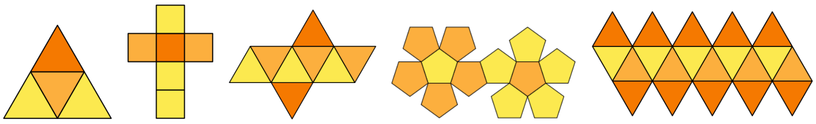
8. Exercices

On commence par trois exercices de géométrie que l'on prendra avec légèreté.

EXERCICE 5.1. (Patrons des solides de Platon) *Indiquer les identifications des patrons suivants des solides de Platon :*



EXERCICE 5.2. (Une construction de l'icosaèdre) *Soit* $\varphi = \frac{1+\sqrt{5}}{2}$ *le* nombre d'or*. On considère les* 4 *points* $(0, \pm 1, \pm\varphi) \in \mathbb{R}^3$*, sommets d'un* rectangle d'or*, ainsi que les* 8 *autres points obtenus en permutant circulairement leurs coordonnées*[24] *:*

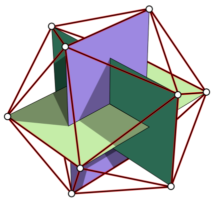


FIGURE 7. *Un triplet de rectangles d'or orthogonaux dans l'icosaèdre*

(i) En calculant une longueur bien choisie, montrer que les 12 *points ci-dessus sont les sommets d'un icosaèdre régulier*[25] I.

(ii) Montrer que les 20 *sommets du dodécaèdre dual à* I *sont*
$$\frac{1}{3}(\varphi, 0, \varphi^3), \quad \frac{1}{3}(\varphi^2, \varphi^2, \varphi^2),$$
et les 18 *autres points qui s'en déduisent par permutation circulaire des coordonnées et changements de signes.*

EXERCICE 5.3. *On suppose donnés* $f \geqslant 3$ *segments du plan ayant un sommet commun et d'angles consécutifs strictement plus grands que l'angle au sommet d'un polygone régulier à* $n \geqslant 3$ *côtés.*

(i) Montrer $\frac{1}{2} < \frac{1}{n} + \frac{1}{f}$.

(ii) En déduire les valeurs possibles de (n, f) *et retrouver la classification des solides de Platon.*

EXERCICE 5.4. *Expliquer en quel sens le groupe de Klein est*[26] *« le groupe des retournements d'un matelas ».*

EXERCICE 5.5. *Soient* $n \geqslant 1$ *un entier et* E *un plan euclidien. Montrer qu'il existe un polygone convexe compact* $P \subset E$ *vérifiant* $\mathrm{Iso}(P) \simeq \mathbb{Z}/n\mathbb{Z}$.

---

24. Cette image est issue du site de J. Baez.
25. On notera que le nombre d'or est l'unique réel $\varphi > 1$ pour lequel cette assertion est vraie.
26. Voir aussi Brian Hayes, *Group Theory in the Bedroom, and other mathematical diversions*.

EXERCICE 5.6. *Montrer que tout sous-groupe fini de* A_5 *est isomorphe à*

$$\mathrm{A}_5,\ \mathrm{A}_4,\ \mathrm{D}_{10},\ \mathrm{S}_3,\ \mathbb{Z}/5\mathbb{Z},\ \mathrm{K}_4,\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \text{ ou } 1.$$

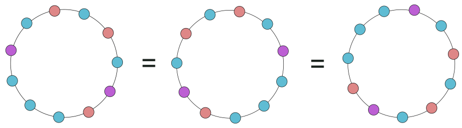
EXERCICE 5.7. *Soient* $m \geqslant 3$, $\mathscr{P}_m$ *un polygone régulier à* m *côtés d'un plan euclidien, et* G *le groupe d'isométries de* $\mathscr{P}_m$ *(on a vu* $G \simeq \mathrm{D}_{2m}$*).*

(i) Montrer qu'il y a exactement une ou deux classes de conjugaison de réflexions orthogonales dans G*, selon que* m *est impair ou non.*

(ii) Soient s *et* t *deux réflexions de* $\mathscr{P}_m$ *dont les axes forment un angle* $\frac{\pi}{m}$ *(justifier). Montrer* $G = \langle s, t\rangle$*.*

Les exercices suivants sont des applications de la formule de Burnside-Frobenius.

EXERCICE 5.8. (Colliers de Polya) *Combien peut-on fabriquer de colliers non similaires contenant* 2 *perles violettes,* 3 *perles rouges et* 6 *perles bleues ?*



EXERCICE 5.9. (Lemme de Jordan) *Soit* G *un groupe fini.*

(i) On suppose que G *agit transitivement sur un ensemble* X *avec* $|X| > 1$*. Montrer qu'il existe un élément de* G *n'ayant aucun point fixe dans* X*.*

(ii) Soit H *un sous-groupe de* G *avec* $H \neq G$*. Montrer* $\cup_{g\in G}\, gHg^{-1} \neq G$*.*

(iii) (Application) On suppose que le sous-groupe H *de* G *contient un représentant de chaque classe de conjugaison de* G*. Montrer* $H = G$*.*

(iv) Donner des contre-exemples à (i), (ii) et (iii) pour $G = \mathrm{SO}(3)$*.*

EXERCICE 5.10. *Soit* G *un groupe fini agissant sur un ensemble fini non vide* X*. On suppose que les propriétés suivantes sont satisfaites :*

(a) Pour tout $x \in X$ *on a* $G_x \neq 1$*,*

(b) Le seul élément de G *fixant deux points distincts de* X *est son neutre* 1*.*

Montrer que G *agit transitivement sur* X*.*

Dans la série d'exercices qui suivent, on s'intéresse aux sous-groupes distingués de $\mathrm{O}(n)$ et $\mathrm{SO}(n)$.

EXERCICE 5.11. *Soit* $n \geqslant 1$ *un entier.*

(i) Déterminer le centre de $\mathrm{O}(n)$*.*

(ii) Montrer $\mathrm{D}(\mathrm{O}(n)) = \mathrm{SO}(n)$*.*

(iii) Montrer que l'on a $\mathrm{O}(n) \simeq \mathrm{SO}(n) \times \{\pm 1\}$ *si, et seulement si,* n *est impair.*

EXERCICE 5.12. *Un retournement d'un espace euclidien* E *de dimension* $n \geqslant 3$ *est une symétrie orthogonale dont l'espace des points fixes est de dimension* $n-2$*.*

(i) Montrer que pour $n \geqslant 3$, les retournements de $\mathrm{SO}(n)$ *sont conjugués et engendrent* $\mathrm{SO}(n)$.

(ii) Déterminer le centre et le groupe dérivé de $\mathrm{SO}(n)$ *pour tout* $n \geqslant 1$.

Exercice 5.13. *Montrer qu'un sous-groupe G de* $\mathrm{O}(2)$ *est distingué si, et seulement si, on a* $G \subset \mathrm{SO}(2)$ *ou* $G = \mathrm{O}(2)$.

Exercice 5.14. *On se propose de montrer que le groupe* $\mathrm{SO}(3)$ *est simple.*

(i) Soit g dans $\mathrm{SO}(3)$ *une rotation d'angle*[27] θ. *Montrer* $\mathrm{tr}\, g = 1 + 2\cos\theta$.

(ii) Montrer que deux éléments de $\mathrm{SO}(3)$ *sont conjugués si, et seulement si, ils ont même trace.*

(iii) Quels sont les $g \in \mathrm{SO}(3)$ *avec* $\mathrm{tr}\, g = 3$ *?*

On fixe H un sous-groupe distingué non trivial de $\mathrm{SO}(3)$.

(iv) On suppose $\mathrm{tr}\, H \supset]x, 3]$ *avec* $x < 3$. *Montrer* $H = \mathrm{SO}(3)$.

(v) Conclure en considérant l'application $\mathrm{SO}(3) \times H \to \mathbb{R}$, $(g, h) \mapsto \mathrm{tr}\, [g, h]$.

Exercice 5.15. (Sous-groupes distingués de $\mathrm{Sp}(1)$ et $\mathrm{SO}(4)$)

(i) En utilisant la simplicité de $\mathrm{SO}(3)$, *lister les sous-groupes distingués de* $\mathrm{Sp}(1)$.

(ii) En déduire les sous-groupes distingués de $\mathrm{SO}(4)$.

Exercice 5.16. *En utilisant la simplicité de* $\mathrm{SO}(3)$ *et des commutateurs bien choisis, montrer que pour* $n > 1$ *:*

(i) le groupe $\mathrm{SO}(2n+1)$ *est simple,*

(ii) les seuls sous-groupes distingués de $\mathrm{SO}(2n+2)$ *sont* 1, $\{\pm 1\}$ *et* $\mathrm{SO}(2n+2)$.

Exercice 5.17. (Structures complexes) *Soient un entier* $n \geqslant 1$ *et* $\mathrm{C}(n) = \{g \in \mathrm{O}(n) \mid g^2 = -1\}$. *Le groupe* $\mathrm{O}(n)$ *agit naturellement sur* $\mathrm{C}(n)$ *par conjugaison.*

(i) Montrer $\mathrm{C}(n) \neq \varnothing \iff n \equiv 0 \bmod 2$, *et* $\mathrm{C}(n) \subset \mathrm{SO}(n)$.

(ii) Montrer que $\mathrm{C}(2n)$ *admet deux orbites sous l'action de* $\mathrm{SO}(2n)$, *et une seule orbite sous celle de* $\mathrm{O}(2n)$.

On notera $\mathrm{C}_+(2n)$ *et* $\mathrm{C}_-(2n)$ *les deux orbites ci-dessus, ainsi que* $\mathrm{G}_+(2n)$ *et* $\mathrm{G}_-(2n)$ *les sous-groupes de* $\mathrm{SO}(2n)$ *qu'elles engendrent respectivement.*

(iii) Que valent $-\mathrm{C}_+(2n)$ *et* $-\mathrm{C}_-(2n)$ *?*

(iv) On suppose $n > 2$. *Montrer* $\mathrm{G}_\pm(2n) = \mathrm{SO}(2n)$.

(v) Montrer que pour tout $x \in \mathrm{C}_+(4)$ *et* $y \in \mathrm{C}_-(4)$ *on a* $xy = yx$, *puis que* $\mathrm{G}_+(4)$ *et* $\mathrm{G}_-(4)$ *sont deux sous-groupes distingués de* $\mathrm{SO}(4)$ *vérifiant* $\mathrm{G}_\pm(4) \simeq \mathrm{Sp}(1)$, $\mathrm{SO}(4) = \mathrm{G}_+(4)\mathrm{G}_-(4)$ *et* $\mathrm{G}_+(4) \cap \mathrm{G}_-(4) = \{\pm 1\}$.

27. On rappelle que si $g \neq 1$, g a une unique droite fixe, et définit une rotation du plan orthogonal : c'est de l'angle de cette rotation dont on parle. On convient qu'il est nul pour $\theta = 1$.

Dans les exercices suivants, on utilise la notion de *bloc* d'une action pour redémontrer que le groupe $\mathrm{SO}(3)$ est simple. Soient G un groupe agissant sur un ensemble X et $B \subset X$ un sous-ensemble non vide. On dira que B est *équilibré* pour cette action si pour tout $b \in B$ et tout $g \in G_b$ on a $g(B) \subset B$. On dit que B est un *bloc* pour cette action si pour tout $g \in G$ on a soit $g(B) = B$, soit $g(B) \cap B = \varnothing$. Un bloc $B \subset X$ est dit *trivial* si on a soit $B = X$, soit $|B| = 1$.

Exercice 5.18. (Blocs, équilibres et sous-groupes distingués) *Soit G un groupe agissant transitivement sur un ensemble X.*

(i) Montrer que $B \subset X$ est un bloc si, et seulement si, les parties de la forme $g(B)$ avec $g \in G$ forment une partition de X.
(ii) Montrer que si $B \subset X$ est un bloc, alors B est équilibré.
(iii) Vérifier que la réciproque est fausse en général.
(iv) Soit N un sous-groupe distingué de G. Montrer que les orbites de X sous N sont des blocs pour l'action de G sur X.

Exercice 5.19. *Soit $n \geqslant 1$ un entier. On considère l'action naturelle de* $\mathrm{SO}(n)$ *sur la sphère unité euclidienne* S^{n-1}.

(i) On suppose[28] *$n \neq 2$. Montrer que pour cette action, les seules parties équilibrées de S^{n-1} de cardinal > 1 sont S^{n-1} et les $\{x, -x\}$ avec $x \in \mathrm{S}^{n-1}$.*
(ii) (Cas $n = 2$) *Montrer que* S^1 *admet des blocs de tout cardinal fini.*

Exercice 5.20. *On se propose de donner une seconde démonstration de la simplicité de* $\mathrm{SO}(3)$. *Soit $H \subset \mathrm{SO}(3)$ un sous-groupe distingué non trivial.*

(i) Montrer[29] *que H agit transitivement sur* S^2.
(ii) Conclure en utilisant des commutateurs bien choisis.

On donne maintenant quelques propriétés et applications des éléments d'ordre 2 de $\mathrm{O}(n)$ (symétries orthogonales), ainsi que des sous-groupes engendrés par un nombre fini de symétries orthogonales qui commutent entre elles.

Exercice 5.21. (Sous-groupes abéliens 2-élémentaires de $\mathrm{O}(n)$)

(i) Montrer que le groupe $\mathrm{O}(n)$ a exactement n classes de conjugaison constituées d'éléments d'ordre 2.
(ii) Soit $G \subset \mathrm{O}(n)$ un sous-groupe abélien 2-élémentaire. Montrer $|G| \leqslant 2^n$.
(iii) On suppose $\mathrm{O}(m) \simeq \mathrm{O}(n)$. Montrer $m = n$.
(iv) On suppose $\mathrm{O}(a) \times \mathrm{O}(b) \simeq \mathrm{O}(a') \times \mathrm{O}(b')$. Montrer $\{a, b\} = \{a', b'\}$.

Exercice 5.22. (Quelques automorphismes non intérieurs)

(i) Soit n un entier pair $\geqslant 2$. Montrer que l'application $g \mapsto (\det g)g$ est un automorphisme non intérieur de $\mathrm{O}(n)$.
(ii) Montrer que $\mathrm{SO}(2)$ *et* $\mathrm{SO}(4)$ *admettent tout deux un automorphisme non intérieur.*

28. Le cas $n = 3$ étant suffisamment intéressant, on pourra s'en contenter.
29. On utilisera les deux exercices précédents.

EXERCICE 5.23. (Automorphismes de $\mathrm{O}(n)$) *On se propose de montrer que tout automorphisme de* $\mathrm{O}(n)$ *est soit intérieur, soit de la forme* $g \mapsto (\det g)\, p\, g\, p^{-1}$ *avec* $p \in \mathrm{O}(n)$ *quand* n *est pair. On note* $\mathcal{S} \subset \mathrm{O}(n)$ *le sous-ensemble des réflexions et on fixe* $s \in \mathcal{S}$ *et* $\alpha \in \mathrm{Aut}\,\mathrm{O}(n)$.

(i) Montrer[30] *que l'on a soit* $\alpha(s) \in \mathcal{S}$*, soit* n *est pair et* $-\alpha(s) \in \mathcal{S}$.

(ii) On suppose $\alpha(s) \in \mathcal{S}$*. Montrer* $\alpha(\mathcal{S}) \subset \mathcal{S}$.

(iii) (suite) En déduire que α *est intérieur par récurrence sur* n.

(iv) Conclure.

EXERCICE 5.24. (Automorphismes de $\mathrm{SO}(n)$)

(i) On suppose $n \neq 2, 4$*. Montrer que tout automorphisme de* $\mathrm{SO}(n)$ *est intérieur.*

(ii) On suppose $n = 2, 4$*. Montrer que* $\mathrm{Aut}\,\mathrm{SO}(n)/\mathrm{Int}\,\mathrm{SO}(n) \simeq \mathbb{Z}/2\mathbb{Z}$.

Dans les exercices suivants on s'intéresse à la fois à la réduction des endomorphismes orthogonaux et à la topologie du groupe orthogonal. On munit $\mathrm{O}(E)$ de la topologie induite par celle du $\mathbb{R}$-espace vectoriel de dimension finie $\mathrm{End}_{\mathbb{R}}(E)$.

EXERCICE 5.25. *Soient* E *un espace euclidien de dimension* $n \geqslant 1$ *et* $u \in \mathrm{O}(E)$.

(i) Montrer que u *possède soit une droite stable, soit un plan stable dans* E.[31]

(ii) On suppose $u \in \mathrm{SO}(E)$*. Montrer qu'il existe une décomposition orthogonale*

$$E = P_1 \perp P_2 \perp \cdots \perp P_r \perp D$$

avec $r = [n/2]$ *et* $\dim P_i = 2$, $u(P_i) \subset P_i$ *et* $u_{|P_i} \in \mathrm{SO}(P_i)$ *pour tout* $1 \leqslant i \leqslant r$.

(iii) On suppose $\det u = -1$*. Montrer qu'il existe* $v \in E$ *et une décomposition orthogonale* $E = F \perp \mathbb{R}v$ *avec* $u(v) = -v$, $u(F) \subset F$ *et* $u_{|F} \in \mathrm{SO}(F)$.

On notera $\mathcal{F}(E)$ l'ensemble des r-uples $F = (P_1, \ldots, P_r)$ de plans $P_i \subset E$ qui sont deux à deux orthogonaux, avec $r = [n/2]$ et $n = \dim E$. Pour chaque $F \in \mathcal{F}(E)$, on a une décomposition associée $E = P_1 \perp P_2 \perp \cdots \perp P_r \perp D$ avec $\dim D = n - 2r \leqslant 1$, et on note T_F le sous-groupe des $g \in \mathrm{SO}(E)$ tels que $g(P_i) = P_i$ pour tout i et $g_{|P_i} \in \mathrm{SO}(P_i)$ (*« tore défini par le drapeau* F *»*).

EXERCICE 5.26. *Soient* E *un espace euclidien de dimension* $n \geqslant 1$.

(i) Montrer que $\mathrm{O}(E)$ *est compact dans* $\mathrm{End}_{\mathbb{R}}(E)$.

(ii) Montrer que pour tout $F \in \mathcal{F}(E)$*, le sous-groupe* T_F *est fermé dans* $\mathrm{O}(E)$ *et continûment isomorphe à* $(\mathrm{S}^1)^r$ *avec* $r = [n/2]$.

(iii) Montrer que l'action naturelle de $\mathrm{SO}(E)$ *sur* $\mathcal{F}(E)$ *est transitive et que l'on a* $T_{gF} = g T_F g^{-1}$ *pour tout* $g \in \mathrm{SO}(E)$ *et tout* $F \in \mathcal{F}(E)$.

(iv) Montrer $\mathrm{SO}(E) = \bigcup_{F \in \mathcal{F}(E)} T_F$.

(v) En déduire que $\mathrm{SO}(E)$ *est connexe par arcs.*

EXERCICE 5.27. (Sous groupes infinis fermés de $\mathrm{O}(2)$ et $\mathrm{SO}(3)$).

30. On pourra examiner le centralisateur de $\alpha(s)$ dans $\mathrm{O}(n)$ et utiliser l'Exercice 5.21.

31. Plus généralement, montrer que tout endomorphisme d'un espace vectoriel réel de dimension finie possède soit une droite stable, soit un plan stable.

(i) Montrer que les sous-groupes infinis fermés de $\mathrm{O}(2)$ *sont* $\mathrm{SO}(2)$ *et* $\mathrm{O}(2)$.

(ii) En déduire les sous-groupes infinis, fermés et réductibles de $\mathrm{SO}(3)$.

(iii) Montrer que le seul sous-groupe fermé, infini et irréductible de $\mathrm{SO}(3)$ *est* $\mathrm{SO}(3)$ *tout entier.*

On s'intéresse maintenant à la structure de la $\mathbb{R}$-algèbre des quaternions.

Exercice 5.28. (Les copies de $\mathbb{C}$ dans $\mathbb{H}$) *Posons* $\mathscr{I} = \{q \in \mathbb{H} \mid q^2 = -1\}$. *On rappelle que pour tout* $q \in \mathscr{I}$ *on a posé* $\mathbb{C}_q = \mathbb{R} + q\mathbb{R}$*, on sait que c'est une sous-*$\mathbb{R}$*-algèbre de* $\mathbb{H}$ *isomorphe à* $\mathbb{C}$.

(i) Montrer que l'action par conjugaison de $\mathrm{Sp}(1)$ *sur* $\mathscr{I}$ *est transitive.*

(ii) Soit $q \in \mathscr{I}$. *Montrer que si* A *est un sous-anneau de* $\mathbb{H}$ *contenant* $\mathbb{C}_q$*, alors on a* $A = \mathbb{C}_q$ *ou* $A = \mathbb{H}$. *(On pourra regarder* $\mathbb{H}$ *comme* $\mathbb{C}_q$*-espace vectoriel).*

(iii) Soit $q \in \mathbb{H} \smallsetminus \mathbb{R}1$. *Montrer qu'il existe* $q' \in \mathscr{I}$ *avec* $\mathbb{R} + \mathbb{R}q = \mathbb{C}_{q'}$.

(iv) En déduire que les sous-$\mathbb{R}$*-algèbres de* $\mathbb{H}$ *sont* $\mathbb{R}$, $\mathbb{H}$, *et les* $\mathbb{C}_q$ *pour* $q \in \mathscr{I}$, *et que ces dernières sont permutées transitivement par conjugaison par* $\mathrm{Sp}(1)$.

Exercice 5.29. *Soient* q *et* q' *deux éléments de* $\mathrm{Sp}(1)$. *Montrer que* q *et* q' *sont conjugués dans* $\mathrm{Sp}(1)$ *si, et seulement si, on a* $\mathrm{t}(q) = \mathrm{t}(q')$.

Exercice 5.30. *Soit* $m > 2$ *entier. Montrer qu'un élément* $q \in \mathrm{Sp}(1)$ *est d'ordre* m *si, et seulement si, on a* $\mathrm{t}(q) = 2\cos(2k\pi/m)$ *avec* $k \in \mathbb{Z}$ *et* $(k, m) = 1$.

Les deux exercices suivants concernent les quaternions *entiers*. Le premier montre notamment que pour p premier impair, $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ peut être vu comme un anneau de *quaternions modulo* p.

Exercice 5.31. *Soit* p *un nombre premier impair.*

(i) Montrer qu'il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ *tels que* $x^2 + y^2 = -1$.

On considère les deux matrices $I = \begin{bmatrix} x & y \\ y & -x \end{bmatrix}$ *et* $J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ *de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(ii) Vérifier $I^2 = -1$, $J^2 = -1$ *et* $IJ = -IJ$.

(iii) Montrer que $\{1, I, J, IJ\}$ *est une base du* $\mathbb{Z}/p\mathbb{Z}$*-espace vectoriel* $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

(iv) En déduire que H_8 *est isomorphe à un sous-groupe de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ *pour tout nombre premier* $p > 2$.

Pour $q \in \mathbb{H}$ on pose $\chi_q = t^2 - \mathrm{t}(q)t + \mathrm{n}(q)$ (polynôme caractéristique de q).

Exercice 5.32. (Quaternions de Hurwitz, partie I) *On considère l'élément* $\omega = \frac{1+I+J+K}{2}$ *de* $\mathbb{H}$ *et on pose* $\mathrm{Hur} = \mathbb{Z} + \mathbb{Z}\,I + \mathbb{Z}\,J + \mathbb{Z}\,K + \mathbb{Z}\omega$.

(i) Montrer que Hur *est un sous-anneau de* $\mathbb{H}$, *et* $\chi_q \in \mathbb{Z}[t]$ *pour tout* $q \in \mathrm{Hur}$.

(ii) Montrer $\mathrm{Hur}^\times = \{q \in \mathrm{Hur} \mid \mathrm{n}(q) = 1\}$.

(iii) En déduire $|\mathrm{Hur}^\times| = 24$ *et lister les* 24 *éléments de* $\mathrm{Hur}^\times$ *ainsi que leurs polynômes caractéristiques.*

(iv) Montrer que $\mathrm{Hur}^\times$ *contient* H_8 *comme sous-groupe distingué d'indice* 3.

Dans l'exercice suivant, on se propose de montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ pour tout premier $p \neq 2$ (un fait assez surprenant !).

Exercice 5.33. (Quaternions de Hurwitz, partie II) *Soit p premier impair.*

(i) Exhiber[32] *un morphisme d'anneaux surjectif* $\varphi : \mathrm{Hur} \to \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$.

(ii) Vérifier $\mathrm{trace}(\varphi(q)) \equiv \mathrm{tr}(q) \bmod p$, *et en déduire* $\det \varphi(q) \equiv \mathrm{n}(q) \bmod p$, *pour tout* $q \in \mathrm{Hur}$.

(iii) En déduire $\mathrm{Hur}^\times \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

(iv) Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ *est isomorphe à un sous-groupe de* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Exercice 5.34. *(i) Montrer que* $\mathrm{Aut}(\mathrm{H}_8)$ *est naturellement isomorphe au groupe des isométries directes de l'octaèdre de sommets* $\pm I, \pm J, \pm K$ *de* $\mathbb{H}^0$.

(ii) En déduire $\mathrm{Aut}(\mathrm{H}_8) \simeq \mathrm{S}_4$.

Les Exercices 5.35 à 5.39 portent sur la notion d'action *primitive*, due à Galois. On rappelle que la notion de bloc d'une action a été introduite avant l'Exercice 5.18.

Exercice 5.35. (*Blocs d'une action transitive*) *Soit G un groupe agissant transitivement sur X. Pour toute partie $B \subset X$ on pose $G_B = \{g \in G \mid g(B) = B\}$, c'est un sous-groupe de G.*

(i) Montrer que si B est un bloc alors G_B agit transitivement sur B et contient G_x pour tout $x \in B$.

(ii) Soient $x \in X$ et H un sous-groupe de G contenant G_x. Montrer que $B := Hx$ est un bloc contenant x et vérifiant $G_B = H$.

(iii) En déduire que $B \mapsto G_B$ est une bijection croissante entre l'ensemble des blocs de X contenant x, et l'ensemble des sous-groupes de G contenant G_x.

Exercice 5.36. *Une action transitive d'un groupe G sur un ensemble X est dite* primitive *si on a $|X| \geqslant 2$ et si ses seuls blocs sont les blocs triviaux.*

(i) Montrer qu'une action 2-transitive est primitive.

(ii) Soit N un sous-groupe distingué de G agissant non trivialement sur X. Montrer que si G agit primitivement sur X, alors N agit transitivement sur X.

(iii) En déduire que le critère d'Iwasawa vaut encore en remplaçant dans son énoncé l'hypothèse « 2-transitivement » par « primitivement ».

(iv) En utilisant l'exercice précédent, montrer qu'une action transitive de G sur X est primitive si, et seulement si, ses stabilisateurs sont des sous-groupes maximaux de G.

(v) Supposons que G agit transitivement sur X avec $|X| \geqslant 2$. Montrer que G agit 2-transitivement sur X si, et seulement si, pour un $x \in X$ (ou tous) et $g \in G \smallsetminus G_x$, on a $G = G_x \cup G_x g G_x$.

Dans les exercices ci-dessous on retrouve la classification des sous-groupes distingués de S_n et A_n à l'aide du critère d'Iwasawa.

32. On pourra utiliser l'exercice A.1 (iii).

Exercice 5.37. *Soient* $n \geqslant 3$ *et* X_n *l'ensemble des parties à* 2 *éléments de* $\{1, \ldots, n\}$. *On rappelle que* S_n *agit transitivement sur* X_n.

(i) Montrer que S_n *agit* 2*-transitivement sur* X_n*, si et seulement si,* $n = 3$.

(ii) Montrer que S_n *agit primitivement sur* X_n *pour* $n \neq 4$.

(iii) Retrouver les sous-groupes distingués de S_n *à l'aide du critère d'Iwasawa.*

Exercice 5.38. *Soient* $n \geqslant 5$ *et* X_n *l'ensemble des parties à* 3 *éléments de* $\{1, \ldots, n\}$. *On rappelle que* A_n *agit transitivement sur* X_n.

(i) Montrer que A_n *n'agit pas* 2*-transitivement sur* X_n.

(ii) Montrer que A_n *agit primitivement sur* X_n *pour* $n \neq 6$.

(iii) Montrer que les blocs non triviaux de l'action de A_6 *sur* X_6 *ont deux éléments, et décrire leurs stabilisateurs.*

On donne aussi une troisième démonstration de la simplicité de SO(3).

Exercice 5.39. *On considère l'action naturelle de* SO(3) *sur* $\mathbb{P}(\mathbb{R}^3)$.

(i) Montrer que cette action est primitive.

(ii) Est-elle 2*-transitive ?*

(iii) Redémontrer la simplicité de SO(3) *en utilisant le critère d'Iwasawa.*

Exercice 5.40. *Soit* G *un groupe fini* $\neq 1$ *agissant sur un ensemble* X *tel que :*

(a) tout élément de $G \smallsetminus \{1\}$ *a exactement deux points fixes dans* X,

(b) tout point de X *est fixé par au moins un élément de* $G \smallsetminus \{1\}$.

Montrer que les conclusions du Lemme 1.16 sont encore vérifiées.

On donne maintenant quelques exercices sur les groupes linéaires.

Exercice 5.41. *Soit* k *un corps.*

(i) Montrer que toute transvection de $\mathrm{SL}_2(k)$ *est conjuguée dans* $\mathrm{SL}_2(k)$ *à* $\mathrm{T}_{1,2}(\lambda)$*, pour un certain* $\lambda \in k^\times$.

(ii) Montrer que $\mathrm{T}_{1,2}(\lambda)$ *et* $\mathrm{T}_{1,2}(\mu)$ *sont conjuguées dans* $\mathrm{SL}_2(k)$ *si, et seulement si,* μ/λ *est un carré dans* $k^\times$.

Le (ii) ci-dessous montre que le groupe $\mathrm{SL}_2(\mathbb{R})$, dont on a vu en cours qu'il est égal à son groupe dérivé, possède un élément qui n'est pas un commutateur.

Exercice 5.42. *Si* k *est un corps, on note* $\mathrm{P}(k)$ *la propriété* « -1_2 est un commutateur dans $\mathrm{SL}_2(k)$ ».

(i) Montrer que $\mathrm{P}(\mathbb{C})$ *est vraie.*

(ii) Montrer que $\mathrm{P}(\mathbb{R})$ *est fausse.*

(iii) Montrer $\mathrm{P}(k) \iff$ « -1 est somme de deux carrés dans k ».

(iv) Que se passe-t-il si l'on remplace $\mathrm{SL}_2(k)$ *par* $\mathrm{GL}_2(k)$ *?*

Dans l'exercice suivant on note $\mathbb{F}_4$ un corps à 4 éléments. Par exemple, on peut prendre pour $\mathbb{F}_4$ le sous $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de $\mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$ engendré par 1 et

$$\omega = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

C'est un sous-anneau de $\mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$ par la relation $\omega^2 = \omega + 1$, et même un corps car cette relation entraîne $\omega^3 = 1$.

EXERCICE 5.43. *On se propose de montrer que les groupes simples* A_8 *et* $\mathrm{PSL}_3(\mathbb{F}_4)$ *ne sont pas isomorphes, bien que de même cardinal.*

(i) Vérifier $|\mathrm{A}_8| = |\mathrm{PSL}_3(\mathbb{F}_4)|$.

(ii) Montrer que $\mathrm{SL}_3(\mathbb{F}_4)$ *a exactement une classe de conjugaison d'éléments d'ordre* 2*, à savoir les transvections.*

(iii) Montrer que la surjection naturelle $\mathrm{SL}_3(\mathbb{F}_4) \to \mathrm{PSL}_3(\mathbb{F}_4)$ *induit une bijection sur les sous-ensembles respectifs des éléments d'ordre* 2.

(iv) Conclure.

EXERCICE 5.44. *Soient k un corps, $n \geqslant 1$ un entier, D le sous-groupe des matrices diagonales dans* $\mathrm{GL}_n(k)$ *et N le normalisateur de D dans* $\mathrm{GL}_n(k)$. *Montrer que l'on a un isomorphisme*

$$N \simeq (k^\times)^n \rtimes_\alpha \mathrm{S}_n,$$

avec pour morphisme $\alpha : \mathrm{S}_n \to \mathrm{Aut}((k^\times)^n)$ celui induit par les permutations des coordonnées.

EXERCICE 5.45. *On se propose de montrer que* $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ *possède un sous-groupe isomorphe à* D_{2n} *avec $n = p^2 - 1$. On fixe $a \in \mathbb{Z}/p\mathbb{Z}$.*

(i) Montrer qu'il existe $g, h \in \mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ avec $g^2 = a1_2$, $gh = -hg$ et $h^2 = 1_2$.

(ii) On suppose que a n'est pas un carré. Montrer que le sous $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de $\mathrm{M}_2(\mathbb{Z}/p\mathbb{Z})$ engendré par 1_2 et g est un sous-corps de cardinal p^2.

(iii) Conclure.

EXERCICE 5.46. *Soient p premier et α un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ est engendré par les trois homographies $x \mapsto -1/x$, $x \mapsto x+1$ et $x \mapsto \alpha^2 x$.*

EXERCICE 5.47. *Soient p un nombre premier et $f : \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{S}_{p+1}$ un morphisme associé à l'action de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ sur $\widehat{\mathbb{Z}/p\mathbb{Z}}$. Déterminer $\varepsilon \circ f$, où $\varepsilon : \mathrm{S}_{p+1} \to \{\pm 1\}$ désigne la signature.*

EXERCICE 5.48. (Un théorème de Carlitz, suivant Zieve) *Soit p un nombre premier > 2. On se propose de montrer que $\mathrm{S}_{\mathbb{Z}/p\mathbb{Z}}$ est engendré par les bijections affines $x \mapsto ax + b$, et la bijection $x \mapsto x^{p-2}$ (justifier).*

(i) Montrer que l'homographie $1 - 1/x$ est d'ordre 3 et permute $\{0, 1, \infty\}$.

(ii) En déduire $h \circ h \circ h$, où $h(x) = 1 - x^{p-2}$.

(iii) Conclure.

Exercice 5.49. *Montrer que l'action par homographies de* $\mathrm{SL}_2(\mathbb{Z})$ *sur* $\widehat{\mathbb{Q}}$ *est transitive.*