. Mais toutes les transvections sont conjuguées dans $\mathrm{SL}_3(k)$. Il ne reste qu'à vérifier sur une seule transvection qu'elle est d'ordre 2 pour en déduire que les éléments d'ordre 2 de $\mathrm{SL}_3(\mathbb{F}_4)$ forment une unique classe de conjugaison. On conclut car on a par exemple $(1_3 + \mathrm{E}_{2,3})^2 = 1_3 + 2\mathrm{E}_{2,3} = 1_3$ dans $\mathrm{M}_3(\mathbb{F}_4)$ car on a $2x = 0$ pour tout $x \in \mathbb{F}_4$.

(iii) Posons $f : \mathrm{SL}_3(\mathbb{F}_4) \to \mathrm{PSL}_3(\mathbb{F}_4)$ la projection canonique. On a $\ker f = \mu_3(\mathbb{F}_4) = \mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Notons A (resp. B) l'ensemble des éléments d'ordre 2 de $\mathrm{SL}_3(\mathbb{F}_4)$ (resp. $\mathrm{PSL}_3(\mathbb{F}_4)$). Aucun élément de $\ker f$ n'est d'ordre 2. Ainsi, pour $g \in A$ on a $f(g)^2 = 1$ et $f(g) \neq 1$, et donc $f(g) \in B$. Vérifions que l'application $f_{|A} : A \to B, a \mapsto f(a)$, bien définie, est bijective. Si on a $g, h \in A$ avec $f(g) = f(h)$, on a donc $g = \lambda h$ pour un $\lambda \in \mathbb{F}_4^\times$. Mézalor on a $g = g^3 = \lambda^3 h^3 = 1 \cdot h$, puis $g = h$. Ainsi, $f_{|A}$ est injective. Reste à voir sa surjectivité. Soit $g \in B$. Par surjectivité de f il existe $h \in \mathrm{SL}_3(\mathbb{Z}/2\mathbb{Z})$ avec $f(h) = g$. On a $h^6 = 1$, donc l'ordre de h divise 6. Mais on a $f(h^3) = g^3 = g \neq 1$, donc l'ordre de h est 2 ou 6. Dans le premier cas on a $h \in A$ et on a gagné. Dans le second, on a $h^3 \in A$ et $f(h^3) = g$: on a aussi gagné.

(iv) Comme A est l'ensemble des conjugués d'un certain $a \in A$ par le (ii), et comme on a $f(gag^{-1}) = f(g)f(a)f(g)^{-1}$ car f est un morphisme, on déduit du (iii) que tous les éléments d'ordre 2 de $\mathrm{PSL}_3(\mathbb{F}_4)$ sont conjugués. Si on avait $\mathrm{A}_8 \simeq \mathrm{PSL}_2(\mathbb{F}_4)$, alors A_8 n'aurait qu'une classe de conjugaison d'éléments d'ordre 2. Mais les éléments $(1\,2)(3\,4)$ et $(1\,2)(3\,4)(5\,6)(7\,8)$ sont d'ordre 2, dans A_8, et non conjugués dans S_8.