## 4. Sous-groupes distingués, groupes symétriques et actions de groupes

**Exercice 1.** Soit G un groupe. On fait opérer G sur l'ensemble de ses sous-groupes par automorphismes intérieurs : étant donnés un sous-groupe H de G et un élément $g \in \mathrm{G}$, on pose $g.\mathrm{H} = g\mathrm{H}g^{-1}$.

Le stabilisateur d'un sous-groupe H sous cette action est le *normalisateur* de H dans G :

$$\mathrm{N_G(H)} = \{g \in \mathrm{G} \mid g\mathrm{H}g^{-1} = \mathrm{H}\}.$$

1. Quel est le normalisateur d'un sous-groupe distingué ? Est-ce une caractérisation des sous-groupes distingués ?
2. Vérifier que $\mathrm{N_G(H)}$ est le plus grand sous-groupe de G dans lequel H soit distingué.
3. Déterminer le normalisateur du sous-groupe de $\mathfrak{S}_4$ engendré par les transposition $(1,2)$ et $(3,4)$.

**Exercice 2.** (*Produit direct*) 1. Soit G un groupe et soient H et K deux sous-groupes distingués de G tels que $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que l'on a $hk = kh$ pour tous $h \in \mathrm{H}$, $k \in \mathrm{K}$. En déduire que $\mathrm{HK} = \{hk \in \mathrm{G},\ h \in \mathrm{H} \text{ et } k \in \mathrm{K}\}$ est un sous-groupe de G isomorphe au groupe produit $\mathrm{H} \times \mathrm{K}$.

2. *Application*. Soit G un groupe abélien fini d'ordre $n$. Pour tout nombre premier $p$, on désigne par $\mathrm{G}(p)$ l'ensemble des éléments de G dont l'ordre est une puissance de $p$.

– Vérifier que $\mathrm{G}(p)$ est un sous-groupe de G (appelé la *composante $p$-primaire* de G).
– Démontrer que G est isomorphe au produit direct des groupes $\mathrm{G}(p)$, $p|n$.
– Démontrer qu'un groupe abélien H d'ordre $n$ est isomorphe à G si et seulement si, pour tout diviseur premier $p$ de $n$, les groupes $\mathrm{G}(p)$ et $\mathrm{H}(p)$ sont isomorphes.

**Exercice 3.** Soit G un groupe fini, soit $p$ le plus petit facteur premier de $|\mathrm{G}|$ et soit H un sous-groupe de G d'indice $p$. L'objectif est de démontrer que H est distingué.

1. On considère l'action de G sur l'ensemble $\mathrm{G/H}$ des classes à gauche modulo H définie par $g.a\mathrm{H} = a\mathrm{H}$. Démontrer que tout sous-groupe de G opère soit transitivement, soit trivialement (c'est-à-dire fixe chaque point).
2. En déduire que H est un sous-groupe distingué de G.

**Exercice 4.** Dresser la liste des éléments du groupe $\mathfrak{S}_n$ ainsi que sa table de multiplication pour $2 \leq n \leq 4$.

**Exercice 5.** Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$ dans $\mathfrak{S}_5$.

1. Expliciter les permutations $\sigma\tau$, $\tau\sigma$, $\sigma^2\tau$ et $\sigma\tau^{-1}$.
2. Déterminer l'ordre de $\sigma$, $\tau$ et $\sigma\tau$.
3. Écrire $\tau$ comme un produit de transpositions de la forme $(i, i+1)$ $(1 \leq i \leq 4)$ puis comme un produit de transpositions de la forme $(1,i)$ $(2 \leq i \leq 5)$.
4. Décomposer $\sigma$ en produit de cycles de supports disjoints.
5. Expliciter $\sigma^{2008}$ et $\tau^{2008}$.

**Exercice 6.** 1. Étant donné un cycle $c = (a_1, a_2, \ldots, a_m)$ dans $\mathfrak{S}_n$, démontrer que l'on a

$$\sigma c \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_m))$$

pour toute permutation $\sigma \in \mathfrak{S}_n$. En déduire que deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si les longueurs des cycles intervenant dans leur décomposition canonique en un produit de cycles disjoints sont les mêmes.

2. Déterminer toutes les classes de conjugaison dans $\mathfrak{S}_5$.

**Exercice 7.** Les permutations suivantes sont-elles conjuguées dans $\mathfrak{S}_7$ ? Si oui, donner explicitement un élément $\tau$ de $\mathfrak{S}_7$ tel que $\sigma' = \tau\sigma\tau^{-1}$.

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 1 & 7 & 6 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 6 & 1 & 4 & 3 \end{pmatrix}$.
2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 3 & 4 & 7 & 1 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 1 & 7 & 2 & 5 \end{pmatrix}$.

**Exercice 8.** Soit $n \geq 2$ un nombre entier. Démontrer que le groupe $\mathfrak{S}_n$ est engendré par

1. les $n-1$ transpositions de la forme $(i, i+1)$, $1 \leq i \leq n-1$ (*Indication : récurrence sur n*) ;
2. les $n-1$ transpositions de la forme $(1, i)$, $2 \leq i \leq n$ ;
3. la transposition $(1,2)$ et le $n$-cycle $(1,2,\ldots,n)$.

**Exercice 9.** On rappelle que le *groupe alterné* $\mathfrak{A}_n$ est le sous-groupe de $\mathfrak{S}_n$ constitué des permutations paires et on suppose $n \geq 3$.

1. Démontrer que le produit de deux transpositions est un produit de 3-cycles.
2. En déduire que le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.
3. Démontrer que tout élément de $\mathfrak{A}_n$ peut s'écrire sous la forme d'un produit de carrés d'éléments de $\mathfrak{S}_n$.

**Exercice 10.** 1. Combien y a-t-il d'éléments dans $\mathfrak{S}_8$ qui se décomposent en un produit de trois cycles disjoints, deux de longueur 2 et un de longueur 3 ?

2. Combien y a-t-il de $m$-cycles dans $\mathfrak{S}_n$ ?

**Exerice 11.** Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_6$.

1. Quel est le nombre d'inversions de $\sigma$ ? En déduire la signature de cette permutation.
2. Décomposer $\sigma$ en un produit de cycles disjoints et en déduire son ordre.
3. Justifier que $\sigma^{2006}$ est un produit de transpositions disjointes puis les déterminer explicitement.
4. Combien y a-t-il d'éléments dans la classe de conjugaison de $\sigma$ ?
5. Décomposer $\sigma$ en un produit de transpositions de la forme $(1, i)$, $2 \leq i \leq 6$.

**Exercice 12.** Décrire les classes de conjugaison dans $\mathrm{GL}(\mathrm{N}, \mathbb{C})$.

**Exercice 13.** (*Commutateurs et groupe dérivé*) Soit G un groupe. Étant donnés deux éléments $x$ et $y$ de G, leur *commutateur* est par définition l'élément $[x,y] = x^{-1}y^{-1}xy$.

On appelle *groupe dérivé* de G le sous-groupe $\mathrm{D}(\mathrm{G})$ de G engendré par les commutateurs $[x,y]$, $x,\ y \in \mathrm{G}$.

1. À quelle condition sur G a-t-on $\mathrm{D}(\mathrm{G}) = \{e\}$ ?
2. Vérifier que $\mathrm{D}(\mathrm{G})$ est un sous-groupe distingué de G.
3. Démontrer que le groupe quotient $\mathrm{G}/\mathrm{D}(\mathrm{G})$ est abélien puis vérifier que, pour tout homomorphisme $f$ de G dans un groupe abélien, $\mathrm{Ker}(f)$ contient $\mathrm{D}(\mathrm{G})$.

**Exercice 14.** (*Groupe dérivé du groupe* $\mathfrak{S}_n$) On utilise les notations de l'exercice précédent.

1. Si $n \geq 5$, démontrer que deux 3-cycles sont toujours conjugués par un élément de $\mathfrak{A}_n$.
2. On suppose encore $n \geq 5$. Étant donné un 3-cycle $\sigma \in \mathfrak{A}_n$, démontrer qu'il existe une permutation $\tau \in \mathfrak{A}_n$ telle que $\sigma = [\sigma, \tau]$. (*Indication : écrire* $\sigma = \sigma^{-1}\sigma^2$)
3. En déduire que l'on a $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$. (*Indication : utiliser l'exercice 9*)
4. Démontrer que l'on a $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$ pour tout $n \geq 2$. [(1)]

**Exercice 15.** Soit $p$ un nombre premier et soit G un groupe fini dont le cardinal est une puissance de $p$. Le but de cet exercice est de démontrer que le centre de G n'est pas réduit à l'élément neutre.

1. Supposons que G opère sur un ensemble fini X et désignons par $\mathrm{X}^{\mathrm{G}}$ l'ensemble des points fixes de X sous G. Démontrer que l'on a $|\mathrm{X}| \equiv |\mathrm{X}^{\mathrm{G}}| \pmod{p}$.
2. Déduire de la question précédente que le centre de G n'est pas réduit à l'élément neutre.

**Exercice 16.** (*Théorème de Cauchy*) Soit G un groupe fini d'ordre $n$ et soit $p$ un diviseur premier de $n$. Le but de cet exercice est de démontrer que G contient un élément d'ordre $p$.

On considère l'ensemble $\mathrm{X} = \{(x_1, \ldots, x_p) \in \mathrm{G}^p \mid x_1 \ldots x_p = e\}$ et on note $\sigma$ le cycle dans $\mathfrak{S}(\mathrm{X})$ défini par $\sigma(x_1, x_2, \ldots, x_p) = (x_2, x_3, \ldots, x_p, x_1)$.

Déterminer le cardinal de X, l'ordre de la permutation $\sigma$ et l'ensemble de ses points fixes. Finalement, conclure.

---

(1) étant donné un corps $k$, Évariste Galois (1811-1832) a décrit une correspondance très précise entre les propriétés des groupes finis et celles des racines $x$ des équations algébriques $f(x) = 0$, où $f \in k[\mathrm{T}]$ est un polynôme. Dans ce dictionnaire, les résultats 3 et 4 impliquent le fait suivant : il est en général impossible de résoudre une équation de degré $\geq 5$ en n'utilisant que des racines $n$-èmes successives ! (Voir par exemple le livre *Théorie de Galois* de J.-P. Escoffier, chez Dunod)