MAT35B - L3A ALGÈBRE

Premier semestre — 2023-2024

Fiche 3: Groupes symétriques

1. Déterminer la signature et l'ordre des permutations suivantes.

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$;

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$;

(c) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 4 & 5 & 8 & 7 & 9 & 11 & 10 & 1 & 12 & 3 & 2 \end{pmatrix}$;

(d) $\sigma = (1\ 2\ 3\ 12)(2\ 3\ 5\ 7\ 10)(4\ 8\ 1)$.

Solution. On rappelle d'abord que l'on notera $\sigma \in \mathbb{S}_n$ typiquement par

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}.$$

En outre, étant donné une injection $\jmath : [\![1,m]\!] \to [\![1,n]\!]$ pour $m,n \in \mathbb{N}^*$, on définit $\mathsf{cyc}(\jmath) \in \mathbb{S}_n$ via $\sigma(i) = i$ pour tout $i \in [\![1,n]\!] \setminus \mathsf{Img}(\jmath)$, $\sigma(\jmath(i)) = \jmath(i+1)$ pour $i \in [\![1,m-1]\!]$ et $\sigma(\jmath(m)) = \jmath(1)$. On note $(\jmath(1)\ \dots\ \jmath(m))$ au lieu de $\mathsf{cyc}(\jmath)$ et on l'appelle **cycle de longueur** m. Noter que le seul cycle de longueur 1 est l'identité de $\mathbb{S}_n$. Si $m \geq 2$, on dit que $\mathsf{Img}(\jmath)$ est le **support** de $\mathsf{cyc}(\jmath)$. On note que l'ordre $\mathsf{ord}(\sigma)$ d'un cycle σ de longueur m est prècisément m et sa signature $\epsilon(\sigma)$ est $(-1)^{m+1}$.

Étant donné un élément $\sigma \in \mathbb{S}_n$, il existe un uplet $(\jmath^1, \dots, \jmath^k)$ avec $k \in \mathbb{N}^*$, où $\jmath^i : [\![1,m_i]\!] \to [\![1,n]\!]$ est une injection pour tout $i \in [\![1,k]\!]$, $\mathsf{Img}(\jmath^i) \cap \mathsf{Img}(\jmath^{i'}) = \emptyset$ pour tous $i,i' \in [\![1,k]\!]$ différents et $[\![1,n]\!] = \cup_{i=1}^k \mathsf{Img}(\jmath^i)$, tel que

$$\sigma = \mathsf{cyc}(\jmath^1) \dots \mathsf{cyc}(\jmath^k). \tag{1}$$

On appelle $(\jmath^1, \dots, \jmath^k)$, et par abus de notation (1), **la décomposition de σ en cycles disjoints**. Cette décomposition $(\jmath^1, \dots, \jmath^k)$ est unique à permutation des éléments du k-uplet près. En plus, pour réduire l'écriture, on remarque que dans plusieurs cas on n'écrira pas les 1-cycles dans (1), mais cela sera indiqué de façon explicite dans les arguments.

Finalement, étant donné $\sigma \in \mathbb{S}_n$ avec la décomposition (1) en cycles disjoints, le **type** de σ est l'application $\mathsf{type}(\sigma) : \mathbb{N}^* \to \mathbb{N}$ donnée par

$$\mathsf{type}(\sigma)(i) = \#\big(\{j \in [\![1,k]\!] : \mathsf{cyc}(\jmath^j) \text{ a longueur } i\}\big)$$

pour tout $i \in \mathbb{N}^*$.

(a) On voit bien que la décomposition en cycles disjoints de σ est donnée par

$$\sigma = (1\ 3)(2\ 4),$$

ce qui nous dit que $\mathsf{ord}(\sigma) = 2$ et $\epsilon(\sigma) = (-1)^3(-1)^3 = 1$.

(b) C'est clair que la décomposition en cycles disjoints de σ est donnée par

$$\sigma = (1\ 3\ 5)(2\ 4),$$

ce qui nous dit que $\mathrm{ord}(\sigma) = 3.2 = 6$ et $\epsilon(\sigma) = (-1)^4(-1)^3 = -1$.

(c) On voit bien que la décomposition en cycles disjoints de σ est donnée par

$$\sigma = (1\ 6\ 9)(2\ 4\ 8\ 10\ 12)(3\ 5\ 7\ 11),$$

ce qui nous dit que $\mathrm{ord}(\sigma) = 3.5.4 = 60$ et $\epsilon(\sigma) = (-1)^4(-1)^6(-1)^5 = -1$.

(d) C'est clair que la décomposition en cycles disjoints de σ est donnée par

$$\sigma = (1\ 4\ 8\ 2\ 12)(3\ 5\ 7\ 10),$$

ce qui nous dit que $\mathrm{ord}(\sigma) = 5.4 = 20$ et $\epsilon(\sigma) = (-1)^6(-1)^5 = -1$.

2. Soient $2 \leq m \leq n$ deux entiers et $\gamma = (a_1\ a_2\ \dots a_m) \in \mathbb{S}_n$ un cycle de longueur m. Montrer que pour tout $\sigma \in \mathbb{S}_n$, $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))$. En déduire que deux cycles dans $\mathbb{S}_n$ sont conjugués si et seulement s'ils ont la même longueur.

Solution. C'est clair que $\sigma \circ \gamma \circ \sigma^{-1}(a) = a$ si $a \notin \{\sigma(a_1), \dots, \sigma(a_m)\}$, vu que dans ce cas $\sigma^{-1}(a) \notin \{a_1, \dots, a_m\}$ et en conséquence $\gamma \circ \sigma^{-1}(a) = \sigma^{-1}(a)$, ce qui donne le résultat. Cela nous dit que $\sigma \circ \gamma \circ \sigma^{-1}(a) = a = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))(a)$, pour tout $a \notin \{\sigma(a_1), \dots, \sigma(a_m)\}$.

On suppose que $a = \sigma(a_i)$, pour $i \in [\![1, m-1]\!]$. Dans ce cas,

$$\big(\sigma \circ \gamma \circ \sigma^{-1}\big)\big(\sigma(a_i)\big) = \sigma \circ \gamma(a_i) = \sigma(a_{i+1}) = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))\big(\sigma(a_i)$$

Finalement, si $a = \sigma(a_m)$, on trouve que

$$\big(\sigma \circ \gamma \circ \sigma^{-1}\big)\big(\sigma(a_m)\big) = \sigma \circ \gamma(a_m) = \sigma(a_1) = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))\big(\sigma(a_m)$$

On conclut que $\sigma \circ \gamma \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \dots \sigma(a_m))$.

Pour la dernière partie, on note que l'identité précédente nous dit immédiatement que deux cycles conjugués ont la même longueur. Réciproquement, si $\rho = (a_1\ \dots\ a_\ell)$ et $\sigma = (b_1\ \dots\ b_\ell)$ sont deux cycles dans $\mathbb{S}_n$ de longueur $\ell \in \mathbb{N}^*$, soient $A = \{a_1, \dots, a_\ell\}$ et $B = \{b_1, \dots, b_\ell\}$. Comme $A' = [\![1, n]\!] \setminus A$ et $B' = [\![1, n]\!] \setminus B$ ont le même cardinal, il existe une bijection $\gamma' : A' \to B'$. En conséquence, l'application $\gamma : [\![1, n]\!] \to [\![1, n]\!]$ qui satisfait que $\gamma|_{A'} = \gamma'$ et qui associe b_i à a_i pour $i \in [\![1, \ell]\!]$ est une bijection. En plus, c'est facile à vérifier que $\sigma' = \gamma\rho\gamma^{-1}$.

3. *Classes de conjugaison de* $\mathbb{S}_3$. Faire la liste des classes de conjugaison de $\mathbb{S}_3$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe.

Solution. On remarque d'abord que deux permutations σ et σ' dans $\mathbb{S}_n$ sont conjugués si et seulement si $\mathrm{type}(\sigma) = \mathrm{type}(\sigma')$. En effet, s'il existe $\gamma \in \mathbb{S}_n$ tel que $\sigma' = \gamma \circ \sigma \circ \gamma^{-1}$ et

$$\sigma = \sigma_1 \dots \sigma_k$$

est la décomposition en cycles de supports disjoints de $\sigma \in \mathbb{S}_n$, où σ_i a longueur $\ell_i \in \mathbb{N}^*$ et support S_i pour tout $i \in [\![1,k]\!]$, alors

$$\sigma' = (\gamma\sigma_1\gamma^{-1})\dots(\gamma\sigma_k\gamma^{-1}).$$

est la décomposition en cycles de supports disjoints, car $\gamma\sigma_i\gamma^{-1}$ est un cycle de longueur $\ell_i \in \mathbb{N}^*$ et de support $\gamma(S_i)$ pour tout $i \in [\![1,k]\!]$. De façon réciproque, si

$$\sigma = \sigma_1 \dots \sigma_k \text{ et } \sigma' = \sigma'_1 \dots \sigma'_{k'}$$

sont les décompositions en cycles de supports disjoints de $\sigma, \sigma' \in \mathbb{S}_n$, où σ_i a longueur $\ell_i \in \mathbb{N}^*$ et support S_i pour tout $i \in [\![1,k]\!]$, et σ'_i est un cycle de longueur $\ell'_i \in \mathbb{N}^*$ et de support S'_i pour tout $i \in [\![1,k']\!]$, la condition $\mathsf{type}(\sigma) = \mathsf{type}(\sigma')$ et l'exercice **2** nous disent précisément qu'il existe des bijections $\varphi : [\![1,k]\!] \to [\![1,k']\!]$ (et en particulier $k = k'$) et $\gamma : [\![1,n]\!] \to [\![1,n]\!]$ telles que $\gamma(S_i) = S'_{\varphi(i)}$ et $\sigma'_{\varphi(i)} = \gamma\sigma_i\gamma^{-1}$ pour tout $i \in [\![1,k]\!]$. Alors,

$$\gamma\sigma\gamma^{-1} = (\gamma\sigma_1\gamma^{-1})\dots(\gamma\sigma_k\gamma^{-1}) = \sigma'_{\varphi(1)}\dots\sigma'_{\varphi(k)} = \sigma'_1\dots\sigma'_{k'} = \sigma'.$$

Pour $n \in \mathbb{N}^*$, soit

$$\mathscr{F}_n = \Big\{ f : \mathbb{N}^* \to \mathbb{N} \text{ telle que } f \text{ a support fini et } \sum_{i\in\mathbb{N}^*} i f(i) = n \Big\}.$$

L'argument dans le paragraphe précédent nous dit précisément que l'application surjective

$$\mathsf{type} : \mathbb{S}_n \to \mathscr{F}_n$$

qui associe $\mathsf{type}(\sigma)$ à $\sigma \in \mathbb{S}_n$ induit une bijection

$$\overline{\mathsf{type}} : \mathbb{S}_n/\sim \to \mathscr{F}_n,$$

où $\sim$ est la relation d'équivalence donnée par conjugaison, *i.e* $\sigma \sim \sigma'$ si et seulement s'il existe $\gamma \in \mathbb{S}_n$ tel que $\sigma' = \gamma\sigma\gamma^{-1}$. Pour $\sigma \in \mathbb{S}_n$, on notera $\mathsf{cl}(\sigma) = \{\sigma' \in \mathbb{S}_n : \sigma' \sim \sigma\}$, ou $\mathsf{cl}\,\sigma$, la classe d'équivalence de σ pour la relation d'équivalence donnée $\sim$ par la conjugaison. En outre, étant donné $\bar{t} = (t_1, \dots, t_n) \in \mathbb{N}_0^n$ tel que $\sum_{i=1}^n i t_i = n$, un argument combinatoire élémentaire nous dit que

$$\#\Big(\big\{\sigma \in \mathbb{S}_n : \mathsf{type}(\sigma)(i) = t_i \text{ pour tout } i \in [\![1,n]\!]\big\}\Big) = \frac{n!}{\prod_{i=1}^n i^{t_i} t_i!}.$$

En conséquence, si $\sigma \in \mathbb{S}_n$, on a

$$\#(\mathsf{cl}(\sigma)) = \frac{n!}{\prod_{i=1}^n i^{t_i} t_i!}, \tag{2}$$

si $\mathsf{type}(\sigma)(i) = t_i$ pour tout $i \in [\![1,n]\!]$.

C'est facile à vérifier que $\#(\mathscr{F}_3) = 3$,

$$\mathbb{S}_3/\sim = \Big\{ \mathsf{cl}(\mathsf{id}_{[\![1,3]\!]}), \mathsf{cl}(1\ 2), \mathsf{cl}(1\ 2\ 3) \Big\},$$

$[\mathsf{id}_{[\![1,3]\!]}] = \{\mathsf{id}_{[\![1,3]\!]}\}$ a cardinal 1, $\mathsf{cl}(12) = \{(1\ 2), (1\ 3), (2\ 3)\}$ possède 3 éléments et $\mathsf{cl}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2)\}$ a cardinal 2. En plus, $\mathsf{ord}(\mathsf{id}_{[\![1,3]\!]}) = 1$, $\mathsf{ord}(1\ 2) = 2$, $\mathsf{ord}(1\ 2\ 3) = 3$ et $\epsilon(\mathsf{id}_{[\![1,3]\!]}) = -\epsilon(1\ 2) = \epsilon(1\ 2\ 3) = 1$.

4. Soit G un groupe, engendré par un nombre fini d'éléments $g_1, \dots, g_n$. Soient $h_1, \dots, h_m$ des éléments de G et $H = \langle h_1, \dots, h_m \rangle$ le sous-groupe qu'ils engendrent.

(a) Montrer que H est distingué si et seulement si $g_i h_j g_i^{-1} \in H$ et $g_i^{-1} h_j g_i \in H$, pour tous $i \in [\![1,n]\!]$ et $j \in [\![1,m]\!]$.

(b) On considère les éléments $\gamma = (1\ 2\ 3\ 4)$, $s_1 = (1\ 2)(3\ 4)$, $s_2 = (1\ 3)(2\ 4)$ et $s_3 = (1\ 4)(2\ 3)$ de $\mathbb{S}_4$. Montrer que $\langle \gamma \rangle \trianglelefteq \langle \gamma, s_1 \rangle$.

(c) Pour des éléments a, b, c, d de $[\![1,4]\!]$, deux-à-deux distincts, décomposer en cycles disjoints la permutation $((a\ b)(c\ d)) \circ ((a\ c)(b\ d))$.

(d) Soit $K = \{\mathrm{id}, s_1, s_2, s_3\}$. Montrer que $\langle s_1 \rangle \trianglelefteq K$ et $K \trianglelefteq \mathbb{S}_4$, mais $\langle s_1 \rangle \ntrianglelefteq \mathbb{S}_4$.

Solution.

(a) C'est clair que si H est distingué alors $g_i h_j g_i^{-1} \in H$ et $g_i^{-1} h_j g_i \in H$, pour tous $i \in [\![1,n]\!]$ et $j \in [\![1,m]\!]$.

On va montrer la réciproque. Soit $N_G(H) = \{g \in G : gHg^{-1} = H\}$. C'est clair que $H \subseteq N_G(H)$, $N_G(H)$ est un sous-groupe de G et H est normal dans $N_G(H)$. On remarque d'abord qu'il suffit de montrer que $g_i \in N_H$ pour tout $i \in [\![1,n]\!]$, car cela implique que $G = \langle \{g_i : i \in [\![1,n]\!]\} \rangle \subseteq N_H \subseteq G$, *i.e* $N_G(H) = G$, qui équivaut à dire que H est normal.

Or, étant donné $i \in [\![1,n]\!]$, soit $\mathrm{Ad}_i : G \to G$ l'isomorphisme de groupes qui associe $g_i g g_i^{-1}$ à g. Comme pour tout isomorphisme de groupes $f : G \to G'$ et toute partie $S \subseteq G$ on a directement que $f(\langle S \rangle) = \langle f(S) \rangle$, on conlut que, si $S = \{h_j : j \in [\![1,m]\!]\}$, alors

$$\mathrm{Ad}_i^{\pm 1}(H) = \mathrm{Ad}_i^{\pm 1}(\langle S \rangle) = \langle \mathrm{Ad}_i^{\pm 1}(S) \rangle \subseteq H,$$

où la dernière inclusion est une conséquence de l'hypothèse de départ. Comme $\mathrm{Ad}_i^{\pm 1}(H) \subseteq H$, on conlut que $\mathrm{Ad}_i^{\pm 1}(H) = H$, *i.e.* $g_i \in N_G(H)$ pour tout $i \in [\![1,n]\!]$, comme on voulait démontrer.

(b) D'après l'item précédent, il suffit de montrer que $s_1 \circ \gamma \circ s_1 \in \langle \gamma \rangle$. Un calcul direct nous dit que $s_1 \circ \gamma \circ s_1 = \gamma^3$, ce qui implique que $\langle \gamma \rangle \trianglelefteq \langle \gamma, s_1 \rangle$.

(c) À partir d'évaluer $(a\ b) \circ (c\ d) \circ (a\ c) \circ (b\ d)$ en les éléments $\{a, b, c, d\}$, on voit bien que

$$(a\ b) \circ (c\ d) \circ (a\ c) \circ (b\ d) = (a\ d) \circ (b\ c).$$

En conséquence, on voit bien que $s_i \circ s_j = s_k$ pour tous $\{i, j, k\} = \{1, 2, 3\}$, ce qui nous dit que $K = \{\mathrm{id}, s_1, s_2, s_3\}$ est un sous-groupe de $\mathbb{S}_4$.

(d) Noter que K est un sous-groupe abélien, ce qui implique que $\langle s_1 \rangle \trianglelefteq K$. D'après l'exercice **2**, on voit que

$$\sigma \circ \big((a\ b)(c\ d)\big) \circ \sigma^{-1} = \sigma \circ (a\ b) \circ \sigma \circ \sigma^{-1} \circ (c\ d) \circ \sigma^{-1} = \big(\sigma(a)\ \sigma(b)\big)\big(\sigma(c)\ \sigma(d)\big) \in K$$

pour tous a, b, c, d tels que $\{a, b, c, d\} = \{1, 2, 3, 4\}$, ce qui nous dit que $K \trianglelefteq \mathbb{S}_4$. Par ailleurs, on voit bien que $(1\ 3)s_1(1\ 3) = (1\ 3)(1\ 2)(3\ 4)(1\ 3) = (2\ 3)(1\ 4) \notin \langle s_1 \rangle$, ce qui nous dit que $\langle s_1 \rangle \ntrianglelefteq \mathbb{S}_4$.

5. (a) Soient $p \in \mathbb{N}^*$ un nombre premier et $n \geq p$ un entier.

(i) Quels sont les éléments d'ordre p dans $\mathbb{S}_n$?

(ii) Le résultat subsiste-t-il lorsque p n'est pas premier ?

(b) Montrer que dans $\mathbb{S}_8$ tout élément d'ordre 10 a pour signature -1. Montrer que dans $\mathbb{S}_n$ tout élément d'ordre impair a pour signature 1.

Solution.

(a) (i) Soit

$$\sigma = \sigma_1 \dots \sigma_k$$

la décomposition de $\sigma \in \mathbb{S}_n$ en cycles disjoints de longueur strictement supérieure à 1. Alors, $\mathrm{ord}(\sigma) = \mathrm{PPCM}(\mathrm{ord}(\sigma_1), \dots, \mathrm{ord}(\sigma_k))$. Comme $\mathrm{ord}(\sigma) = p$ est premier, on conclut que $\mathrm{ord}(\sigma_1) = \cdots = \mathrm{ord}(\sigma_k) = p$, *i.e.* une permutation σ a ordre p si et seulement si σ est un produit non trivial de p-cycles disjoints.

(ii) Non. Par exemples, $\sigma = (12)(345) \in \mathbb{S}_5$ a ordre 6, mais σ est un produit non trivial de 6-cycles disjoints.

(b) Soit

$$\sigma = \sigma_1 \dots \sigma_k$$

la décomposition de $\sigma \in \mathbb{S}_n$ en cycles disjoints de longueur strictement supérieure à 1. On suppose en plus que $1 < \mathrm{ord}(\sigma_1) \leq \cdots \leq \mathrm{ord}(\sigma_k)$. Alors, $\mathrm{ord}(\sigma) = \mathrm{PPCM}(\mathrm{ord}(\sigma_1), \dots, \mathrm{ord}(\sigma_k))$.

Si $n = 8$, on voit bien que $k = 2$, $\mathrm{ord}(\sigma_1) = 2$ et $\mathrm{ord}(\sigma_2) = 5$. En conséquence, $\epsilon(\sigma) = \epsilon(\sigma_1)\epsilon(\sigma_2) = (-1)^3(-1)^6 = -1$.

Si $n \in \mathbb{N}^*$ et σ a ordre impair, alors $\mathrm{ord}(\sigma_1), \dots, \mathrm{ord}(\sigma_k)$ sont impairs, ce qui implique que

$$\epsilon(\sigma) = \epsilon(\sigma_1) \dots \epsilon(\sigma_k) = (-1)^{\mathrm{ord}(\sigma_1)+1} \dots (-1)^{\mathrm{ord}(\sigma_k)+1} = 1.$$

6. Soit $n \geq 2$ un entier. Dans $\mathbb{S}_n$, on considère le n-cycle $\gamma = (1\ 2\ \dots\ n-1\ n)$ et deux transpositions $\tau_0 = (1\ 2)$ et $\tau = (a_1\ a_2)$, avec $a_1, a_2 \in [\![1, n]\!]$ différents.

(a) Montrer que $\{\gamma, \tau_0\}$ engendre $\mathbb{S}_n$.
Indication : on pourra montrer que $\langle \gamma, \tau_0 \rangle$ contient toutes les transpositions de la forme $(i \quad i+1)$.

⋆ (b) Montrer que si n est premier, alors $\{\gamma, \tau\}$ engendre $\mathbb{S}_n$.
Indication : on pourra montrer qu'il existe r tel que $\gamma^r(a_1) = a_2$ et γ^r est encore un n-cycle.

(c) Donner un exemple où $\{\gamma, \tau\}$ n'engendre pas $\mathbb{S}_n$.

Solution.

(a) Il s'agit d'un résultat du cours.

(b) On affirme d'abord que $\mathrm{ord}(\gamma^r) = n$ pour tout $r \in [\![1, n-1]\!]$. En effet, comme γ a ordre n, $\gamma^r \neq \mathrm{id}_{[\![1,n]\!]}$, ce qui nous dit que le sous-groupe $\langle \gamma^r \rangle$ engendré par γ^r a ordre strictement supérieur à 1. Comme $1 < |\langle \gamma^r \rangle| = \mathrm{ord}(\gamma^r)$ divise n et n est premier, on conclut que $\mathrm{ord}(\gamma^r) = n$ pour tout $r \in [\![1, n-1]\!]$. D'après l'exercice **5**, γ^r est un produit non trivial de n-cycles, mais cela nous dit que γ^r est un n-cycle, vu que $\gamma^r \in \mathbb{S}_n$.

Or, comme γ est un n-cycle, il existe $r \in [\![1, n-1]\!]$ tel que $\gamma^r(a_1) = a_2$. Soit $f : [\![1, n]\!] \to [\![1, n]\!]$ l'application qui associe $\gamma^{r(i-1)}(a_1)$ à $i \in [\![1, n]\!]$. On voit bien que f est une bijection, car γ^r l'est. Noter que $f(1) = a_1$ et $f(2) = a_2$. On considère alors l'isomorphisme de groupes

$$\mathrm{Ad}_f : \mathbb{S}_n \to \mathbb{S}_n$$

donné par $\mathsf{Ad}_f(\sigma) = f \circ \sigma \circ f^{-1}$. On voit bien que

$$\mathsf{Ad}_f(\tau_0) = f \circ (1\ 2) \circ f^{-1} = \big(f(1)\ f(2)\big) = (a_1\ a_2) = \tau.$$

En plus, $\mathsf{Ad}_f(\gamma) = f \circ \gamma \circ f^{-1} = \gamma^r$, car

$$(f \circ \gamma \circ f^{-1})(f(i)) = (f \circ \gamma)(i) = f(i+1)$$

pour tous $i \in [\![1, n-1]\!]$ et $(f \circ \gamma \circ f^{-1})(f(n)) = (f \circ \gamma)(n) = f(1)$. Comme $\{\gamma, \tau_0\}$ engendre $\mathbb{S}_n$ et l'image par tout morphisme surjectif de groupes d'un ensemble de générateurs est un ensemble de générateurs, $\{\gamma^r, \tau\}$ engendre $\mathbb{S}_n$, ce qui nous dit *a fortiori* que $\{\gamma, \tau\}$ engendre $\mathbb{S}_n$.

(c) C'est facile à vérifier que si $n = 4$, $\gamma = (1\ 2\ 3\ 4)$ et $\tau = (1\ 3)$, alors $\langle\{\gamma, \tau\}\rangle \subsetneq \mathbb{S}_4$.

⋆ **7.** *Un exemple provenant du mélange d'un jeu de cartes.* Vérifier que l'on définit bien une permutation $\sigma \in \mathbb{S}_{32}$ en posant $\sigma(k) = 2k$ si $k \leq 16$ et $\sigma(k) = 2k-33$ si $k \geq 17$. Déterminer son ordre et sa signature.
Indication : remarquer que $\sigma(k) \equiv 2k \pmod{33}$ pour tout $k \in [\![1, 32]\!]$.

Solution. On montre d'abord que $\sigma \in \mathbb{S}_{32}$. Par ailleurs, $\sigma : [\![1, 32]\!] \to [\![1, 32]\!]$ est bien définie, car $k \in [\![1, 16]\!]$ implique que $\sigma(k) = 2k \in [\![2, 32]\!]$ et $k \in [\![17, 32]\!]$ implique que $\sigma(k) = 2k - 33 \in [\![1, 31]\!]$. En outre, on remarque que σ est une application injective. Pour le montre, on note d'abord que, si $\sigma(k) = \sigma(k')$ avec $k, k' \in [\![1, 32]\!]$, on remarque d'abord que $k, k' \leq 16$ ou $k, k' \geq 17$. En effet, si $k \leq 16$ et $k' \geq 17$, alors $\sigma(k) = 2k$ est pair mais $\sigma(k') = 2k - 33$ est impair. Or, si $k, k' \in [\![1, 16]\!]$ c'est clair que $2k = \sigma(k) = \sigma(k') = 2k'$ implique $k = k'$, et si $k, k' \in [\![17, 32]\!]$ c'est clair que $2k - 33 = \sigma(k) = \sigma(k') = 2k' - 33$ implique $k = k'$. Comme toute application injective entre deux ensembles finis de la même cardinalité est bijective, on conclut que $\sigma \in \mathbb{S}_{32}$.

Finalement, c'est clair que la décomposition en cycles disjoints de σ est donnée par

$$\begin{aligned}\sigma = {} & (1\ 2\ 4\ 8\ 16\ 32\ 31\ 29\ 25\ 17)(3\ 6\ 12\ 24\ 15\ 30\ 27\ 21\ 9\ 18) \\ & (5\ 10\ 20\ 7\ 14\ 28\ 23\ 13\ 26\ 19)(11\ 22),\end{aligned}$$

ce qui nous dit que $\mathsf{ord}(\sigma) = 10$ et $\epsilon(\epsilon) = 1$.

8. Soient p un nombre premier impair et $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Pour tout a dans G, on note σ_a et ρ_a les permutations de G dans G définies par $\sigma_a(x) = ax^{-1}$ et $\rho_a(x) = ax$. Déterminer le type, l'ordre et la signature des permutations σ_a et ρ_a en fonction de la quantité de racines carrées de a dans G et de l'ordre de a, respectivement.

Solution. On traitera d'abord le cas général d'un groupe abélien quelconque G, pour spécifier après le cas où $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Soit $\mathcal{O}_{a,x} = \{\sigma_a^k(x) : k \in \mathbb{Z}\}$ l'orbite de x sous l'action de σ_a. Comme $\sigma_a \circ \sigma_a = \mathrm{id}_G$, vu que $a(ax^{-1})^{-1} = axa^{-1} = xaa^{-1} = x$ pour tout $x \in G$, on conclut que $\mathcal{O}_{a,x} = \{x, ax^{-1}\}$. En particulier, $\#(\mathcal{O}_{a,x}) = 1$ si et seulement si $ax^{-1} = x$, *i.e.* $a = x^2$. Sinon, $\#(\mathcal{O}_{a,x}) = 2$. Soit

$$\sigma_a = \omega_1 \dots \omega_{k_a} \tag{3}$$

la décomposition de $\sigma_a \in \mathsf{Aut}_{\mathsf{Ens}}(G)$ en cycles disjoints de longueur supérieure ou égal à 1.

On remarque que la longueur de chaque cycle ω_i dans (3) coïncide avec le cardinal de l'orbite $\#(\mathscr{O}_{a,x})$, pour x dans le support de ω_i. On suppose alors que σ_i a longueur 1 pour $i \in [\![1, k'_a]\!]$ et longueur 2 pour $i \in [\![k'_a + 1, k_a]\!]$, où $k'_a \in \mathbb{N}$. Pour $i \in [\![1, k'_a]\!]$, soit $\{x_i\}$ le support de ω_i. En conséquence, $X_a = \{x \in G : x^2 = a\} \subseteq G$ coïncide avec $\{x_1, \dots, x_{k'_a}\}$ et $k_a - k'_a = (|G| - k'_a)/2$, vu que $k'_a + 2(k_a - k'_a) = |G|$. C'est clair que $k'_a < |G|$ si $a \neq 1_G$ car dans ce cas $a \notin X_a$. On voit bien que le type $\mathsf{type}(\sigma_a)$ de σ_a est donné par $\mathsf{type}(\sigma_a)(i) = 0$ si $i \in \mathbb{N} \setminus \{1, 2\}$, $\mathsf{type}(\rho_a)(1) = k'_a$ et $\mathsf{type}(\rho_a)(2) = (|G| - k'_a)/2$. En plus,

$$\mathsf{ord}(\sigma_a) = \begin{cases} 1, & \text{si } a = 1_G \text{ et } x^2 = 1_G \text{ pour tout } x \in G, \\ 2, & \text{sinon,} \end{cases}$$

et $\epsilon(\rho_a) = (-1)^{(|G| - k'_a)/2}$.

Pour le cas particulier de $G = (\mathbb{Z}/p\mathbb{Z})^\times$, on note d'abord que, d'après l'exercice **17** de la fiche 2, il existe un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. En particulier, si $p = 3$, $x^2 = 1_G$ pour tout $x \in G$, ce qui nous dit que $k' = |G| = 2$ et $\mathsf{ord}(\sigma_{1_G}) = 1$ dans ce cas. Si $p > 3$, alors c'est clair qu'il existe $x \in G$ tel que $x^2 \neq 1_G$, vu que $2.\bar{1} = \bar{2} \neq \bar{0}$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Par conséquent, $k'_a < |G|$ et $\mathsf{ord}(\sigma_a) = 2$ pour tout $a \in G$ dans ce cas. On peut même dire un peu plus sur la valeur de k'_a. Pour cela, on considère le polynôme unitaire $X^2 - a \in (\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $X^2 - a \in (\mathbb{Z}/p\mathbb{Z})[X]$ admet au plus 2 racines différentes dans $\mathbb{Z}/p\mathbb{Z}$, *i.e.* $k'_a \in \{0, 1, 2\}$. Or, comme $k'_a + 2(k_a - k'_a) = |G| = p - 1$ est pair, k'_a est pair aussi, *i.e.* $k'_a \in \{0, 2\}$. C'est facile à voir dans des exemples que les valeurs $k'_a = 0$ et $k'_a = 2$ sont possibles (*e.g*, si $p = 7$ et $a \in (\mathbb{Z}/7\mathbb{Z})^\times$, $k'_a = 0$ si et seulement si $a \in \{\bar{1}, \bar{2}, \bar{4}\} \subsetneq (\mathbb{Z}/7\mathbb{Z})^\times$).

On continue avec le cas général d'un groupe quelconque G (qui n'est pas forcément abélien). On considère l'application de groupes

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

qui associe ρ_a à tout $a \in G$, où $\rho_a(x) = ax$ pour $x \in G$. Soit $\mathscr{O}_{a,x} = \{a^k x : k \in \mathbb{Z}\}$ l'orbite de x sous l'action de ρ_a. On remarque d'abord que, étant donné $x, y \in G$, l'application bijective $f : G \to G$ donnée par $f(z) = zx^{-1}y$ satisfait que $f(\mathscr{O}_{a,x}) = \mathscr{O}_{a,y}$. En effet, c'est clair que $f(\mathscr{O}_{a,x}) \subseteq \mathscr{O}_{a,y}$, car $f(a^k x) = a^k x x^{-1} y = a^k y$, et l'application bijective $f^{-1} : G \to G$ donnée par $f(z) = zy^{-1}x$ satisfait aussi que $f^{-1}(\mathscr{O}_{a,y}) \subseteq \mathscr{O}_{a,x}$. Cela nous dit que $\#(\mathscr{O}_{a,x}) = \#(\mathscr{O}_{a,1_G}) = |\langle a \rangle| = \mathsf{ord}(a)$, pour tout $x \in G$. Soit

$$\rho_a = \sigma_1 \dots \sigma_k \tag{4}$$

la décomposition de $\rho_a \in \mathsf{Aut}_{\mathsf{Ens}}(G)$ en cycles disjoints de longueur supérieure ou égal à 1. Comme la longueur de chaque cycle σ_i dans (4) coïncide avec le cardinal de l'orbite $\#(\mathscr{O}_{a,x})$, pour x dans le support de σ_i, on conclut que σ_i a longueur $\mathsf{ord}(a)$ pour tout $i \in [\![1, k]\!]$, ce qui nous dit en particulier que $k = |G|/\mathsf{ord}(a)$. En conséquence, le type $\mathsf{type}(\rho_a)$ de ρ_a est donné par $\mathsf{type}(\rho_a)(i) = 0$ si $i \neq \mathsf{ord}(a)$ et $\mathsf{type}(\rho_a)(\mathsf{ord}(a)) = |G|/\mathsf{ord}(a)$. En plus, $\mathsf{ord}(\rho_a) = \mathsf{ord}(a)$ et $\epsilon(\rho_a) = (-1)^{(\mathsf{ord}(a)+1)|G|/\mathsf{ord}(a)}$.

9. *Nombre d'orbites et signature d'une permutation I.* Soit E un ensemble fini de cardinal $n \geq 2$. Pour tout $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ et $x \in E$, on note $O_\sigma(x)$ l'orbite de x sous l'action de σ, $N(\sigma)$ le nombre d'orbites de σ et $\varepsilon(\sigma) = (-1)^{n - N(\sigma)}$. On cherche à retrouver les principales propriétés de l'invariant $\varepsilon(\sigma)$ à partir de cette définition.

(*a*) Soient $\sigma \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ et la transposition $\tau = (a\ b) \in \mathsf{Aut}_{\mathsf{Ens}}(E)$ pour $a, b \in E$ distincts. L'objet des questions suivantes est de comparer les orbites sous l'action de σ avec les orbites sous l'action de $\tau \circ \sigma$. On note O_1 et O_2 les orbites de a et de b sous l'action de σ.

(i) Montrer que $O_{\tau \circ \sigma}(x) = O_\sigma(x)$, pour tout $x \in E \setminus (O_1 \cup O_2)$.

(ii) Dans cette question, on suppose que $O_1 = O_2$. Montrer alors que les orbites de a et b sous l'action de $\tau \circ \sigma$ sont différentes et que leur réunion est O_1.

(iii) Dans cette question, on suppose que $O_1 \neq O_2$. Montrer alors que l'orbite de a sous l'action de $\tau \circ \sigma$ est $O_1 \cup O_2$.

(iv) Quelle relation y a-t-il entre $N(\tau \circ \sigma)$ et $N(\sigma)$? Entre $\mathscr{e}(\tau \circ \sigma)$ et $\mathscr{e}(\sigma)$?

(b) En déduire les conséquences suivantes :

(i) $\min(\{k \in \mathbb{N} : \sigma = \tau_1 \dots \tau_k \in \mathbb{S}_n, \tau_1, \dots, \tau_k \text{ transpositions}\}) = n - N(\sigma)$;

(ii) si $\sigma = \tau_1 \dots \tau_k \in \mathbb{S}_n$ est une composée de k transpositions $\tau_1, \dots, \tau_k$, alors $\mathscr{e}(\sigma) = (-1)^k$;

(iii) $\mathscr{e}(\sigma)$ coïncide avec la signature $\epsilon(\sigma)$ de σ.

Solution.

(a) (i) On remarque d'abord que $(\tau \circ \sigma)^k(x) = \sigma^k(x) \in E \setminus (O_1 \cup O_2)$, pour tout $x \in E \setminus (O_1 \cup O_2)$ et $k \in \mathbb{N}$. En effet, le cas $k = 0$ est trivial et le cas $k = 1$ suit du fait que, dans ce cas, $\sigma(x) \in E \setminus (O_1 \cup O_2) \subseteq E \setminus \{a, b\}$, ce qui nous dit que $\tau(\sigma(x)) = \sigma(x)$. Pour le cas $k \geq 2$ on procède par récurrence sur k. En effet, $(\tau \circ \sigma)^{k-1}(x) = \sigma^{k-1}(x) \in E \setminus (O_1 \cup O_2)$ nous dit que

$$
\begin{aligned}
(\tau \circ \sigma)^k(x) &= \big((\tau \circ \sigma) \circ (\tau \circ \sigma)^{k-1}\big)(x) = \big((\tau \circ \sigma) \circ \sigma^{k-1}\big)(x) \\
&= (\tau \circ \sigma^k)(x) = \sigma^k(x) \in E \setminus (O_1 \cup O_2),
\end{aligned}
$$

vu que $\sigma^k(x) \in E \setminus (O_1 \cup O_2)$. Cela nous dit *a fortiori* que

$$
O_{\tau\circ\sigma}(x) = \{(\tau \circ \sigma)^k(x) : k \in \mathbb{N}\} = \{\sigma^k(x) : k \in \mathbb{N}\} = O_\sigma(x)
$$

pour tout $x \in E \setminus (O_1 \cup O_2)$.

(ii) Soit $\ell \in \mathbb{N}^*$ le cardinal de $O_1 = O_2$. Comme $b \in O_1$, on voit bien qu'il existe $k \in [\![1, \ell - 1]\!]$ tel que $\sigma^k(a) = b$. Soit

$$
\ell' = \min\big\{k \in [\![1, \ell - 1]\!] : \text{ tel que } \sigma^k(a) = b\big\}.
$$

De la même façon, comme $a \in O_2$, il existe $j \in [\![1, \ell - 1]\!]$ tel que $\sigma^j(b) = a$. Soit

$$
\ell'' = \min\big\{j \in [\![1, \ell - 1]\!] : \text{ tel que } \sigma^j(b) = a\big\}.
$$

Un argument par récurrence sur i' et i'' montre directement que $(\tau \circ \sigma)^{i'}(a) = \sigma^{i'}(a)$ pour $i' \in [\![0, \ell' - 1]\!]$ et $(\tau \circ \sigma)^{i''}(b) = \sigma^{i''}(b)$ pour $i'' \in [\![0, \ell'' - 1]\!]$, car $\sigma^{i'}(a), \sigma^{i''}(b) \notin \{a, b\}$ pour $i' \in [\![1, \ell' - 1]\!]$ et $i'' \in [\![1, \ell'' - 1]\!]$. On note en plus que

$$
(\tau \circ \sigma)^{\ell'}(a) = \big((\tau \circ \sigma) \circ (\tau \circ \sigma)^{\ell'-1}\big)(a) = (\tau \circ \sigma^{\ell'})(a) = \tau(b) = a
$$

et

$$
(\tau \circ \sigma)^{\ell''}(b) = \big((\tau \circ \sigma) \circ (\tau \circ \sigma)^{\ell''-1}\big)(b) = (\tau \circ \sigma^{\ell''})(b) = \tau(a) = b,
$$

ce qui nous dit que

$$
O_{\tau\circ\sigma}(a) = \big\{\sigma^{i'}(a) : i' \in [\![0, \ell' - 1]\!]\big\} \subseteq O_1
$$

et

$$
O_{\tau\circ\sigma}(b) = \big\{\sigma^{i''}(b) = \sigma^{\ell'+i''}(a) : i'' \in [\![0, \ell'' - 1]\!]\big\} \subseteq O_1,
$$

qui sont des parties disjointes. Cela nous dit en particulier que $\ell' + \ell'' \leq \ell$. En plus comme $a = \sigma^{\ell''}(b) = \sigma^{\ell'+\ell''}(a)$, on conclut que $\ell' + \ell'' \geq \ell$ et par conséquent $\ell' + \ell'' = \ell$, ce qui implique en particulier que

$$
O_1 = O_{\tau\circ\sigma}(a) \sqcup O_{\tau\circ\sigma}(b).
$$

(iii) Soit $\ell_1 \in \mathbb{N}^*$ le cardinal de O_i, pour $i \in \{1,2\}$. De façon analogue à l'item précédent, un argument par récurrence sur i' et i'' montre directement que $(\tau\circ\sigma)^{i'}(a) = \sigma^{i'}(a)$ pour $i' \in [\![0,\ell_1-1]\!]$ et $(\tau\circ\sigma)^{i''}(b) = \sigma^{i''}(b)$ pour $i'' \in [\![0,\ell_2-1]\!]$, car $\sigma^{i'}(a), \sigma^{i''}(b) \notin \{a,b\}$ pour $i' \in [\![1,\ell_1-1]\!]$ et $i'' \in [\![1,\ell_2-1]\!]$. On note en plus que

$$(\tau\circ\sigma)^{\ell_1}(a) = \big((\tau\circ\sigma)\circ(\tau\circ\sigma)^{\ell_1-1}\big)(a) = (\tau\circ\sigma^{\ell_1})(a) = \tau(a) = b$$

et

$$(\tau\circ\sigma)^{\ell_2}(b) = \big((\tau\circ\sigma)\circ(\tau\circ\sigma)^{\ell_2-1}\big)(b) = (\tau\circ\sigma^{\ell_2})(b) = \tau(b) = a,$$

ce qui nous dit que

$$\begin{aligned} O_{\tau\circ\sigma}(a) = &\left\{(\tau\circ\sigma)^{i'}(a) = \sigma^{i'}(a) : i' \in [\![0,\ell_1-1]\!]\right\} \\ &\sqcup \left\{(\tau\circ\sigma)^{\ell_1+i''}(a) = (\tau\circ\sigma)^{i''}(b) = \sigma^{i''}(b) : i'' \in [\![0,\ell_2-1]\!]\right\}, \\ = &\, O_1 \sqcup O_2, \end{aligned}$$

car $(\tau\circ\sigma)^{\ell_1+\ell_2}(a) = (\tau\circ\sigma)^{\ell_2}(b) = a$.

(iv) À partir des items précédents on conclut que

$$N(\tau\circ\sigma) = \begin{cases} N(\sigma)+1, & \text{si } O_1 = O_2, \\ N(\sigma)-1, & \text{si } O_1 \neq O_2. \end{cases}$$

Cela nous dit que $\varepsilon(\tau\circ\sigma) = -\varepsilon(\sigma)$.

(*b*) (i) Comme $N(\tau\circ\sigma) \geq N(\sigma)-1$ pour toute transpositions τ et pour toute permutation σ, un argument immédiat par récurrence sur ℓ nous dit que, si $\sigma = \bar{\tau}_1\dots\bar{\tau}_\ell$ est une factorisation de σ comme produit de transpositions, alors $N(\sigma) \geq N(\mathrm{id}_E) - \ell = n-\ell$, *i.e.* $\ell \geq n - N(\sigma)$. Par conséquent,

$$\min\big(\{k\in\mathbb{N} : \sigma = \tau_1\dots\tau_k \in \mathbb{S}_n, \tau_1,\dots,\tau_k \text{ transpositions}\}\big) \geq n - N(\sigma)$$

pour tout $\sigma \in \mathrm{Aut}_{\mathsf{Ens}}(E)$. Il reste à démontrer que

$$\min\big(\{k\in\mathbb{N} : \sigma = \tau_1\dots\tau_k \in \mathbb{S}_n, \tau_1,\dots,\tau_k \text{ transpositions}\}\big) \leq n - N(\sigma)$$

pour tout $\sigma \in \mathrm{Aut}_{\mathsf{Ens}}(E)$. Pour le faire, on va procéder par récurrence sur la cardinalité de E. On suppose que $\sigma = \tau_1\dots\tau_k$ est une factorisation de σ comme produit de transpositions. Le cas $k=0$ correspond exactement à $\sigma = \mathrm{id}_E$. Dans ce cas $N(\sigma) = n$ et $k = 0 = n-n$, ce qui montre le résultat. On suppose maintenant que $k>0$. Comme $\sigma \neq \mathrm{id}_E$, il existe $e \in E$ tel que $\sigma(e) \neq e$. Soit $\tau = (e\ \sigma(e)) \in \mathrm{Aut}_{\mathsf{Ens}}(E)$ et $E' = E \setminus \{e\}$. Alors, $(\tau\circ\sigma)(e) = e$, ce qui implique que $\sigma' = (\tau\circ\sigma)|_{E'} \in \mathrm{Aut}_{\mathsf{Ens}}(E')$. Noter que $N(\sigma') = (n-1)-(N(\tau\circ\sigma)-1) = n - N(\tau\circ\sigma) = n - N(\sigma) - 1$, d'après l'item précédent. L'hypothèse de la récurrence nous dit qu'il existe une décomposition

$$\sigma' = \tau'_1\dots\tau'_k$$

avec $\tau'_1,\dots,\tau'_k \in \mathrm{Aut}_{\mathsf{Ens}}(E')$ des transpositions de et $k = n - N(\sigma) - 1$. On considère la transposition $\tau_i \in \mathrm{Aut}_{\mathsf{Ens}}(E)$ tel que $\tau_i|_{E'} = \tau'_i$ et $\tau_i(e) = e$ pour tout $i \in [\![1,k]\!]$. Alors, $\sigma = \tau\tau_1\dots\tau_k$, ce qui implique que σ est un produit de $k+1 = n - N(\sigma) - 1 + 1 = n - N(\sigma)$ transpositions.

(ii) Il s'agit d'une conséquence immédiate de l'item (a), (iv).

(iii) Comme les transpositions engendrent le groupe $\mathrm{Aut}_{\mathsf{Ens}}(E)$ et les morphismes de groupes ϵ et ε coïncident dans des transpositions, on conclut que $\epsilon = \varepsilon$.

10. *Nombre d'orbites et signature d'une permutation II.* Soit n un entier strictement positif. Pour une permutation $\sigma \in \mathbb{S}_n$ on note A_σ l'ensemble des orbites de σ et $N(\sigma) = \#(A_\sigma)$ le nombre des orbites de σ. On se propose de donner une autre preuve du fait que le nombre minimal de transpositions nécessaires pour écrire $\sigma \in \mathbb{S}_n$ comme produit de transpositions est $n - N(\sigma)$.

(a) Soit E un espace vectoriel réel de dimension finie n muni d'un produit scalaire fixe $\langle\, ,\rangle$. On se propose d'abord de montrer que le nombre minimal de réflexions orthogonales nécessaires pour écrire une isométrie $f : E \to E$ comme produit de réflexions orthogonales est $n - \mathsf{dim}(\mathsf{Ker}(f - \mathsf{id}_E))$.

On rappelle le résultat démontré en cours qui dit qu'il est possible d'écrire une isométrie f comme un produit de $n - \mathsf{dim}(\mathsf{Ker}(f - \mathsf{id}_E))$ réflexions orthogonales. Soit maintenant $f = s_1 \circ \cdots \circ s_p$ une telle écriture et soit F le sous-espace vectoriel de E engendré par les vecteurs orthogonaux aux hyperplans des réflexions qui interviennent dans cette écriture.

Montrer que l'espace orthogonal $F^\perp$ de F est inclus dans $\mathsf{Ker}(f - \mathsf{id}_E)$. En déduire que $p \geq n - \mathsf{dim}(\mathsf{Ker}(f - \mathsf{id}_E))$ et conclure.

(b) En considérant l'écriture de la permutation $\sigma \in \mathbb{S}_n$ comme produit de cycles à supports disjoints et en écrivant chaque cycle de longueur $k \geq 2$ comme un produit de $k-1$ tranpositions, montrer qu'il est possible d'écrire σ comme un produit de $n - N(\sigma)$ transpositions.

(c) Soit $(e_1, \ldots, e_n)$ une base orthonormée de E et soit $\phi : \mathbb{S}_n \to \mathsf{O}(E)$ l'application qui associe à $\sigma \in \mathbb{S}_n$ l'unique endomorphisme $\phi(\sigma) = f_\sigma : E \to E$ de E qui satisfait que $f_\sigma(e_j) = e_{\sigma(j)}$ pour $j \in [\![1, n]\!]$. Montrer que ϕ est un morphisme de groupes.

(d) Pour une orbite $\mathscr{O} \subseteq [\![1, n]\!]$ de σ notons $F_{\mathscr{O}} = \mathsf{Vect}_{\mathbb{R}}\langle\{e_j : j \in \mathscr{O}\}\rangle \subseteq E$. Montrer que $F_{\mathscr{O}}$ est stable par f_σ. Déterminer $\mathsf{Img}((f_\sigma - \mathsf{id}_E)|_{F_{\mathscr{O}}})$ et sa dimension.

(e) Montrer que

$$E = \bigoplus_{\mathscr{O} \in A_\sigma} F_{\mathscr{O}} \text{ et } \mathsf{Img}(f_\sigma - \mathsf{id}_E) = \bigoplus_{\mathscr{O} \in A_\sigma} \mathsf{Img}\big((f_\sigma - \mathsf{id}_E)|_{F_{\mathscr{O}}}\big).$$

En déduire que $\mathsf{dim}(\mathsf{Ker}(f_\sigma - \mathsf{id}_E)) = N(\sigma)$.

(f) Montrer que si τ est une transposition alors f_τ est une réflexion orthogonale.

(g) Utiliser les items précédents pour montrer que le nombre minimal de transpositions nécessaires pour écrire $\sigma \in \mathbb{S}_n$ comme produit de transpositions est $n - N(\sigma)$.

Solution.

(a) On rappelle d'abord qu'une **réflexion orthogonale** de E est une application de la forme $s_v : E \to E$ pour $v \in E$ non nul où

$$s_v(w) = w - \frac{\langle w, v\rangle}{\langle v, v\rangle} v \tag{5}$$

pour tout $w \in E$. C'est clair que, étant donnés $v, v' \in E$ non nuls, $s_v = s_{v'}$ si et seulement si v et v' sont linéairement dépendants. Le sous-espace vectoriel $H_v = \mathsf{Ker}(s_v - \mathsf{id}_E)$ de E a dimension $n-1$ et il est appelé **l'hyperplan de E associé à la réflexion s_v**. C'est clair que $\mathsf{Vect}_{\mathbb{R}}\langle\{v\}\rangle$ est l'espace vectoriel orthogonal $H_v^\perp$ à l'hyperplan H_v de E associé à la réflexion s_v. On suppose que $f = s_{v_1} \circ \cdots \circ s_{v_p}$, avec $v_1, \ldots, v_p \in E$ non nuls. Le sous-espace vectoriel F de E engendré par les vecteurs orthogonaux aux hyperplans associés aux réflexions $s_{v_1}, \dots, s_{v_p}$ est précisément $\mathsf{Vect}_{\mathbb{R}}\langle\{v_1, \dots, v_p\}\rangle$. En particulier, $\dim(F) \leq p$. Soit $w \in F^{\perp}$, *i.e.* $\langle w, v_i\rangle = 0$ pour tout $i \in [\![1, p]\!]$, ce qui implique que $s_{v_i}(w) = w$ pour tout $i \in [\![1, p]\!]$, d'après (5). Un argument direct nous dit alors que $f(w) = (s_{v_1} \circ \dots \circ s_{v_p})(w) = w$, ce qui implique que $w \in \mathsf{Ker}(f - \mathrm{id}_E)$. En conséquence, $F^{\perp} \subseteq \mathsf{Ker}(f - \mathrm{id}_E)$, ce qui implique que

$$n - \dim(F) = \dim(F^{\perp}) \leq \dim\Big(\mathsf{Ker}(f - \mathrm{id}_E)\Big),$$

ce qui nous dit que

$$p \geq \dim(F) \geq n - \dim\Big(\mathsf{Ker}(f - \mathrm{id}_E)\Big).$$

Comme on a admis qu'il est possible d'écrire une isométrie f comme un produit de $n - \dim(\mathsf{Ker}(f - \mathrm{id}_E))$ réflexions orthogonales, on conclut que le nombre minimal de réflexions orthogonales nécessaires pour écrire f comme produit de réflexions orthogonales est $n - \dim(\mathsf{Ker}(f - \mathrm{id}_E))$.

(b) Pour $k \in [\![1, n]\!]$, soit $n_k(\sigma)$ la quantité de cycles de longueur k dans l'écriture de la permutation $\sigma \in \mathbb{S}_n$ comme produit de cycles à supports disjoints. En conséquence,

$$n = \sum_{k=1}^{n} k n_k(\sigma) \text{ et } N(\sigma) = \sum_{k=1}^{n} n_k(\sigma).$$

Comme tout cycle de longueur $k \geq 2$ peut s'écrire comme un produit de $k-1$ tranpositions, alors on peut écrire σ comme un produit de

$$\sum_{k=1}^{n}(k-1)n_k(\sigma) = \sum_{k=1}^{n} k n_k(\sigma) - \sum_{k=1}^{n} n_k(\sigma) = n - N(\sigma)$$

tranpositions, comme on voulait démontrer.

(c) C'est clair que $f_\sigma \in \mathsf{O}(E)$ pour tout $\sigma \in \mathbb{S}_n$, vu que

$$\langle f_\sigma(e_i), f_\sigma(e_j)\rangle = \langle e_{\sigma(i)}, e_{\sigma(j)}\rangle = \delta_{\sigma(i),\sigma(j)} = \delta_{i,j} = \langle e_i, e_j\rangle$$

pour tous $i, j \in [\![1, n]\!]$, où $\delta_{i,j}$ vaut 0 si $i \neq j$ et 1 si $i = j$. Étant donné $\sigma, \tau \in \mathbb{S}_n$, on voit bien que

$$\phi(\sigma \circ \tau)(v_i) = v_{(\sigma\circ\tau)(i)} = \phi(\sigma)(v_{\sigma(i)}) = \phi(\sigma) \circ \phi(\tau)(v_i)$$

pour tout $j \in [\![1, n]\!]$, ce qui nous dit que $\phi(\sigma\circ\tau) = \phi(\sigma)\circ\phi(\tau)$, *i.e.* ϕ est un morphisme de groupes.

(d) Pour montrer que $F_{\mathcal{O}}$ est stable par f_σ (*i.e.* $f_\sigma(F_{\mathcal{O}}) \subseteq F_{\mathcal{O}}$), il suffit de montrer que $f_\sigma(e_j) \in F_{\mathcal{O}}$ pour tout $j \in \mathcal{O}$. Or, comme $f_\sigma(e_i) = e_{\sigma(i)}$ pour tout $i \in [\![1, n]\!]$ et $\sigma(j) \in \mathcal{O}$ pour $j \in \mathcal{O}$, on conclut que $f_\sigma(e_j) = e_{\sigma(j)} \in F_{\mathcal{O}}$ pour tout $j \in \mathcal{O}$. Soit $\mathcal{O} \subseteq [\![1, n]\!]$ une orbite de cardinalité $k \in \mathbb{N}^*$ et soit $j_0 \in \mathcal{O}$ son minimum. On voit bien que

$$\begin{aligned}
\mathsf{Img}\Big((f_\sigma - \mathrm{id}_E)|_{F_{\mathcal{O}}}\Big) &= \mathsf{Vect}_{\mathbb{R}}\Big\langle\{f_\sigma(e_j) - e_j : j \in \mathcal{O}\}\Big\rangle = \mathsf{Vect}_{\mathbb{R}}\Big\langle\{e_{\sigma(j)} - e_j : j \in \mathcal{O}\}\Big\rangle \\
&= \mathsf{Vect}_{\mathbb{R}}\Big\langle\{e_{\sigma^{i+1}(j_0)} - e_{\sigma^i(j_0)} : i \in [\![0, k-2]\!]\}\Big\rangle \\
&= \mathsf{Vect}_{\mathbb{R}}\Big\langle\{e_{\sigma^i(j_0)} - e_{j_0} : i \in [\![1, k-1]\!]\}\Big\rangle,
\end{aligned}$$

où l'on a utilisé la définition de f_σ dans les deux premiers égalités. Comme l'ensemble $\{e_{\sigma^i(j_0)} - e_{j_0} : i \in [\![1, k-1]\!]\}$ est libre, on conclut alors que $\dim(\mathsf{Img}((f_\sigma - \mathrm{id}_E)|_{F_{\mathcal{O}}})) = k - 1 = \#(\mathcal{O}) - 1$.

(*e*) L'identité

$$E = \bigoplus_{\mathcal{O}\in A_\sigma} F_{\mathcal{O}} \tag{6}$$

suit directément du fait que

$$[\![1,n]\!] = \bigsqcup_{\mathcal{O}\in A_\sigma} \mathcal{O}$$

et que $\{e_i : i \in [\![1,n]\!]\}$ est une base de E. L'identité

$$\mathsf{Img}(f_\sigma - \mathsf{id}_E) = \bigoplus_{\mathcal{O}\in A_\sigma} \mathsf{Img}\big((f_\sigma - \mathsf{id}_E)|_{F_{\mathcal{O}}}\big)$$

suit directément de (6) et du fait que $(f_\sigma - \mathsf{id}_E)(F_{\mathcal{O}}) \subseteq F_{\mathcal{O}}$ pour tout $\mathcal{O} \in A_\sigma$. L'item précédent nous dit alors que

$$\begin{aligned}\mathsf{dim}\big(\mathsf{Img}(f_\sigma - \mathsf{id}_E)\big) &= \sum_{\mathcal{O}\in A_\sigma} \mathsf{dim}\Big(\mathsf{Img}\big((f_\sigma - \mathsf{id}_E)|_{F_{\mathcal{O}}}\big)\Big) = \sum_{\mathcal{O}\in A_\sigma} \big(\#(\mathcal{O}) - 1\big) \\ &= \sum_{\mathcal{O}\in A_\sigma} \#(\mathcal{O} - \#(A_\sigma) = n - \#(A_\sigma) = n - N(\sigma).\end{aligned}$$

En conséquence,

$$\mathsf{dim}\big(\mathsf{Ker}(f_\sigma - \mathsf{id}_E)\big) = \mathsf{dim}(E) - \mathsf{dim}\big(\mathsf{Img}(f_\sigma - \mathsf{id}_E)\big) = n - \big(n - N(\sigma)\big) = N(\sigma).$$

(*f*) Soit $\tau = (i\,j)$, avec $i, j \in [\![1,n]\!]$ différents. On pose $v = (e_i - e_j)/\sqrt{2} \in E$. C'est clair que v est non nul, et en fait $\langle v, v\rangle = 1$. Alors, $f_\tau(e_k) = e_{\tau(k)} = e_k = s_v(e_k)$ pour tout $k \in [\![1,n]\!] \setminus \{i, j\}$, vu que $\langle v, e_k\rangle = 0$ dans ce cas. En outre,

$$f_\tau(e_i) = e_{\tau(i)} = e_j = e_i - \langle v, e_i\rangle v = s_v(e_i) \text{ et } f_\tau(e_j) = e_{\tau(j)} = e_i = e_j - \langle v, e_j\rangle v = s_v(e_j).$$

En conséquence, $f_\tau = s_v$.

(*g*) Soit $\sigma = \tau_1 \circ \cdots \circ \tau_p$, avec $\tau_1, \dots, \tau_p \in \mathbb{S}_n$ des transpositions. Alors, $f_\sigma = f_{\tau_1} \circ \cdots \circ f_{\tau_p}$, d'après l'item (c), et f_{τ_i} est une réflexion orthogonale, d'après l'item précédent. Le premier item nous dit alors que $p \geq n - \mathsf{dim}(\mathsf{Ker}(f_\sigma - \mathsf{id}_E))$, tandis que l'item (e) nous dit que $p \geq n - \mathsf{dim}(\mathsf{Ker}(f_\sigma - \mathsf{id}_E)) = n - N(\sigma)$. D'après l'item (b), il est possible d'écrire $\sigma \in \mathbb{S}_n$ comme produit de $n - N(\sigma)$ transpositions. On conclut que le nombre minimal de transpositions nécessaires pour écrire $\sigma \in \mathbb{S}_n$ comme produit de transpositions est $n - N(\sigma)$.

11. *Décomposition en orbites et carré d'une permutation.*

(*a*) Décomposer en cycles le carré d'un cycle de longueur ℓ.

(*b*) Montrer que le produit de deux cycles de longueur ℓ de supports disjoints est le carré d'une permutation.

(*c*) À quelle condition, un cycle de longueur ℓ est-il le carré d'une permutation ?

(*d*) Soit $\sigma \in \mathbb{S}_n$. Décrire la décomposition en cycles de σ^2 en fonction de celle de σ.

(*e*) À quelle condition une permutation $\sigma \in \mathbb{S}_n$ est-elle un carré ?

Solution.

(a) Soit $\sigma = (a_1 \ \dots \ a_\ell) \in \mathbb{S}_n$ un cycle de longueur ℓ. Si ℓ est pair, *i.e.* $\ell = 2\ell'$ avec $\ell' \in \mathbb{N}^*$, alors on voit bien que

$$\sigma^2 = (a_1 \ a_3 \ \dots \ a_{2\ell'-3} \ a_{2\ell'-1})(a_2 \ a_4 \ \dots \ a_{2\ell'-2} \ a_{2\ell'}).$$

Si ℓ est impair, *i.e.* $\ell = 2\ell' + 1$ avec $\ell' \in \mathbb{N}$, alors on voit bien que

$$\sigma^2 = (a_1 \ a_3 \ \dots \ a_{2\ell'-1} \ a_{2\ell'+1} \ a_2 \ a_4 \ \dots \ a_{2\ell'-2} \ a_{2\ell'}).$$

Noter que $\sigma^2 = \mathrm{id}_{[\![1,n]\!]}$ si et seulement si $\ell = 2$.

(b) Soient $\sigma = (a_1 \ \dots \ a_\ell) \in \mathbb{S}_n$ et $\sigma' = (b_1 \ \dots \ b_\ell) \in \mathbb{S}_n$ deux cycles de longueur ℓ de supports disjoints. Alors, on voit bien que

$$(a_1 \ b_1 \ \dots \ a_\ell \ \ b_\ell)^2 = \sigma \circ \sigma'.$$

(c) Soit

$$\sigma = \sigma_1 \dots \sigma_k$$

la décomposition en cycles de support disjoints de $\sigma \in \mathbb{S}_n$, où σ_i a longueur $\ell_i > 1$ pour tout $i \in [\![1,k]\!]$. En conséquence,

$$\sigma^2 = \sigma_1^2 \dots \sigma_k^2.$$

Alors, σ^2 est un cycle si et seulement il existe $i_0 \in [\![1,k]\!]$ tel que $\sigma_{i_0}^2$ est un cycle et $\sigma_i^2 = \mathrm{id}_{[\![1,n]\!]}$ pour tout $i \in [\![1,k]\!] \setminus \{i_0\}$. D'après le premier item, σ_i est un 2-cycle pour tout $i \in [\![1,k]\!] \setminus \{i_0\}$, et ℓ_{i_0} est impair. En particulier, si un ℓ-cycle est un carré d'une permutation, ℓ est impair. De façon réciproque, le premier item nous dit aussi qu'un ℓ-cycle $(a_1 \ \dots \ a_\ell)$ avec $\ell = 2\ell' + 1$ impair est le carré de la permutation

$$\sigma' = (b_1 \ \dots \ b_{2\ell'+1}),$$

où $b_{2j-1} = a_j$ pour $j \in [\![1, \ell' + 1]\!]$ et $b_{2j} = a_{\ell'+j+1}$ pour $j \in [\![1, \ell']\!]$.

(d) Soit

$$\sigma = \sigma_1 \dots \sigma_k$$

la décomposition en cycles de support disjoints de $\sigma \in \mathbb{S}_n$, où σ_i a longueur $\ell_i > 1$ pour tout $i \in [\![1,k]\!]$. En conséquence,

$$\sigma^2 = \sigma_1^2 \dots \sigma_k^2.$$

D'après le premier item, on voit que $\sigma_i^2 = \mathrm{id}_{[\![1,n]\!]}$ pour tout $i \in [\![1,k]\!]$ tel que $\ell_i = 2$. En outre, si ℓ_i est impair, alors σ_i^2 est un ℓ_i-cycle. Finalement, si $\ell_i > 2$ est pair, alors σ_i^2 est un produit de deux $(\ell_i/2)$-cycle disjoints.

(e) Soit

$$\sigma = \sigma_1 \dots \sigma_k$$

la décomposition en cycles de support disjoints de $\sigma \in \mathbb{S}_n$, où σ_i a longueur $\ell_i > 1$ pour tout $i \in [\![1,k]\!]$. On pose

$$\sigma' = \prod_{\substack{i \in [\![1,k]\!] \\ \ell_i \text{ impair}}} \sigma_i \text{ et } \sigma'' = \prod_{\substack{i \in [\![1,k]\!] \\ \ell_i \text{ pair}}} \sigma_i$$

Si ℓ_i est impair, il existe d'après l'item précédent $\rho_i \in \mathbb{S}_n$ tel que $\rho_i^2 = \sigma_i$, ce qui nous dit que

$$\sigma' = \Big(\prod_{\substack{i \in [\![1,k]\!] \\ \ell_i \text{ impair}}} \rho_i\Big)^2.$$

Alors, σ est un carré si et seulement si σ'' est un carré. Soit $P = \{\ell_i : i \in [\![1,k]\!] \text{ et } \ell_i \text{ pair}\}$. Pour tout $\ell \in P$, soit $E_\ell = \{i \in [\![1,k]\!] : \ell_i = \ell\} \neq \emptyset$ et

$$\sigma''_\ell = \prod_{\substack{i \in [\![1,k]\!] \\ \ell_i = \ell}} \sigma_i.$$

Si $\#(E_\ell)$ est pair, on pose $\bar{\sigma}''_\ell = \sigma''_\ell$, et si $\#(E_\ell)$ est impair, on pose $\bar{\sigma}''_\ell = \sigma''_\ell \sigma_{i_\ell}^{-1}$, où $i_\ell = \min(E_\ell)$. Soit $P' = \{\ell \in P : \#(E_\ell) \text{ est impair}\}$. En outre, d'après l'item (b), on voit bien que $\bar{\sigma}''_\ell$ est un carré, ce qui nous dit que σ'' est un carré si et seulemen si

$$\bar{\sigma}'' = \prod_{\ell \in P'} \sigma_{i_\ell}.$$

est un carré. D'après l'item précédent, $\bar{\sigma}''$ est un carré si et seulement si $\bar{\sigma}'' = \mathrm{id}_{[\![1,n]\!]}$, car la quantité de cycles de longueur paire dans un carré est pair. En conclusion, σ est un carré si et seulement si son type $\mathrm{type}(\sigma)$ satisfait que $\mathrm{type}(\sigma)(2j)$ est pair pour tout $j \in \mathbb{N}^*$.

12. *Classes de conjugaison de* $\mathbb{S}_5$.

(a) Faire la liste des classes de conjugaison de $\mathbb{S}_5$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe.

(b) En déduire les sous-groupes distingués de $\mathbb{S}_5$.

(c) Montrer que dans $\mathbb{A}_5$, les 3-cycles, les produits de deux transpositions de supports disjoints et les 5-cycles forment respectivement une, une et deux classes de conjugaison. En déduire les sous-groupes distingués de $\mathbb{A}_5$.

Solution.

(a) On reprend la notation de l'exercice **3**. On remarque que $\#(\mathscr{F}_5) = 7$,

$$\begin{aligned}\mathbb{S}_5/\sim = \Big\{&\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}), \mathrm{cl}(1\ 2), \mathrm{cl}(1\ 2\ 3), \mathrm{cl}(1\ 2\ 3\ 4), \mathrm{cl}(1\ 2\ 3\ 4\ 5),\\ &\mathrm{cl}(1\ 2)(3\ 4), \mathrm{cl}(1\ 2)(3\ 4\ 5)\Big\},\end{aligned}$$

$\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}) = \{\mathrm{id}_{[\![1,5]\!]}\}$ a cardinal 1,

$$\mathrm{cl}(1\ 2) = \Big\{(1\ 2), (1\ 3), (1\ 4), (1\ 5), (2\ 3), (2\ 4), (2\ 5), (3\ 4), (3\ 5), (4\ 5)\Big\}$$

possède 10 éléments, $\mathrm{cl}(1\ 2\ 3)$ et $\mathrm{cl}(1\ 2)(3\ 4\ 5)$ possèdent 20 éléments, $\mathrm{cl}(1\ 2\ 3\ 4)$ a cardinal 30, $\mathrm{cl}(1\ 2\ 3\ 4\ 5)$ possède 24 éléments et $\mathrm{cl}(1\ 2)(3\ 4)$ a cardinal 15. En plus, $\mathrm{ord}(\mathrm{id}_{[\![1,5]\!]}) = 1$, $\mathrm{ord}(1\ 2) = \mathrm{ord}(1\ 2)(3\ 4) = 2$, $\mathrm{ord}(1\ 2\ 3) = 3$, $\mathrm{ord}(1\ 2\ 3\ 4) = 4$, $\mathrm{ord}(1\ 2\ 3\ 4\ 5) = 5$, $\mathrm{ord}(1\ 2)(3\ 4\ 5) = 6$, et

$$\begin{aligned}\epsilon(\mathrm{id}_{[\![1,5]\!]}) &= -\epsilon(1\ 2) = \epsilon\big((1\ 2)(3\ 4)\big) = \epsilon(1\ 2\ 3) = -\epsilon(1\ 2\ 3\ 4)\\ &= \epsilon(1\ 2\ 3\ 4\ 5) = -\epsilon\big((1\ 2)(3\ 4\ 5)\big) = 1.\end{aligned}$$

(b) Les sous-groupes $\{1_G\}$ et G d'un groupe G sont toujours distingués. En particulier, $\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]})$ et $\mathbb{S}_5$ sont des sous-groupes distingués de $\mathbb{S}_5$. On va considérer maintenant des sous groupes distingués non triviaux. En outre, c'est clair qu'un sous-groupe normal non trivial H de G est une réunion d'orbites de G sous l'action adjointe incluant l'orbite de 1_G. On suppose alors que H est une réunion de $p \in \mathbb{N}^*$ orbites sous l'action adjointe, incluant l'orbite de $\mathrm{id}_{[\![1,5]\!]}$. Pour les cas $p = 2$ et $p = 3$, on note que, comme les diviseurs positifs propres de $|\mathbb{S}_5| = 120$ sont $2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60$, une vérification immédiate donne que l'ordre de $\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}) \cup \mathrm{cl}(x) \cup \mathrm{cl}(y)$ n'est pas un diviseur de $|\mathbb{S}_5| = 120$ pour tous $x, y \in \mathbb{S}_5 \setminus \{\mathrm{id}_{[\![1,5]\!]}\}$, sauf dans le cas $x = (1\ 2)(3\ 4)$ et $y = (1\ 2\ 3\ 4\ 5)$ à permutation près, mais $S = \mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}) \cup \mathrm{cl}(x) \cup \mathrm{cl}(y)$ n'est pas un sous-groupe de $\mathbb{S}_5$ dans ce cas, car $(1\ 2\ 3\ 4\ 5)(1\ 2)(3\ 4) = (1\ 3\ 5) \notin S$. Si $p \geq 3$, les seules possibles réunions d'orbites dont l'odre soit un diviseur de 120 sont $S = [\mathrm{id}_{[\![1,5]\!]}] \cup \mathrm{cl}(x) \cup \mathrm{cl}(y) \cup \mathrm{cl}(z)$ avec

(C.1) $x = (1\ 2)(3\ 4)$, $y = (1\ 2\ 3\ 4\ 5)$ et $z = (1\ 2\ 3)$,

(C.2) $x = (1\ 2)(3\ 4)$, $y = (1\ 2\ 3\ 4\ 5)$ et $z = (1\ 2)(3\ 4\ 5)$,

à permutation près. Par contre, le même calcul que précédemment nous dit que S n'est pas un sous-groupe de $\mathbb{S}_5$ dans le cas (C.2). Dans le cas (C.1), $S = \mathbb{A}_5$, qui est un sous-groupe distingué de $\mathbb{S}_5$. En conclusion, les sous-groupes distingués de $\mathbb{S}_5$ sont $\{\mathrm{id}_{[\![1,5]\!]}\}$, $\mathbb{A}_5$ et $\mathbb{S}_5$.

(c) Étant donné $\sigma \in \mathbb{A}_n$, pour éviter les confusions on notera $\mathrm{cl}_{\mathbb{A}_n}(\sigma) = \{\rho\sigma\rho^{-1} : \rho \in \mathbb{A}_n\}$ sa classe de conjugaison dans $\mathbb{A}_n$ et $\mathrm{cl}_{\mathbb{S}_n}(\sigma) = \{\rho\sigma\rho^{-1} : \rho \in \mathbb{S}_n\}$ sa classe de conjugaison dans $\mathbb{S}_n$. C'est clair que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \subseteq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ pour tout $\sigma \in \mathbb{A}_n$. Soit

$$\sigma = \omega_1 \dots \omega_k \tag{7}$$

la décomposition de σ en cycles disjoints de longueur supérieure ou égal à 1. On écrira $\ell_i \in \mathbb{N}^*$ la longueur du cycle σ_i pour $i \in [\![1, k]\!]$. Noter que $\ell_1 + \dots + \ell_k = n$.

On affirme que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \neq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ si et seulement si $\mathrm{type}(\sigma)(2i - 1) \leq 1$ et $\mathrm{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$. Pour le démontrer on note d'abord que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) = \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ si et seulement s'il existe $\rho \in \mathbb{S}_n \setminus \mathbb{A}_n$ tel que $\rho\sigma\rho^{-1} = \sigma$, *i.e.* σ et ρ commutent. En effet, s'il existe un tel ρ, alors, étant donné $\rho' \in \mathbb{S}_n \setminus \mathbb{A}_n$, on voit que $\rho'\sigma\rho'^{-1} = \rho'\sigma\rho\rho^{-1}\rho'^{-1} = (\rho'\rho)\sigma(\rho'\rho)^{-1} \in \mathrm{cl}_{\mathbb{A}_n}(\sigma)$, car $\rho'\rho \in \mathbb{A}_n$, ce qui nous dit que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \supseteq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$. De façon réciproque, si $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \supseteq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$, alors, étant donné $\rho' \in \mathbb{S}_n \setminus \mathbb{A}_n$, il existe $\bar{\rho} \in \mathbb{A}_n$ tel que $\rho'\sigma\rho'^{-1} = \bar{\rho}\sigma\bar{\rho}^{-1}$, ce qui nous dit que σ et $\rho = \bar{\rho}^{-1}\rho' \in \mathbb{S}_n \setminus \mathbb{A}_n$ commutent.

On montre maintenant que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \neq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ implique que $\mathrm{type}(\sigma)(2i - 1) \leq 1$ et $\mathrm{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$. Or, on note que $\mathrm{type}(\sigma)(2i - 1) \leq 1$ et $\mathrm{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$ équivaut à dire que les longuers des cycles dans (7) satisfont que $\ell_i \neq \ell_j$ pour tous $i, j \in [\![1, k]\!]$ différents et $\ell_1, \dots, \ell_k$ sont impaires. La condition complémentaire équivaut donc à dire qu'il existe $i \in [\![1, k]\!]$ tel que ℓ_i est pair, ou il existe $i, j \in [\![1, k]\!]$ différents tels que $\ell_i = \ell_j$ est impair. Dans le premier cas $\rho = \sigma_i \in \mathbb{S}_n \setminus \mathbb{A}_n$ commute avec σ, et dans le deuxième cas, si $\sigma_i = (a_1\ \dots\ a_\ell)$ et $\sigma_j = (b_1\ \dots\ b_\ell)$ la paermutation $\rho = (a_1\ b_\ell)\dots(a_\ell\ b_\ell) \in \mathbb{S}_n \setminus \mathbb{A}_n$ commute avec σ, où $\ell = \ell_i = \ell_j$. On conclut que, s'il existe $i \in [\![1, k]\!]$ tel que ℓ_i est pair, ou il existe $i, j \in [\![1, k]\!]$ différents tels que $\ell_i = \ell_j$ est impair, alors $\mathrm{cl}_{\mathbb{A}_n}(\sigma) = \mathrm{cl}_{\mathbb{A}_n}(\sigma)$.

Finalement, on montre que $\mathrm{type}(\sigma)(2i-1) \leq 1$ et $\mathrm{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$ implique que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \neq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$. Dans ce cas, d'après l'exercice **16**, un élément ρ de $\mathbb{S}_n$ commute avec σ si et seulement si $\rho = \prod_{i=1}^{k} \sigma_i^{r_i}$, pour $r_i \in \mathbb{N}$. Cela implique que tout élément qui commute avec σ est dans $\mathbb{A}_n$, ce qui implique que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \neq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$.

Si $\mathrm{cl}_{\mathbb{A}_n}(\sigma) \neq \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ pour $\sigma \in \mathbb{A}_n$, *i.e.* $\mathrm{type}(\sigma)(2i-1) \leq 1$ et $\mathrm{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$, alors il existe $\tau \in \mathbb{S}_n \setminus \mathbb{A}_n$ tel que $\tau\sigma\tau^{-1} \notin \mathrm{cl}_{\mathbb{A}_n}(\sigma)$. L'application

$$\mathrm{cl}_{\mathbb{A}_n}(\sigma) \to \mathrm{cl}_{\mathbb{A}_n}(\tau\sigma\tau^{-1})$$

qui associe $\tau\sigma'\tau^{-1}$ à $\sigma' \in \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ est bien définie et une bijection. En effet, la surjectivité est immédiate de la définition, et l'injectivité suit du fait que $\mathrm{cl}_{\mathbb{A}_n}(\sigma) = \mathrm{cl}_{\mathbb{A}_n}(\sigma)$ si et seulement s'il existe $\rho \in \mathbb{S}_n \setminus \mathbb{A}_n$ tel que $\rho\sigma\rho^{-1} = \sigma$. En outre, c'est clair que dans ce cas

$$\mathrm{cl}_{\mathbb{S}_n}(\sigma) = \mathrm{cl}_{\mathbb{A}_n}(\sigma) \cup \mathrm{cl}_{\mathbb{A}_n}(\tau\sigma\tau^{-1}).$$

En conséquence, à partir de l'identité précédente et (2) on conclut que, si $\sigma \in \mathbb{A}_n$, on a

$$\#(\mathrm{cl}(\sigma)) = \begin{cases} \frac{n!}{2\prod_{i=1}^{n} i^{t_i} t_i!}, & \text{si } t_{2i-1} \leq 1 \text{ et } t_{2i} = 0 \text{ pour tout } i \in \mathbb{N}^*, \\ \frac{n!}{\prod_{i=1}^{n} i^{t_i} t_i!}, & \text{sinon,} \end{cases}$$

où $\mathrm{type}(\sigma)(i) = t_i$ pour tout $i \in \mathbb{N}^*$.

On voit bien que

$$\mathbb{A}_5/\sim = \Big\{ \mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}), \mathrm{cl}(1\ 2\ 3), \mathrm{cl}(1\ 2)(3\ 4), \mathrm{cl}(1\ 2\ 3\ 4\ 5), \mathrm{cl}(2\ 1\ 3\ 4\ 5) \Big\},$$

$\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}) = \{\mathrm{id}_{[\![1,5]\!]}\}$ a cardinal 1, $\mathrm{cl}(1\ 2\ 3)$ possède 20 éléments, $\mathrm{cl}(1\ 2)(3\ 4)$ a cardinal 15, et $\mathrm{cl}(1\ 2\ 3\ 4\ 5)$ et $\mathrm{cl}(2\ 1\ 3\ 4\ 5)$ possèdent 12 éléments. Comme les diviseurs positifs propres de $|\mathbb{A}_5| = 60$ sont $3, 4, 5, 12, 15, 20$, une vérification immédiate donne que l'ordre de $\mathrm{cl}(\mathrm{id}_{[\![1,5]\!]}) \cup \mathrm{cl}(x) \cup \mathrm{cl}(y) \cup \mathrm{cl}(z)$ n'est pas un diviseur de $|\mathbb{A}_5| = 60$ pour tous $x, y, z \in \mathbb{A}_5 \setminus \{\mathrm{id}_{[\![1,5]\!]}\}$. En conclusion, les sous-groupes distingués de $\mathbb{A}_5$ sont $\{\mathrm{id}_{[\![1,5]\!]}\}$ et $\mathbb{A}_5$, *i.e.* $\mathbb{A}_5$ est un groupe simple.

De façon plus générale, on va démontrer le résultat suivant.

> $\mathbb{A}_n$ est un groupe simple pour tout entier positif $n \neq 4$ (pour le cas $n = 4$, voir l'exercice **14**, (b)).

En effet, si $n \in \{1, 2, 3\}$, alors $\mathbb{A}_n \simeq \mathbb{Z}/n\mathbb{Z}$, qui n'a pas de sous groupes non triviaux dans ce cas. Il suffit donc de démontrer que $\mathbb{A}_n$ est un groupe simple pour tout entier $n \geq 5$ Pour démonter ce résultat on note d'abord que $\mathbb{A}_n$ est engendré par les 3-cycles si $n \geq 3$. En effet, il suffit de montrer que toute permutation σ de la forme $(a\ b)(c\ d)$ peut s'écrire comme un produit de 3-cycles. Si $\{a, b\} = \{c, d\}$, $\sigma = \mathrm{id}_{[\![1,5n]\!]}$, et donc $\sigma = \rho\rho^{-1}$ pour n'importe quel 3-cycle ρ. Si $\#(\{a, b\} \cap \{c, d\}) = 1$, disons $a = c$, alors $\sigma = (a\ d\ b)$. Si $\{a, b\} \cap \{c, d\} = \emptyset$ (en particulier, $n \geq 4$), alors $\sigma = (a\ b\ c)(b\ c\ d)$. En conclusion, $\mathbb{A}_n$ est engendré par les 3-cycles si $n \geq 3$. Par ailleurs, on affirme aussi que tous les 3-cycles son conjugués dans $\mathbb{A}_n$ si $n \geq 5$. En effet, étant donné deux 3-cycles $(a\ b\ c)$ et $(a'\ b'\ c')$, il existe $\gamma \in \mathbb{S}_n$ tel que $\gamma(a\ b\ c)\gamma^{-1} = (a'\ b'\ c')$. Si $\epsilon(\gamma) = 1$, alors $(a\ b\ c)$ et $(a'\ b'\ c')$ sont conjugués dans $\mathbb{A}_n$. Si $\epsilon(\gamma) = -1$, alors $\gamma' = \gamma(d\ e) \in \mathbb{A}_n$ pour $d, e \notin \{a, b, c\}$ différents satisfait que $\gamma'(a\ b\ c)\gamma'^{-1} = (a'\ b'\ c')$.

Finalement, soit $H \subseteq \mathbb{A}_n$ un sous-groupe normal différent de $\{\mathrm{id}_{[\![1,n]\!]}\}$. Par les résultats dans le paragraphe précédent, il suffit de montrer qu'il existe un 3-cycle dans H. Soit $\sigma \in H$ différent de $\mathrm{id}_{[\![1,n]\!]}$ avec un quantité maximal de points fixes. Soit

$$\sigma = \omega_1 \ldots \omega_k \tag{8}$$

la décomposition de σ en cycles disjoints de longueur strictément supérieure à 1. Si la longueur de tous les cycles précédents est 2, alors $k \geq 2$. Suppons dans ce cas que $\sigma_1 = (a\ b)$ et $\sigma_2 = (c\ d)$, et soit $e \in [\![1,n]\!] \setminus \{a, b, c, d\}$. Alors, $\hat{\sigma} = (c\ d\ e)\sigma(c\ d\ e)^{-1}\sigma^{-1} \in H$, car c'est le produit de $(c\ d\ e)\sigma(c\ d\ e)^{-1} \in H$ et $\sigma^{-1} \in H$, $\hat{\sigma}(a) = a$, $\hat{\sigma}(b) = b$ et $\hat{\sigma}(i) = i$ pour tout point fixe i de σ différent de e. Comme $\hat{\sigma} \neq \mathrm{id}_{[\![1,n]\!]}$, vu que $\hat{\sigma}(c) = e$, et $\hat{\sigma}$ a plus de points fixes que σ, on trouve une contradiction. L'absurde nous dit qu'il existe un cycle dans (8) de longueur supérieur ou égal à 3. On suppose sans perte de généralité que c'est σ_1, que son support inclut l'ensemble $\{a,b,c\}$ de cardinal 3 et que $\sigma(a)=b$ et $\sigma(b)=c$. Si $\sigma \neq (a\ b\ c)$, il existe $d,e \notin \{a,b,c\}$ différents tels que $\sigma(d)\neq d$ et $\sigma(e)\neq e$. Soit $\hat{\sigma}=(c\ d\ e)\sigma(c\ d\ e)^{-1}\sigma^{-1}$. On remarque que, comme précédemment, $\hat{\sigma}\in H$, $\hat{\sigma}(a)=a$ et $\hat{\sigma}(i)=i$ pour tout point fixe i de σ. Comme $\hat{\sigma}\neq \mathrm{id}_{[\![1,n]\!]}$, vu que $\hat{\sigma}(c)=e$, et $\hat{\sigma}$ a plus de points fixes que σ, on trouve une contradiction. En conséquence, $\sigma=(a\ b\ c)$, comme on voulait démontrer.

13. *Sous-groupes distingués de* $\mathbb{S}_n$ *pour* $n\in\mathbb{N}^*\setminus\{4\}$. Soit n un entier positif avec $n\neq 4$. Le but de cet exercice est de montrer que les sous-groupes distingués de $\mathbb{S}_n$ sont $\{\mathrm{id}_{[\![1,n]\!]}\}$, $\mathbb{A}_n$ et $\mathbb{S}_n$.

(a) Soit H un sous-groupe distingué de $\mathbb{S}_n$. Montrer que $H\cap\mathbb{A}_n=\{\mathrm{id}_{[\![1,n]\!]}\}$ ou $H\cap\mathbb{A}_n=\mathbb{A}_n$.

(b) Montrer que si $H\cap\mathbb{A}_n=\mathbb{A}_n$ alors $H=\mathbb{A}_n$ ou $H=\mathbb{S}_n$.

(c) Montrer que si $H\cap\mathbb{A}_n=\{1\}$ alors $|H|=1$ ou $|H|=2$ (utiliser la restriction à H du morphisme signature). Montrer que $\mathbb{S}_n$ ne peut pas contenir de sous-groupe distingué de cardinal 2 et conclure.

Solution. Noter que les trois groupes $\{\mathrm{id}_{[\![1,n]\!]}\}$, $\mathbb{A}_n$ et $\mathbb{S}_n$ coïncident si $n=1$, $\{\mathrm{id}_{[\![1,2]\!]}\}=\mathbb{A}_2\neq\mathbb{S}_2$, et ils sont les trois différents si $n\geq 3$.

(a) Ce résultat suit facilement du résultat mentionné dans l'exercice **12**, (c), qui dit que le groupe $\mathbb{A}_n$ est simple pour tout entier positif $n\neq 4$. En effet, si $H\subseteq\mathbb{S}_n$ est un sous-groupe distingué, $H'=H\cap\mathbb{A}_n$ est un sous-groupe distingué de $\mathbb{A}_n$, *i.e.* $H'=\mathbb{A}_n$ ou $H'=\{\mathrm{id}_{[\![1,n]\!]}\}$.

(b) Si $H'=\mathbb{A}_n$, *i.e.* $\mathbb{A}_n\subseteq H$, alors $[\mathbb{S}_n:H]\leq[\mathbb{S}_n:\mathbb{A}_n]=2$, ce qui implique que $[\mathbb{S}_n:H]=1$, *i.e.* $H=\mathbb{S}_n$, ou $[\mathbb{S}_n:H]=2$, *i.e.* $H=\mathbb{A}_n$.

(c) Si $H'=\{\mathrm{id}_{[\![1,n]\!]}\}$ et $H\neq\{\mathrm{id}_{[\![1,n]\!]}\}$, alors $|H|=2$, vu que l'application

$$H\simeq\frac{H}{H\cap\mathbb{A}_n}\simeq\frac{H.\mathbb{A}_n}{\mathbb{A}_n}\to\frac{\mathbb{S}_n}{\mathbb{A}_n}\simeq\mathbb{Z}/2\mathbb{Z}$$

est injective et $|H|>1$. Dans ce cas, $H=\langle\sigma\rangle$, avec σ un produit d'un nombre impair de transpositions disjointes de la forme

$$\sigma=(a_1\ b_1)\dots(a_m\ b_m)$$

avec m impair et $2m\leq n$. Alors, si $m\geq 2$, $(a_1\ a_2)\sigma(a_1\ a_2)\notin H$, ce qui contredit le fait que H est normal. Si $m=1$, on choisit $a_2\notin\{a_1,b_2\}$ et $(a_1\ a_2)\sigma(a_1\ a_2)\notin H$ contredit le fait que H est normal. En conséquence, si $H'=\{\mathrm{id}_{[\![1,n]\!]}\}$ on a $H=\{\mathrm{id}_{[\![1,n]\!]}\}$. On a donc prouvé le résultat suivant.

Pour tout entier positif $n\neq 4$, les sous-groupes distingués du groupe simétrique $\mathbb{S}_n$ sont $\{\mathrm{id}_{[\![1,n]\!]}\}$, $\mathbb{A}_n$ et $\mathbb{S}_n$.

Pour le cas $n=4$, voir l'exercice **14**, (b).

14. *Sous-groupes distingués de* $\mathbb{S}_4$. Dans $\mathbb{S}_4$, on note $s_1=(1\ 2)(3\ 4)$, $s_2=(1\ 3)(2\ 4)$ et $s_3=(1\ 4)(2\ 3)$. Soient $E=\{s_1,s_2,s_3\}$ et $K=E\cup\{\mathrm{id}\}$.

(a) Faire la liste des classes de conjugaison de $\mathbb{S}_4$ en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe. En déduire que K est un sous-groupe distingué dans $\mathbb{S}_4$.

(*b*) Soit H un sous-groupe distingué de $\mathbb{S}_4$. Montrer que H est égal à $\{\mathrm{id}_{[\![1,4]\!]}\}$, K, $\mathbb{A}_4$ ou $\mathbb{S}_4$.

(*c*) Montrer que $\mathbb{S}_4/K$ n'est pas isomorphe à $\mathbb{Z}/6\mathbb{Z}$. En déduire que $\mathbb{S}_4/K$ est isomorphe à $\mathbb{S}_3$.

(*d*) En utilisant l'action par conjugaison de $\mathbb{S}_4$ sur E, construire un isomorphisme entre $\mathbb{S}_4/K$ et $\mathbb{S}_3$.

(*e*) On note $[\mathbb{A}_4, \mathbb{A}_4]$ le sous-groupe de $\mathbb{A}_4$ engendré par $\alpha \circ \beta \circ \alpha^{-1} \circ \beta^{-1}$, avec $\alpha, \beta \in \mathbb{A}_4$. Montrer que $[\mathbb{A}_4, \mathbb{A}_4] = K$.
Indication : pour l'inclusion $[\mathbb{A}_4, \mathbb{A}_4] \subseteq K$, montrer que le groupe quotient $\mathbb{A}_4/K$ est abélien. Qu'en déduit-on sur $\alpha \circ \beta \circ \alpha^{-1} \circ \beta^{-1}$ lorsque $\alpha, \beta \in \mathbb{A}_4$? Pour une autre méthode, si ρ et σ sont des éléments dans $\mathbb{A}_4$, il y a deux possibilités : soit ρ et σ sont des 3-cycles, soit ρ ou σ est dans K.

Solution.

(*a*) On reprend la notation de l'exercice **3**. On note que $\#(\mathscr{F}_4) = 5$,

$$\mathbb{S}_4/\sim = \Big\{ \mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}, \mathrm{cl}(1\ 2), \mathrm{cl}(1\ 2\ 3), \mathrm{cl}(1\ 2\ 3\ 4), \mathrm{cl}(1\ 2)(3\ 4) \Big\},$$

$\mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}) = \{\mathrm{id}_{[\![1,4]\!]}\}$ a cardinal 1, $\mathrm{cl}(1\ 2) = \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}$ et $\mathrm{cl}(1\ 2\ 3\ 4) = \{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$ possèdent 6 éléments,

$$\mathrm{cl}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}$$

a cardinal 8 et $\mathrm{cl}(1\ 2)(3\ 4) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ possède 3 éléments. En plus, $\mathrm{ord}(\mathrm{id}_{[\![1,4]\!]}) = 1$, $\mathrm{ord}(1\ 2) = \mathrm{ord}(1\ 2)(3\ 4) = 2$, $\mathrm{ord}(1\ 2\ 3) = 3$, $\mathrm{ord}(1\ 2\ 3\ 4) = 4$ et $\epsilon(\mathrm{id}_{[\![1,4]\!]}) = -\epsilon(1\ 2) = \epsilon(1\ 2\ 3) = -\epsilon(1\ 2\ 3\ 4) = 1$.

(*b*) Si l'on dénote $\sim$ la relation d'équivalence donnée par la conjugaison, on voit bien que

$$\mathbb{A}_4/\sim = \Big\{ \mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}), \mathrm{cl}(1\ 2\ 3), \mathrm{cl}(1\ 3\ 2), \mathrm{cl}(1\ 2)(3\ 4) \Big\},$$

$\mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}) = \{\mathrm{id}_{[\![1,4]\!]}\}$ a cardinal 1, $\mathrm{cl}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$ et $\mathrm{cl}(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)\}$ possède 4 éléments et $\mathrm{cl}(1\ 2)(3\ 4) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ a cardinal 3. On voit bien que $K = [\mathrm{id}_{[\![1,4]\!]}] \cup \mathrm{cl}(1\ 2)(3\ 4)$ est un sous-groupe normal de $\mathbb{A}_4$. Comme les diviseurs positifs propres de $|\mathbb{A}_4| = 12$ sont $2, 3, 4, 6, 8$, une vérification immédiate donne que l'ordre de $\mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}) \cup \mathrm{cl}(x) \cup \mathrm{cl}(y)$ n'est pas un diviseur de $|\mathbb{A}_4| = 12$ pour tous $x, y \in \mathbb{A}_4 \setminus \{\mathrm{id}_{[\![1,4]\!]}\}$ avec $x \notin \mathrm{cl}(1\ 2)(3\ 4)$ ou $y \notin \mathrm{cl}(1\ 2)(3\ 4)$. On a donc démontré le résultat suivant.

$$\boxed{\text{Les sous-groupes distingués du groupe alterné } \mathbb{A}_4 \text{ sont } \{\mathrm{id}_{[\![1,4]\!]}\},\ K = \mathrm{cl}(\mathrm{id}_{[\![1,4]\!]}) \cup \mathrm{cl}(1\ 2)(3\ 4) \text{ et } \mathbb{A}_4.}\ .$$

Soit H un sous-groupe distingué de $\mathbb{S}_4$. Alors, $H' = H \cap \mathbb{A}_4$ est un sous-groupe distingué de $\mathbb{A}_4$. D'après l'item précédent, on peut avoir $H' = \mathbb{A}_4$ (*i.e.* $\mathbb{A}_4 \subseteq H$), $H' = K$ ou $H' = \{\mathrm{id}_{[\![1,4]\!]}\}$. Si $H' = \mathbb{A}_4$, alors $[\mathbb{S}_4 : H] \leq [\mathbb{S}_4 : \mathbb{A}_4] = 2$, ce qui implique que $[\mathbb{S}_4 : H] = 1$, *i.e.* $H = \mathbb{S}_4$, ou $[\mathbb{S}_4 : H] = 2$, *i.e.* $H = \mathbb{A}_4$. Si $H' = \{\mathrm{id}_{[\![1,4]\!]}\}$ et $H \neq \{\mathrm{id}_{[\![1,4]\!]}\}$, alors $|H| = 2$, vu que l'application

$$H \simeq \frac{H}{H \cap \mathbb{A}_4} \simeq \frac{H.\mathbb{A}_4}{\mathbb{A}_4} \to \frac{\mathbb{S}_4}{\mathbb{A}_4} \simeq \mathbb{Z}/2\mathbb{Z}$$

est injective et $|H| > 1$. Dans ce cas, $H = \langle\sigma\rangle$, avec $\sigma = (a\ b)$ une transposition. On choisit $c \notin \{a, b\}$ et $(a\ c)\sigma(a\ c) \notin H$ contredit le fait que H est normal. En conséquence, si $H' = \{\mathrm{id}_{[\![1,4]\!]}\}$ on a $H = \{\mathrm{id}_{[\![1,4]\!]}\}$. Finalement, si $H' = K$, on considère le sous-groupe distingué $\varphi(K)$ de $\mathbb{S}_3$. Comme le sous-groupes distingués de $\mathbb{S}_3$ sont $\{\mathrm{id}_{[\![1,3]\!]}\}$, $\mathbb{A}_3$ et $\mathbb{S}_3$, cela nous dit que $\varphi(K) = \{\mathrm{id}_{[\![1,3]\!]}\}$, $\varphi(K) = \mathbb{A}_3$ ou $\varphi(K) = \mathbb{S}_3$, *i.e.* $H = K$, $H = \mathbb{A}_4$ ou $\mathbb{S}_4$, respectivement. On a donc démontré le résultat suivant.

$$\boxed{\text{Les sous-groupes distingués de } \mathbb{S}_4 \text{ sont } \{\mathrm{id}_{[\![1,4]\!]}\}, K, \mathbb{A}_4 \text{ et } \mathbb{S}_4.}$$

(c) C'est facile à voir que $\mathbb{S}_4/K$ n'a pas d'élément d'ordre 6. En conséquence, $\mathbb{S}_4/K$ n'est pas isomorphe à $\mathbb{Z}/6\mathbb{Z}$. D'après l'exercice **12** de la fiche 2, on déduite que $\mathbb{S}_4/K$ est isomorphe à $\mathbb{S}_3$.

(d) Étant donné $\sigma \in \mathbb{S}_4$, on définit $\varphi_\sigma : [\![1,3]\!] \to [\![1,3]\!]$ via $s_{\varphi_\sigma(i)} = \sigma s_i \sigma^{-1}$ pour tout $i \in [\![1,3]\!]$. C'est clair que $\varphi_\sigma \in \mathbb{S}_3$. En plus, comme

$$s_{(\varphi_\sigma\circ\varphi_{\sigma'})(i)} = \sigma s_{\varphi_{\sigma'}(i)}\sigma^{-1} = \sigma\sigma' s_i \sigma'^{-1}\sigma^{-1} = (\sigma\sigma')s_i(\sigma\sigma')^{-1} = s_{\varphi_{\sigma\sigma'}(i)}$$

pour tout $i \in [\![1,3]\!]$, on conlut que l'application $\varphi : \mathbb{S}_4 \to \mathbb{S}_3$ qui associe φ_σ à σ est un morphisme de groupes. En plus, comme K est un groupe abélien, c'est clair que $\varphi_\sigma = \mathrm{id}_{[\![1,3]\!]}$ pour tout $\sigma \in K$. Cela nous dit que $K \subseteq \mathrm{Ker}(\varphi)$. En outre, on voit bien que $\varphi(1\ 2) = (2\ 3)$, $\varphi(1\ 3) = (1\ 3)$ et $\varphi(1\ 4) = (1\ 2)$, ce qui nous dit que φ est surjectif. En conséquence, φ induit un morphisme surjectif de groupes $\bar{\varphi} : \mathbb{S}_4/K \to \mathbb{S}_3$. Comme les ensembles de départ et d'arrivé ont le même cardinal fini et $\bar{\varphi}$ est surjectif, alors $\bar{\varphi}$ est un isomorphisme de groupes.

(e) On rappelle d'abord que, étant donné un groupe G', on définit le **commutateur** $[G', G']$ de G' comme le sous-groupe de G' engendré par l'ensemble $\{ghg^{-1}h^{-1} : g, h \in G'\}$. C'est facile à vérifier que $[G', G']$ est un sous-groupe normal de G', car

$$k\big(ghg^{-1}h^{-1}\big)k^{-1} = kghg^{-1}k^{-1}h^{-1}hkh^{-1}k^{-1} = \Big((kg)h(kg)^{-1}h^{-1}\Big)\Big(hkh^{-1}k^{-1}\Big) \in [G, G],$$

et que $[G', G'] \neq \{1_G\}$ si et seulement si G n'est pas abélien. En plus, étant donné un morphisme de groupes $f : G' \to G$ avec G abélien, alors $[G', G'] \subseteq \mathrm{Ker}(f)$ et f induit un morphisme de groupes $\bar{f} : G'/[G', G'] \to G$ tel que $\bar{f} \circ p = f$, où $p : G' \to G'/[G', G']$ est la projection canonique. Cela implique que l'application

$$p_* : \mathrm{Hom}_{\mathrm{Gr}}(G/[G, G], G') \to \mathrm{Hom}_{\mathrm{Gr}}(G, G')$$

qui associe $p \circ g$ à $g \in \mathrm{Hom}_{\mathrm{Gr}}(G/[G, G], G')$ est une bijection.

Or, le morphisme surjectif de groupes $\varphi : \mathbb{S}_4 \to \mathbb{S}_3$ se restreint à un morphisme surjectif de groupes $\varphi' = \varphi|_{\mathbb{A}_4} : \mathbb{A}_4 \to \mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ dont le noyau est K. Comme $\mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien, $[\mathbb{A}_4, \mathbb{A}_4] \subseteq \mathrm{Ker}(\varphi') = K$. En outre, comme $[\mathbb{A}_4, \mathbb{A}_4] \neq \{\mathrm{id}_{[\![1,4]\!]}\}$, car $\mathbb{A}_4$ n'est pas abélien, et $[\mathbb{A}_4, \mathbb{A}_4]$ est normal, on conclut de l'item précédent que $[\mathbb{A}_4, \mathbb{A}_4] = K$.

De façon plus générale, on peut montrer que $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$ pour $n = 1, 2$ ou $n \geq 5$. En effet, si $n = 1$ ou $n = 2$, l'identité précédente est triviale. Si $n \geq 5$, cela suit du fait que $\mathbb{A}_n$ est simple, d'après l'exercice **12**, $[\mathbb{A}_n, \mathbb{A}_n] \neq \{\mathrm{id}_{[\![1,n]\!]}\}$, car $\mathbb{A}_n$ n'est pas abélien, et $[\mathbb{A}_n, \mathbb{A}_n]$ est normal. On remarque que $[\mathbb{A}_3, \mathbb{A}_3] = \{\mathrm{id}_{[\![1,3]\!]}\}$, car $\mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien. On a donc démontré le résultat suivant.

$$[\mathbb{A}_n, \mathbb{A}_n] = \begin{cases} \mathbb{A}_n, & \text{if } n = 1, 2 \text{ ou } n \geq 5, \\ \{\mathrm{id}_{[\![1,3]\!]}\}, & \text{if } n = 3, \\ K, & \text{if } n = 4. \end{cases}$$

15. Soient $n \geq 2$, G un groupe et $f : \mathbb{S}_n \to G$ un morphisme de groupes.

(a) Si $G = \mathbb{C}^\times$, montrer que f est soit le morphisme trivial, soit la signature.

(b) Si G est abélien, montrer que $\mathsf{Img}(f)$ est d'ordre 1 ou 2. En déduire que $\mathbb{A}_n$ est le seul sous-groupe d'indice 2 dans $\mathbb{S}_n$.

(c) On suppose ici que $n \neq 4$. Montrer que $\mathsf{Img}(f)$ est d'ordre 1, 2 ou $n!$.

(d) Soit H un sous-groupe de $\mathbb{S}_n$ tel que $[\mathbb{S}_n : H] > 2$. Montrer que $[\mathbb{S}_n : H] \geq n$. **Indication :** utiliser l'action par translation à gauche de $\mathbb{S}_n$ sur $\mathbb{S}_n/H$.

(e) Exhiber un sous-groupe d'indice n dans $\mathbb{S}_n$.

Solution.

(a) On remarque d'abord que $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$ pour tout $n \in \mathbb{N}^*$. En effet, si $n = 1$ ou $n = 2$ l'identité précédente est immédiate. En outre, le morphisme de groupes $\epsilon : \mathbb{S}_n \to \{\pm 1\}$ nous dit que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathsf{Ker}(\epsilon) = \mathbb{A}_n$ pour tout $n \in \mathbb{N}^*$. Si $n \geq 3$, $[\mathbb{S}_n, \mathbb{S}_n] \neq \{\mathsf{id}_{[\![1,n]\!]}\}$, car $\mathbb{S}_n$ n'est pas abélien. Si $n \geq 3$, on note que $(a\ b)(a\ c)(a\ b)(a\ c) = (a\ c\ b)$ pour tous $a, b, c \in \{[\![1, n]\!]$ différents, ce qui nous dit que ous les 3-cycles sont dans $[\mathbb{S}_4, \mathbb{S}_4]$. Comme les 3-cycles engendrent $\mathbb{A}_n$ pour tout $n \geq 3$, d'après l'exercice **12**, on conclut que $\mathbb{A}_n \subseteq [\mathbb{S}_n, \mathbb{S}_n]$. On a donc démontré le résultat suivant.

$$\boxed{[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n \text{ pour tout } n \in \mathbb{N}^*.}$$

Par ailleurs, on a montré dans l'exercice **14** que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathsf{Ker}(f)$ pour tout morphisme de groupes $f : \mathbb{S}_n, \mathbb{S}_n \to G$ avec G abélien, ce qui nous dit que $f = \bar{f} \circ p$, où $\bar{f} : \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n] \to G$ et $p : \mathbb{S}_n \to \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n]$ est la projection canonique. En particulier, comme a déjà expliqué, l'application

$$p_* : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n], G) \to \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{S}_n, G)$$

qui associe $g \circ p : \mathbb{S}_n \to G$ à $g : \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n] \to G$ est une bijection. Comme $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$ pour tout $n \in \mathbb{N}^*$ et $\bar{\epsilon} : \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n] \to \mathbb{Z}/2\mathbb{Z}$ est un isomorphisme de groupes, on trouve la bijection

$$p^* : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{Z}/2\mathbb{Z}, G) \to \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{S}_n, G)$$

qui associe $h \circ \epsilon : \mathbb{S}_n \to G$ à $h : \mathbb{Z}/2\mathbb{Z} \to G$. Or, on a montré dans l'exercice **19** que

$$\mathsf{ev}_{\bar{1}} : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{Z}/2\mathbb{Z}, G) \to \{g \in G : g^2 = 1_G\}$$

qui associe $h(\bar{1})$ à $h : \mathbb{Z}/2\mathbb{Z} \to G$ est un bijection. En conséquence, l'application

$$\varphi : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{S}_n, G) \to \{g \in G : g^2 = 1_G\}$$

qui associe $f(1\ 2)$ à $f : \mathbb{S}_n \to G$ est un bijection. Si $G = \mathbb{C}^\times$, soient $\mathsf{t} : \mathbb{S}_n \to G$ le morphisme trivial, qui associe 1 à tout $\sigma \in \mathbb{S}_n$, et $\hat{\epsilon}$ la composition de ϵ et l'inclusion $\{\pm 1\} \subseteq \mathbb{C}^\times$. Alors, $\varphi(\mathsf{t}) = 1$ et $\varphi(\hat{\epsilon}) = -1$. Comme $\{z \in \mathbb{C}^\times : z^2 = 1\}$, on conclut que t et $\hat{\epsilon}$ sont les seuls morphismes de groupes de $\mathbb{S}_n$ dans $\mathbb{C}^\times$.

(b) On a montré ce résultat dans l'item précédent. Par ailleurs, si $H \subseteq \mathbb{S}_n$ est un sous-groupe d'indice 2, alors H est normal. On considère le morphisme de groupes $\pi : \mathbb{S}_n \to \mathbb{S}_n/H = G$. Comme tout groupe d'ordre 2 est abélien, $H = \mathsf{Ker}(\pi) \supseteq [\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$, ce qui implique que $H = \mathbb{A}_n$.

(c) Il s'agit d'une conséquence immédiate de la description de sous-groupes normales de $\mathbb{S}_n$ pour $n \neq 4$ dans l'exercice **12**.

(d) Soient $H \subseteq \mathbb{S}_n$ un sous-groupe, $X = \mathbb{S}_n/H$ l'ensemble de classes d'équivalence et

$$\rho : \mathbb{S}_n \to \mathsf{Aut}_{\mathsf{Ens}}(X)$$

le morphisme de groupes qui associe $g.g'.H$ à $g'.H$. Soit $K = \mathsf{Ker}(\rho)$. On voit bien que $K \subseteq H$, car $\rho(g)(H) = H$ implique $g \in H$. Si $[\mathbb{S}_n : K] = 1$, alors $[\mathbb{S}_n : K] = 1$, tandis que si $[\mathbb{S}_n : K] = 2$, alors $[\mathbb{S}_n : K] \in \{1, 2\}$. Si $[\mathbb{S}_n : K] = n!$, *i.e.* ρ est injectif, $\rho|_H$ est aussi injectif. Comme H est un point fixe de $\rho|_H(h)$ pour tout $h \in H$, l'application

$$\rho' : H \to \mathsf{Aut}_{\mathsf{Ens}}\big(X \setminus \{H\}\big)$$

qui associe $\rho(h)|_{X\setminus\{H\}}$ à $h \in H$ est un morphisme de groupes injectif. En particulier, $|H|$ divise $(n-1)!$, ce qui nous dit que $n | [\mathbb{S}_n : H]$ et *a fortiori* $n \leq [\mathbb{S}_n : H]$.

(e) Soit $H = \{\sigma \in \mathbb{S}_n : \sigma(n) = n\}$. C'est clair que H est un sous-groupe de $\mathbb{S}_n$ et que $|H| = (n-1)!$, ce qui implique que $[\mathbb{S}_n : H] = n$.

16. Soient $n \geq \ell \geq 2$ des entiers.

(a) Quel est le sous-groupe de $\mathbb{S}_n$ engendré par les ℓ-cycles ?

(b) Combien y a-t-il de ℓ-cycles différents ?

(c) On se donne un ℓ-cycle $\gamma = (a_1 \ \ldots \ a_\ell)$ dans $\mathbb{S}_n$. Quelles sont les permutations de $\mathbb{S}_n$ qui commutent avec γ ? Combien y en a-t-il ?
Indication : pour tout $\sigma \in \mathbb{S}_n$, $\sigma \circ \gamma = \gamma \circ \sigma$ si et seulement si $\sigma \circ \gamma \circ \sigma^{-1} = \gamma$.

Solution.

(a) Soit $S_\ell \subseteq \mathbb{S}_n$ l'ensemble formé des ℓ-cycles. Comme $\gamma\sigma\gamma^{-1} \in S_\ell$ pour tout $\sigma \in S_\ell$, l'exercice **5** nous dit que $G_\ell = \langle S_\ell \rangle$ est un sous-groupe normal de $\mathbb{S}_n$, de cardinal strictément supérieur à $\#(S_\ell) \geq 1$. En particulier, $G_\ell \neq \{\mathsf{id}_{[\![1,n]\!]}\}$.

Si $\ell = 2$, on sait déjà que $G_\ell = \mathbb{S}_n$. Si $\ell = 3$ (et en particulier $n \geq 3$), alors $G_\ell = \mathbb{A}_n$, d'après l'exercice **12**. On suppose désormais que $\ell \geq 4$ (et en particulier $n \geq 4$). Si ℓ est impair, $n \geq \ell \geq 5$ et $S_\ell \subseteq \mathbb{A}_n$, ce qui implique que $G_\ell \subseteq \mathbb{A}_n$. Comme G_ℓ est normal et non trivial, $G_\ell = \mathbb{A}_n$ si ℓ est pair, d'après la charactérisation des sous-groupes distingués de $\mathbb{S}_n$ dans l'exercice **12**.

Si ℓ est pair, $n \geq \ell \geq 4$, ce qui implique que G_ℓ n'est pas inclus dans $\mathbb{A}_n$. Comme G_ℓ est normal et tous les sous-groupes distingués de $\mathbb{S}_n$ différents de $\mathbb{S}_n$ sont inclus dans $\mathbb{A}_n$, d'après l'exercice **12**, on conclut que $G_\ell = \mathbb{S}_n$ si ℓ est pair.

(b) C'est clair que $\#(S_\ell) = (\ell - 1)!$.

(c) On rappelle que σ et γ commutent si et seulement si $\sigma \circ \gamma \circ \sigma^{-1} = \gamma$. Comme $\sigma \circ (a_1 \ \ldots \ a_\ell) \circ \sigma^{-1} = (\sigma(a_1) \ \ldots \ \sigma(a_\ell))$ pour $\sigma \in \mathbb{S}_n$, on voit que σ et γ commutent si et seulement si $(a_1 \ \ldots \ a_\ell) = (\sigma(a_1) \ \ldots \ \sigma(a_\ell))$, *i.e.* il existe $k \in [\![0, \ell-1]\!]$ tel que $\sigma(a_i) = a_{i+k}$ pour $i \in [\![1, \ell-k]\!]$ et $\sigma(a_i) = a_{i-\ell+k}$ pour $i \in [\![\ell-k+1, \ell]\!]$. Cela équivaut à dire que σ peut s'écrire de façon unique sous la forme $\sigma = \gamma^{k-1}\sigma'$, où $\sigma' \in \mathbb{S}_n$ satisfait que $\sigma'(a_i) = a_i$ pour tout $i \in [\![1, \ell]\!]$. On fixe une bijection $f : [\![1, n-\ell]\!] \to [\![1, n]\!] \setminus \{a_1, \ldots, a_\ell\}$ et on considère l'application

$$\psi : \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{S}_{n-\ell} \to \mathbb{S}_n$$

qui associe $\gamma^k \circ f \circ \rho \circ f^{-1}$ à $(\bar{k}, \rho)$. C'est facile à vérifier que ψ est bien définie, injective et sont image est $\mathscr{Z}(\gamma) = \{\sigma \in \mathbb{S}_n : \sigma\gamma = \gamma\sigma\}$. En particulier, le cardinal de $\mathscr{Z}(\gamma)$ est $(n-\ell)!\ell$.

⋆ **17.** *Automorphismes de $\mathbb{S}_n$.* Soit $n \in \mathbb{N}^*$ un entier et soit

$$\mathsf{Ad} : \mathbb{S}_n \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n) \tag{9}$$

le morphisme qui associe à $\sigma \in \mathbb{S}_n$ l'automorphisme de groupes $\mathsf{Ad}(\sigma) : \mathbb{S}_n \to \mathbb{S}_n$ donné par $\mathsf{Ad}(\sigma)(\rho) = \sigma\rho\sigma^{-1}$, pour $\rho \in \mathbb{S}_n$. Le but de cet exercice est de montrer que Ad est surjectif si $n \in \mathbb{N}^* \setminus \{6\}$ et injectif si $n \in \mathbb{N}^* \setminus \{2\}$, et en particulier Ad est bijectif si $n \in \mathbb{N}^* \setminus \{2, 6\}$.

(a) Montrer que Ad est bijectif si $n = 1$ et surjectif si $n = 2$.

(b) Montrer que Ad est injectif si $n \geq 3$.

(c) Étant donné $\sigma \in \mathbb{S}_n$, on notera $[\sigma] = \{\rho\sigma\rho^{-1} : \rho \in \mathbb{S}_n\}$ la classe de conjugaison de σ. Montrer que $\varphi([\sigma]) = [\varphi(\sigma)]$, pour tous $\sigma \in \mathbb{S}_n$ et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$, et conclure que $\#([\sigma]) = \#([\varphi(\sigma)])$.

(d) On suppose désormais que $n \geq 3$. Soient $\sigma \in \mathbb{S}_n$ un 2-cycle, $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$ un automorphisme fixe et k la quantité d'orbites de $\varphi(\sigma)$ dans $[\![1, n]\!]$. Montrer que

$$\#([\sigma]) = \frac{n!}{2(n-2)!} \text{ et } \#([\varphi(\sigma)]) = \frac{n!}{2^k k!(n-2k)!}. \tag{10}$$

En déduire de cet item et de l'item précédent que l'on a ou bien $k = 1$ et $n \geq 3$, ou bien $k = 3$ et $n = 6$.

(e) On suppose désormais en plus que $n \neq 6$. En déduire de l'item précédent que si $\sigma \in \mathbb{S}_n$ est un 2-cycle et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$, alors $\varphi(\sigma)$ est un 2-cycle.

(f) Soit $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$. Montrer qu'il existe $a, b_2, \dots, b_n \in [\![1, n]\!]$ différents tels que $\varphi(1\ i) = (a\ b_i)$ pour tout $i \in [\![2, n]\!]$. Soit $\gamma \in \mathbb{S}_n$ tel que $\gamma(1) = a$, $\gamma(i) = b_i$ pour $i \in [\![2, n]\!]$. Montrer que $\varphi(\sigma) = \mathsf{Ad}(\gamma)(\sigma)$, pour tout $\sigma \in \mathbb{S}_n$.

(g) Conclure que Ad est surjectif dans ce cas.

Solution.

(a) Si $n \in \{1, 2\}$, c'est clair que le seul automorphisme de $\mathbb{S}_n$ est l'identité, qui es le seul morphisme intérieur, vu que $\mathbb{S}_n$ est commutatif dans ce cas. C'est clair alors que (9) est bijectif pour $n = 1$ et surjectif pour $n = 2$.

(b) On voit bien que (9) est injectif, vu que le noyau de Ad est le centre $\mathscr{Z}(\mathbb{S}_n)$, qui est trivial, vu qu'un élément σ est dans le centre de $\mathbb{S}_n$ si et seulement si sa classe de conjugaison est précisément $\{\sigma\}$.

(c) C'est clair que

$$\varphi\big([\sigma]\big) = \{\varphi(\rho\sigma\rho^{-1}) : \rho \in \mathbb{S}_n\} = \{\varphi(\rho)\varphi(\sigma)\varphi(\rho^{-1}) : \rho \in \mathbb{S}_n\} \subseteq \big[\varphi(\sigma)\big],$$

pour tous $\sigma \in \mathbb{S}_n$ et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$. En particulier, l'identité précédente nous dit aussi que $\varphi^{-1}([\varphi(\sigma)]) \subseteq [\varphi^{-1}(\varphi(\sigma))] = [\sigma]$, ce qui implique que $\varphi([\sigma]) = [\varphi(\sigma)]$, pour tous $\sigma \in \mathbb{S}_n$ et $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$. Par conséquent, $\#([\sigma]) = \#([\varphi(\sigma)])$, pour tout $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{S}_n)$.

(d) Soit

$$\varphi(\sigma) = \omega_1 \dots \omega_k \tag{11}$$

la décomposition de $\varphi(\sigma) \in \mathbb{S}_n$ en cycles disjoints de longueur supérieure ou égal à 1. Noter que l'indice k dans (11) est précisément la quantité d'orbites de $\varphi(\sigma)$ dans

$[\![1,n]\!]$. Comme σ a ordre 2, $\varphi(\sigma)$ a aussi ordre 2, ω_i est un 2-cycle pour tout $i \in [\![1,k]\!]$. En plus, vu que σ est un 2-cycle, $[\sigma] \subseteq \mathbb{S}_n$ est l'ensemble des 2-cycles de $\mathbb{S}_n$, qui est en bijection avec l'ensemble de parties de $[\![1,n]\!]$ de cardinalité 2. Cela nous donne la première identité de (10). Pour démontrer la dernière identité de (10) on procède de façon analogue.

L'identité $\#([\sigma]) = \#([\varphi(\sigma)])$ dans l'item précédent devient alors

$$2^{k-1} = \frac{(n-2)!}{(n-2k)!k!}. \tag{12}$$

On voit bien que $k=1$ est une solution de l'identité précédente pour tout entier $n \geq 3$. Si $k \geq 2$, on réécrit l'identité précédente sous la forme

$$2^{k-1} = \binom{n-2}{n-2k}\frac{(2(k-1))!}{k!}. \tag{13}$$

On remarque que les facteurs dans le membre de droite sont des entiers, car $k \geq 2$ implique $2(k-1) \geq k$. En plus, si $k \geq 4$, le deuxième facteurs du membre de droite est divisible par $2k-3$, ce qui est impossible pour le membre de gauche. Si $k=2$, (13) devient

$$2 = \binom{n-2}{n-4},$$

qui est impossible. En conséquence, si $k \geq 2$ on doit avoir $k=3$. Dans ce cas, (13) devient

$$1 = \binom{n-2}{n-6},$$

ce qui est équivalent à $n=6$. En conséquence, les seules solutions de (12) sont $k=1$ et $n \geq 3$, ou $k=3$ et $n=6$.

(*e*) Comme $n \neq 6$, l'item précédent nous dit que $\varphi(\sigma)$ est un 2-cycle, pour tout 2-cycle σ. On écrit alors $\varphi(1\ 2) = (a\ b)$ et, étant donné $i \in [\![3,n]\!]$, $\varphi(1\ i) = (a'\ b')$. Comme $(1\ 2)(1\ i) = (1\ 2\ i)$ pour $i \in [\![3,n]\!]$, on conclut que l'odre de $(1\ 2)(1\ i)$ est 3, ce qui implique que l'ordre de $\varphi((1\ 2)(1\ i)) = (a\ b)(a'\ b')$ est aussi 3. Cela implique que $\#(\{a,b,a',b'\}) = 3$, car si $\#(\{a,b,a',b'\}) = 2$, alors $(a\ b)(a'\ b')$ est l'identité et possède donc ordre 1, et si $\#(\{a,b,a',b'\}) = 4$, $(a\ b)(a'\ b')$ possède donc ordre 2. Comme $\#(\{a,b,a',b'\}) = 3$, on peut donc supposer sans perte de généralité que $a = a'$ et donc $\varphi(1\ i) = (a\ b')$. En conséquence, on peut écrire $\varphi(1\ i) = (a\ b_i)$ pour tout $i \in [\![2,n]\!]$, avec $b_2 = b$.

On voit bien que

$$\varphi(1\ i) = (a\ b_i) = \big(\gamma(1)\ \gamma(i)\big) = \gamma(1\ i)\gamma^{-1} \tag{14}$$

pour tout $i \in [\![2,n]\!]$. Comme le sous groupe engendré par $\{(1\ i) : i \in [\![2,n]\!]\}$ est $\mathbb{S}_n$, vu que $(1\ i) = (1\ j) = (i\ j)$ pour $i,j \in [\![2,n]\!]$ différents, (14) nous dit que $\varphi(\sigma) = \mathsf{Ad}(\gamma)(\sigma)$, pour tout $\sigma \in \mathbb{S}_n$.