Actions de groupes

Dans toute cette feuille, G désigne un groupe.

1 Actions de groupe

Définition 1.1. *Soit X un ensemble non vide. On dit que G* ***agit (à gauche) sur*** *X, et on note $G \curvearrowright X$, lorsqu'il existe une application*

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

vérifiant :

1. $\forall x \in X, e.x = x$.
2. $\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$.

Exemple 1.2.

1. G agit trivialement sur n'importe quel ensemble non vide.
2. G agit sur lui-même par translation à gauche : $\forall g, g' \in G, g.g' = gg'$. Il agit aussi sur chacun de ses quotients de cette manière.
3. G agit sur l'ensemble de ses sous-groupes par conjugaison : $\forall g \in G, \forall H$ sous-groupe de $G, g.H = gHg^{-1}$.
4. Si H est un sous-groupe distingué de G, G agit sur H par conjugaison : $\forall g \in G, \forall h \in H, g.h = ghg^{-1}$.
5. $\mathrm{Aut}(G)$ agit sur G : $\forall \varphi \in \mathrm{Aut}(G), \forall g \in G, \varphi.g = \varphi(g)$.
6. Si E est un espace vectoriel, $\mathrm{GL}(E)$ agit sur E : $\forall f \in \mathrm{GL}(E), \forall x \in E, f.g = f(g)$.
7. Pour tout $n \geq 1$, $\mathfrak{S}_n$ agit de manière naturelle sur $\{1, \ldots, n\}$.

⚠ Certaines actions « naturelles » sont en fait des actions à droite. Par exemple, pour X un ensemble non vide, on a envie de dire que $\mathfrak{S}_n$ agit sur X^n par

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

pour $\sigma \in \mathfrak{S}_n$ et $x = (x_1, \ldots, x_n) \in X^n$, mais pour $\tau \in \mathfrak{S}_n$ on a

$$\sigma.(\tau.x) = \sigma.(x_{\tau(1)}, \ldots, x_{\tau(n)}) = (x_{\tau(\sigma(1))}, \ldots, x_{\tau(\sigma(1))}) = \tau\sigma.x.$$

Ici, une action à gauche proche est donnée par

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

Proposition 1.3. *Soit X un ensemble non vide. La donnée d'une action de groupe de G sur X est équivalente à celle d'un morphisme de groupes $G \to \mathfrak{S}(X)$.*

Démonstration. Si $G \curvearrowright X$ alors pour tout $g \in G$ on dispose de $\rho_g \in \mathfrak{S}(X)$ défini par $\rho_g(x) = g.x$ pour $x \in X$. La définition d'une action de groupe signifie que $g \mapsto \rho_g$ est un morphisme de groupes de G dans $\mathfrak{S}(X)$. Réciproquement, si $\rho : G \to \mathfrak{S}(X)$ est un morphisme de groupes alors on définit une action de groupes de G sur X par $g.x = \rho(g)(x)$ pour $g \in G, x \in X$. □

Corollaire 1.4 (Théorème de Cayley)**.** *Si G est fini d'ordre n, alors il existe un plongement $G \hookrightarrow \mathfrak{S}_n$.*

Démonstration. L'action par translation à gauche de G sur lui-même donne un morphisme de groupes $\iota : G \to \mathfrak{S}_n$. Mais ce morphisme est injectif puisque si $\iota(g) = \mathrm{id}_G$ alors en particulier $ge = e$, autrement dit $g = e$. □

Définition 1.5. *Soit X un ensemble non vide sur lequel G agit. L'action est dite :*

1. ***transitive*** *lorsque $\forall x, y \in X, \exists g \in G, g.x = y$. (« On peut passer d'un élément à n'importe quel autre »)*
2. ***simplement transitive*** *lorsque $\forall x, y \in X, \exists! g \in G, g.x = y$. (« On peut passer d'un élément à n'importe quel autre d'une manière unique »)*
3. ***fidèle*** *lorsque le morphisme $G \to \mathfrak{S}(X)$ est injectif. (« Seul le neutre agit trivialement »)*
4. ***libre*** *lorsque $\forall g \in G \setminus \{e\}, \forall x \in X, g.x \neq x$. (« Seul le neutre a des points fixes »)*

Remarque 1.6. Une action libre est fidèle.

Exercice 1. *Parmi les exemples de l'Exemple 1.2, dire si les actions sont transitives, simplement transitives, fidèles ou libres.*

Exercice 2. *Montrer qu'une action est simplement transitive si et seulement si elle est transitive et libre. Donner un exemple d'action fidèle qui n'est pas libre.*

2 Orbites et stabilisateurs

Dans cette section, X est un ensemble non vide sur lequel G agit.

Définition 2.1. *Si $x \in X$, l'**orbite** de x sous l'action de G est*

$$\mathrm{Orb}(x) = \{g.x \mid g \in G\} \subset X$$

*et le **stabilisateur** de x est*

$$\mathrm{Stab}(x) = \{g \in G \mid g.x = x\} \subset G.$$

*Si $g \in G$, le **fixateur** de g est*

$$\mathrm{Fix}(g) = \{x \in X \mid g.x = x\}.$$

*On appelle **espace-quotient**, et on note ${}_G\backslash^X$, l'ensemble des orbites pour cette action.*

Exemple 2.2.

1. L'action de G sur X est transitive si et seulement si l'orbite de n'importe quel élément est X.

2. Pour l'action de G sur lui-même par conjugaison, l'orbite de $g \in G$ est $C(g) = \{g'gg'^{-1} \mid g' \in G\}$, la **classe de conjugaison** de g, et son stabilisateur est $Z(g) = \{g' \in G \mid g'gg'^{-1} = g\}$, le **centralisateur** de g. De même, le fixateur de $g \in G$ est son centralisateur.

3. Si H est un sous-groupe de G alors le **normalisateur** de H dans G est le stabilisateur de H pour l'action de G sur ses sous-groupes par conjugaison. C'est aussi le plus grand sous-groupe de G dans lequel H est distingué.

4. Pour l'action de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$, le stabilisateur de $k \in \{1, \dots, n\}$ est l'ensemble des permutations qui n'ont pas k dans leur support et son orbite est $\{1, \dots, n\}$.

Remarque 2.3. On peut reformuler l'Exercice 2 de la manière suivante : une action est simplement transitive si et seulement si elle est transitive et tous les stabilisateurs sont réduits à un singleton.

Proposition 2.4 (Relations orbite-stabilisateur)**.** *Soit $x \in X$. Alors $\operatorname{Stab}(x)$ est un sous-groupe de G et il y a une bijection naturelle entre $G/\operatorname{Stab}(x)$ et $\operatorname{Orb}(x)$. De plus, deux éléments dans une même orbite ont des stabilisateurs conjugués.*

Démonstration. La bijection est donnée par

$$g \operatorname{Stab}(x) \mapsto g.x,$$

dont on vérifie qu'elle est bien définie. Si $y = g.x$ alors $\operatorname{Stab}(y) = g \operatorname{Stab}(x) g^{-1}$. □

⚠ Il n'y a aucune raison pour que $\operatorname{Stab}(x)$ soit distingué dans G, donc il n'y a en général pas de structure naturelle de groupe sur $G/\operatorname{Stab}(x)$ (ou sur $\operatorname{Orb}(x)$).

Proposition 2.5 (« Équation aux classes »)**.** *Les orbites de X forment une partition de X. En particulier, si X est fini et si $x_1, \dots, x_r$ sont des représentants des orbites, alors*

$$|X| = \sum_{i=1}^{r} |\operatorname{Orb}(x_i)|.$$

Si de plus G est fini, on a aussi

$$|X| = \sum_{i=1}^{r} |G/\operatorname{Stab}(x_i)|.$$

Théorème 2.6 (Burnside)**.** *Supposons que G et X sont finis. Le nombre d'orbites pour l'action de G sur X vaut*

$$\left| {}_{G}\backslash^{X} \right| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|.$$

Démonstration. On compte de deux manières différentes le cardinal de l'ensemble

$$\{(g, x) \in G \times X \mid g.x = x\}.$$

D'un côté il vaut

$$\sum_{g \in G} |\operatorname{Fix}(g)|$$

et de l'autre il vaut
$$\sum_{x\in X} |\operatorname{Stab}(x)|.$$
Mais d'après la relation orbite-stabilisateur, cette dernière somme est égale à
$$\sum_{x\in X} \frac{|G|}{|\operatorname{Orb}(x)|}.$$
Or, si $y \in \operatorname{Orb}(x)$ alors $\operatorname{Orb}(y) = \operatorname{Orb}(x)$ et donc
$$\sum_{x\in X} \frac{|G|}{|\operatorname{Orb}(x)|} = |G| \left| {}_G\backslash^X \right|.$$
$\square$

Exercice 3. *Calculer le nombre de coloriages possibles des 12 pointes d'un cadran fixé avec 6 points bleus, 4 points blancs et 2 points rouges. Faire de même quand on s'autorise à faire tourner le cadran.*

3 Applications aux p-groupes

Définition 3.1. *Supposons que G est fini et soit p un nombre premier. On dit que G est un p-**groupe** lorsque le cardinal de G est une puissance de p.*

Lemme 3.2. *Soit X un ensemble non vide sur lequel G agit. Si G est un p-groupe fini alors*
$$|X| \equiv |X^G| \bmod p,$$
où
$$X^G = \{x \in X \mid \forall g \in G, g.x = x\} = \bigcap_{g\in G} \operatorname{Fix}(g).$$

Démonstration. D'après l'équation aux classes, on a
$$|X| = \sum_{i=1}^{r} |\operatorname{Orb}(x_i)|,$$
où les x_i sont des représentants des orbites de X sous l'action de G. Si $x_i \in X^G$ alors $|\operatorname{Orb}(x_i)| = 1$, tandis que si $x_i \notin X^G$ alors $|\operatorname{Orb}(x_i)| = \frac{|G|}{|\operatorname{Stab}(x_i)|}$ est divisible par p puisque $\operatorname{Stab}(x_i) \subsetneq G$. $\square$

Proposition 3.3. *Supposons que G est un p-groupe fini. Alors $Z(G) \neq \{e\}$.*

Démonstration. Faisons agir G sur lui-même par conjugaison. L'ensemble des points fixes pour cette action est exactement $Z(G)$ et d'après le Lemme 3.2, on a donc $|G| \equiv Z(G) \bmod p$, autrement dit, $p \mid |Z(G)|$. Mais $|Z(G)| \geq 1$ puisque $e \in Z(G)$ et donc $|Z(G)| \geq p > 1$. $\square$

Lemme 3.4. *Si $G/Z(G)$ est monogène alors G est abélien.*

Démonstration. Soit $xZ(G)$ un générateur de $G/Z(G)$ et soit $g_1, g_2 \in G$. Par définition, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $g_1Z(G) = (xZ(G))^{k_1}$ et $g_2Z(G) = (xZ(G))^{k_2}$. En particulier, il existe $z_1, z_2 \in Z(G)$ tels que $g_1 = x^{k_1}z_1$ et $g_2 = x^{k_2}z_2$. Alors
$$g_1g_2 = x^{k_1+k_2}z_1z_2 = g_2g_1$$
et donc g_1 et g_2 commutent. $\square$

Corollaire 3.5. *Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien.*

Démonstration. Soit G un groupe d'ordre p^2. D'après la Proposition 3.3, $Z(G)$ est un sous-groupe non trivial de G. D'après le théorème de Lagrange, son cardinal ne peut être que p ou p^2. On va montrer qu'il s'agit de p^2, ce qui voudra dire que $G = Z(G)$, autrement dit, que G est abélien.

Si par l'absurde $|Z(G)| = p$ alors, toujours d'après le théorème de Lagrange, $|G/Z(G)| = p$. Mais alors $G/Z(G)$ est cyclique, ce qui implique que G est abélien d'après le Lemme 3.4, ce qui est finalement absurde puisqu'on a supposé $|Z(G)| = p$. □

Théorème 3.6 (Cauchy)**.** *Si G est un groupe fini d'ordre divisible par le nombre premier p alors G admet un élément d'ordre p.*

Démonstration. Faisons agir $H = \mathbb{Z}/p\mathbb{Z}$ sur

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \dots g_p = e\}$$

par décalage d'indice modulo p, autrement dit,

$$\overline{k}.(g_1, \dots, g_p) = (g_{\overline{k+1}}, \dots, g_{\overline{k+p}}).$$

D'après le Lemme 3.2, on a $|X| \equiv |X^H| \mod p$. Mais X^H est constitué des éléments de X à coordonnées constantes, c'est-à-dire des p-uplets $(g, \dots, g)$ avec $g^p = e$. Or $|X| = |G|^{p-1}$ puisqu'on peut prendre n'importe quelles $p-1$ premières coordonnées pour un élément de X et la dernière est alors uniquement déterminée. Ainsi $|X^H|$ est divisible par p. Enfin, $(e, \dots, e) \in X^H$ donc $|X^H| \geq p$ et il existe $g \in G \setminus \{e\}$ tel que $g^p = e$, c'est-à-dire que g est un élément d'ordre p de G. □

Le lemme de Cauchy est un cas particulier des résultats suivants.

Théorème 3.7 (Sylow)**.** *Soit p un nombre premier. Supposons que G est fini d'ordre $p^n m$ avec $m, n \in \mathbb{N}$ et p ne divisant pas m. Alors G possède des **p-sous-groupes de Sylow**, c'est-à-dire des sous-groupes d'ordre p^n. De plus, ceux-ci sont tous conjugués dans G et leur nombre n_p vérifie $n_p \equiv 1 \mod p$ et $n_p \mid m$.*

Remarque 3.8. Les théorèmes de Sylow ne sont pas explicitement au programme mais sont suffisamment classiques pour être abordés. On peut les démontrer à l'aide d'actions de groupes bien choisies, voir les exercices.

4 Exercices

Exercice 4. *Soit K un corps et $n \in \mathbb{N}^*$. Déterminer une action non triviale de $\mathfrak{S}_n$ sur $K[X_1, \dots, X_n]$. Faire de même avec le groupe $\mathrm{GL}_n(K)$.*

Exercice 5. *Déterminer les orbites de l'action de $\mathrm{GL}_n(\mathbb{C})$ par conjugaison sur l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$.*

Exercice 6. *Soit p un nombre premier et G un groupe d'ordre p^2. Montrer que $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Exercice 7. *Soit G un groupe fini d'ordre n et $\iota : G \hookrightarrow \mathfrak{S}_n$ le plongement de Cayley. Pour $g \in G$, calculer $\varepsilon(\iota(g))$. À quelle condition le plongement ι est-il à valeurs dans $\mathfrak{A}_n$?*

Exercice 8. *Soit $n \geq 2$. Montrer que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$ (on pourra distinguer les cas $n < 5$ et $n \geq 5$). Déterminer un plongement $\mathfrak{S}_n \hookrightarrow \mathfrak{A}_{n+2}$. Existe-t-il un plongement $\mathfrak{S}_n \hookrightarrow \mathfrak{A}_{n+1}$?*

Exercice 9. *Soit G un groupe fini d'ordre n, p le plus petit facteur premier de n et H un sous-groupe de G d'indice p. Montrer que $H \triangleleft G$. (Indication : Considérer l'action par translation à gauche de G sur G/H.)*

Exercice 10. *Si P est une partie de $\mathbb{R}^n$, on note $\mathrm{Iso}(P)$ l'ensemble des isométries affines f de $\mathbb{R}^n$ telles que $f(P) = P$, et $\mathrm{Iso}^+(P)$ celles qui sont positives.*

1. *Montrer que $\mathrm{Iso}(P)$ est un groupe pour la composition, et que $\mathrm{Iso}^+(P)$ en est un sous-groupe distingué.*
2. *Soit Δ un tétraèdre régulier dans $\mathbb{R}^3$, de sommets A, B, C et D. Déterminer un morphisme de groupes $\varphi : \mathrm{Iso}(\Delta) \to \mathfrak{S}_4$.*
3. *Montrer que φ est bijectif. En déduire $\mathrm{Iso}^+(\Delta)$.*
4. *Calculer le nombre de coloriages différents des faces d'un tétraèdre régulier avec $c \in \{1, \ldots, 4\}$ couleurs.*
5. *Soit maintenant $\mathcal{C}$ un cube dans $\mathbb{R}^3$. On numérote ses sommets $A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4$ de sorte que les grandes diagonales du cube soient les $[A_iB_i]$. Déterminer un morphisme de groupes $\varphi : \mathrm{Iso}(\mathcal{C}) \to \mathfrak{S}_4$.*
6. *Montrer que φ est surjectif et identifier son noyau.*
7. *Montrer que $\varphi_{|\mathrm{Iso}^+(\mathcal{C})}$ est un isomorphisme de $\mathrm{Iso}^+(\mathcal{C})$ dans $\mathfrak{S}_4$.*
8. *En déduire que $\mathrm{Iso}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.*
9. *Calculer le nombre de coloriages différents des faces d'un cube avec $c \in \{1, \ldots, 6\}$ couleurs.*

Exercice 11. *Soit G un groupe fini. Notons $p(G)$ la probabilité que deux éléments choisis uniformément dans G commutent, autrement dit,*

$$p(G) = \frac{|\{(g,h) \in G^2 \mid gh = hg\}|}{|G|^2}.$$

1. *Montrer que $p(\mathbb{H}_8) = \frac{5}{8}$.*
2. *On va montrer que si G est un groupe non abélien alors $p(G) \leq \frac{5}{8}$.*
   (a) *Justifier que si G est non abélien alors $[G : Z(G)] \geq 4$.*
   (b) *Montrer que pour tout $g \in G \setminus \{e\}$, $[G : Z(g)] \geq 2$.*
   (c) *Conclure.*

Exercice 12. *Dans cet exercice, on va montrer les théorèmes de Sylow. Soit donc p un nombre premier et G un groupe fini d'ordre $p^n m$ avec $p \nmid m$ et $n \geq 1$.*

1. *Décrire une action non triviale de G sur l'ensemble de ses parties de cardinal p^n.*

2. *Montrer qu'au moins une orbite a un cardinal non divisible par p et en déduire qu'un des stabilisateurs est un p-Sylow de G.*

3. *Montrer que si H est un sous-groupe de G et S est un p-Sylow de G, alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H. (Indication : Écrire l'équation aux classes pour l'action par translation de H sur G/S.) On admettra (cf. Feuille 4) que cela permet de montrer que tout groupe fini admet un p-Sylow.*

4. *En déduire que tout p-sous-groupe de G est contenu dans un conjugué de S. En particulier, les p-Sylow de G sont tous conjugués.*

5. *En faisant agir G par conjugaison sur l'ensemble de ses p-Sylow, en déduire que $n_p \equiv 1 \bmod p$ et $n_p \mid m$.*

6. *Montrer qu'un p-Sylow de G est distingué dans G si et seulement s'il est le seul p-Sylow de G.*

Exercice 13. *Montrer qu'un groupe d'ordre* 35 *est cyclique et qu'un groupe d'ordre* 48 *n'est pas simple.*

Exercice 14. *Montrer qu'un groupe simple d'ordre* 60 *est isomorphe à* $\mathfrak{A}_5$.

Exercice 15. *Déterminer les* 2*-Sylow de* $\mathfrak{A}_4$ *et ceux de* $\mathfrak{S}_4$.

Exercice 16. *Dénombrer les p-Sylow de $\mathfrak{S}_p$, où p est un nombre premier.*

Exercice 17. *Soit $p < q$ deux nombres premiers distincts. Montrer que si $p \nmid q-1$ alors tout groupe d'ordre pq est cyclique. Dans le cas contraire, montrer qu'un groupe d'ordre pq est soit cyclique, soit isomorphe à un produit semi-direct non abélien $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.*

Exercice 18. *Soit G un groupe fini d'ordre p^n où p est un nombre premier et $n \in \mathbb{N}^*$. Montrer que pour tout $k \in \{0, \ldots, n\}$, G admet un sous-groupe distingué d'ordre p^k. En déduire que tout groupe d'ordre $p^n m$ avec $p \nmid m$ admet des sous-groupes d'ordre p^k pour tout $k \in \{0, \ldots, n\}$.*

Exercice 19. *Soit $n \geq 2$.*

1. *Montrer que si $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ envoie les transpositions sur des transpositions, alors φ est un automorphisme intérieur. (Indication : Utiliser le fait que les transpositions $\tau_i = (1\,i)$ engendrent $\mathfrak{S}_n$.)*

2. *Soit $\sigma \in \mathfrak{S}_n$ qui s'écrit comme produit de n_k k-cycles pour $1 \leq k \leq n$. Montrer que le centralisateur de σ a pour cardinal*

$$|C(\sigma)| = \prod_{k=1}^{n} k^{n_k} n_k!.$$

3. *En déduire que pour $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$.*

4. *Montrer que $\mathfrak{S}_5$ possède six* 5*-Sylow.*

5. *En déduire un morphisme injectif $\mathfrak{S}_5 \to \mathfrak{S}_6$.*

6. *Notons H l'image de ce morphisme et considérons l'action par translation à gauche de $\mathfrak{S}_6$ sur $\mathfrak{S}_6/H$. Montrer que le morphisme associé φ est un automorphisme.*

7. *Montrer que φ n'est pas intérieur. (Indication : Montrer que H n'a pas de point fixe pour l'action naturelle sur $\{1,\dots,6\}$ mais $\varphi(H)$ en a.)*

Exercice 20. *Soit G un groupe et X un ensemble non vide sur lequel G agit. On dit que G agit* ***doublement transitivement*** *sur X lorsque pour tout $x_1, x_2, y_1, y_2 \in X$ avec $x_1 \neq x_2$ et $y_1 \neq y_2$ il existe $g \in G$ tel que $g.x_1 = y_1$ et $g.x_2 = y_2$.*

1. *Montrer qu'un groupe agissant doublement transitivement agit transitivement. La réciproque est-elle vraie ?*

2. *Montrer que si E est un espace vectoriel alors $\mathrm{GL}(E)$ agit doublement transitivement sur l'ensemble des droites de E.*

3. *Montrer que si G est fini et agit doublement transitivement sur X alors*
$$|G| = \frac{1}{2}\sum_{g\in G} |\operatorname{Fix}(g)|^2.$$
(Indication : On pourra considérer l'action naturelle de G sur $X \times X$.)

4. *Montrer que si G agit doublement transitivement sur X alors pour tout $x \in X, \mathrm{Stab}(x)$ est un sous-groupe maximal de G. Montrer également qu'un sous-groupe distingué de G agit trivialement ou transitivement sur X.*

5. *Plus généralement, pour $n \in \mathbb{N}^*$, on dit que G agit* ***n-transitivement*** *sur X lorsque pour $x_1, \dots, x_n \in X$ deux à deux distincts et $y_1, \dots, y_n \in X$ deux à deux distincts, il existe $g \in G$ tel que $g.x_1 = y_1, \dots, g.x_n = y_n$. Montrer que G agit n-transitivement sur X si et seulement si l'action de G sur X induit une action transitive de G sur l'ensemble des parties à n éléments de X.*

6. *Montrer que pour tout $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ agit n-transitivement sur $\{1,\dots,n\}$, et que si $n \geq 3$ alors $\mathfrak{A}_n$ agit $(n-2)$-transitivement sur $\{1,\dots,n\}$ mais pas $(n-1)$-transitivement.*

Remarque. On peut montrer qu'à part les groupes symétriques et alternés d'ordres suffisamment grands, il n'y a qu'un nombre fini de groupes finis de permutations qui agissent n-transitivement pour $n = 4$ ou 5 (groupes de Mathieu). Pour $n \geq 6$, il n'y a plus que les groupes symétriques et alternés d'ordres suffisamment grands.

Exercice 21 (Critère de simplicité d'Iwasawa)**.** *Soit G un groupe agissant doublement transitivement sur un ensemble non vide X et notons H le noyau de cette action. Supposons que $G = D(G)$ et qu'il existe $x \in X$ tel que $S = \mathrm{Stab}(x)$ admet un sous-groupe distingué abélien A tel que G soit engendré par les conjugués de A. On va montrer que G/H est un groupe simple.*

1. *Justifier qu'il suffit de montrer que les seuls sous-groupes distingués K de G tels que $H \subset K$ sont H et G.*

2. *Soit donc $K \triangleleft G$ tel que $H \subset K$. Justifier que KS est un sous-groupe de G.*

3. *En déduire que $KS = S$ ou $KS = G$.*

4. *Supposons que $KS = S$. Montrer que K agit trivialement sur X, puis que $K = H$.*

5. *Supposons que $KS = G$. Montrer que $KA \triangleleft G$ puis que $KA = G$.*

6. *En utilisant le second théorème d'isomorphisme, montrer que G/K est abélien et conclure.*

Remarque. Le critère d'Iwasawa peut être utilisé pour montrer la simplicité des groupes $\mathfrak{A}_n$ pour $n \geq 5$ et des groupes $\mathrm{PSL}_n(K)$ pour $n \geq 3$ ou $|K| > 3$.