
MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

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 $\mathcal{J} : \llbracket 1, m \rrbracket \rightarrow \llbracket 1, n \rrbracket$ pour $m, n \in \mathbb{N}^*$, on définit $\text{cyc}(\mathcal{J}) \in \mathbb{S}_n$ via $\sigma(i) = i$ pour tout $i \in \llbracket 1, n \rrbracket \setminus \text{Im}(\mathcal{J})$, $\sigma(\mathcal{J}(i)) = \mathcal{J}(i+1)$ pour $i \in \llbracket 1, m-1 \rrbracket$ et $\sigma(\mathcal{J}(m)) = \mathcal{J}(1)$. On note $(\mathcal{J}(1) \dots \mathcal{J}(m))$ au lieu de $\text{cyc}(\mathcal{J})$ 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 $\text{Im}(\mathcal{J})$ est le **support** de $\text{cyc}(\mathcal{J})$. On note que l'ordre $\text{ord}(\sigma)$ d'un cycle σ de longueur m est précisément m et sa signature $\epsilon(\sigma)$ est $(-1)^{m+1}$.

Étant donné un élément $\sigma \in \mathbb{S}_n$, il existe un uplet $(\mathcal{J}^1, \dots, \mathcal{J}^k)$ avec $k \in \mathbb{N}^*$, où $\mathcal{J}^i : \llbracket 1, m_i \rrbracket \rightarrow \llbracket 1, n \rrbracket$ est une injection pour tout $i \in \llbracket 1, k \rrbracket$, $\text{Im}(\mathcal{J}^i) \cap \text{Im}(\mathcal{J}^{i'}) = \emptyset$ pour tous $i, i' \in \llbracket 1, k \rrbracket$ différents et $\llbracket 1, n \rrbracket = \cup_{i=1}^k \text{Im}(\mathcal{J}^i)$, tel que

$$\sigma = \text{cyc}(\mathcal{J}^1) \dots \text{cyc}(\mathcal{J}^k). \tag{1}$$

On appelle $(\mathcal{J}^1, \dots, \mathcal{J}^k)$, et par abus de notation (1), la **décomposition de σ en cycles disjoints**. Cette décomposition $(\mathcal{J}^1, \dots, \mathcal{J}^k)$ 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 $\text{type}(\sigma) : \mathbb{N}^* \rightarrow \mathbb{N}$ donnée par

$$\text{type}(\sigma)(i) = \#\{j \in \llbracket 1, k \rrbracket : \text{cyc}(\mathcal{J}^j) \text{ a longueur } i\}$$

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 $\text{ord}(\sigma) = 2$ 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 $\text{ord}(\sigma) = 3 \cdot 2 = 6$ 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 $\text{ord}(\sigma) = 3 \cdot 5 \cdot 4 = 60$ 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 $\text{ord}(\sigma) = 5 \cdot 4 = 20$ 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 $i \in \llbracket 1, m-1 \rrbracket$. Dans ce cas,

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

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

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

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 $A' = \llbracket 1, n \rrbracket \setminus A$ et $B' = \llbracket 1, n \rrbracket \setminus B$ ont le même cardinal, il existe une bijection $\gamma' : A \rightarrow B'$. En conséquence, l'application $\gamma : \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$ qui satisfait que $\gamma|_{A'} = \gamma'$ et qui associe b_i à a_i pour $i \in \llbracket 1, \ell \rrbracket$ est une bijection. En plus, c'est facile à vérifier que $\sigma' = \gamma \rho \gamma^{-1}$.

3. 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.

- 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 $i \in \llbracket 1, n \rrbracket$ et $j \in \llbracket 1, m \rrbracket$.
- 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 $\langle \gamma \rangle \trianglelefteq \langle \gamma, s_1 \rangle$.
- Pour des éléments a, b, c, d de $\llbracket 1, 4 \rrbracket$, deux-à-deux distincts, décomposer en cycles disjoints la permutation $((a\ b)(c\ d)) \circ ((a\ c)(b\ d))$.
- Soit $K = \{\text{id}, s_1, s_2, s_3\}$. Montrer que $\langle s_1 \rangle \trianglelefteq K$ et $K \trianglelefteq \mathbb{S}_4$, mais $\langle s_1 \rangle \not\trianglelefteq \mathbb{S}_4$.

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 $i \in \llbracket 1, n \rrbracket$ et $j \in \llbracket 1, m \rrbracket$.

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 $i \in \llbracket 1, n \rrbracket$, car cela implique que $G = \langle \{g_i : i \in \llbracket 1, n \rrbracket\} \rangle \subseteq N_H \subseteq G$, i.e. $N_G(H) = G$, qui équivaut à dire que H est normal.

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

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

où la dernière inclusion est une conséquence de l'hypothèse de départ. Comme $\text{Ad}_i^{\pm 1}(H) \subseteq H$, on conclut que $\text{Ad}_i^{\pm 1}(H) = H$, i.e. $g_i \in N_G(H)$ pour tout $i \in \llbracket 1, n \rrbracket$, 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 $K = \{\text{id}, s_1, s_2, s_3\}$ 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

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

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 $\langle s_1 \rangle \not\trianglelefteq \mathbb{S}_4$.

4. (a) Soient $p \in \mathbb{N}^*$ un nombre premier et $n \geq p$ un entier.
- Quels sont les éléments d'ordre p dans \mathbb{S}_n ?
 - 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, $\text{ord}(\sigma) = \text{PPCM}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_k))$. Comme $\text{ord}(\sigma) = p$ est premier, on conclut que $\text{ord}(\sigma_1) = \dots = \text{ord}(\sigma_k) = p$, 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 $1 < \text{ord}(\sigma_1) \leq \dots \leq \text{ord}(\sigma_k)$. Alors, $\text{ord}(\sigma) = \text{PPCM}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_k))$.

Si $n = 8$, on voit bien que $k = 2$, $\text{ord}(\sigma_1) = 2$ et $\text{ord}(\sigma_2) = 5$. 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 $\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_k)$ sont impairs, ce qui implique que

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

5. 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 $a_1, a_2 \in \llbracket 1, n \rrbracket$ 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 $(i \ i+1)$.

★ (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 $\text{ord}(\gamma^r) = n$ pour tout $r \in \llbracket 1, n-1 \rrbracket$. En effet, comme γ a ordre n , $\gamma^r \neq \text{id}_{\llbracket 1, n \rrbracket}$, ce qui nous dit que le sous-groupe $\langle \gamma^r \rangle$ engendré par γ^r a ordre strictement supérieur à 1. Comme $1 < |\langle \gamma^r \rangle| = \text{ord}(\gamma^r)$ divise n et n est premier, on conclut que $\text{ord}(\gamma^r) = n$ pour tout $r \in \llbracket 1, n-1 \rrbracket$. D'après l'exercice 4, 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 $r \in \llbracket 1, n-1 \rrbracket$ tel que $\gamma^r(a_1) = a_2$. Soit $f : \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$ l'application qui associe $\gamma^{r(i-1)}(a_1)$ à $i \in \llbracket 1, n \rrbracket$. 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

$$\text{Ad}_f : \mathbb{S}_n \rightarrow \mathbb{S}_n$$

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

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

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

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

pour tous $i \in \llbracket 1, n-1 \rrbracket$ 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 $\langle \{\gamma, \tau\} \rangle \subsetneq \mathbb{S}_4$.

- ★ 6. 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 $k \in \llbracket 1, 32 \rrbracket$.

Solution. On montre d'abord que $\sigma \in \mathbb{S}_{32}$. Par ailleurs, $\sigma : \llbracket 1, 32 \rrbracket \rightarrow \llbracket 1, 32 \rrbracket$ est bien définie, car $k \in \llbracket 1, 16 \rrbracket$ implique que $\sigma(k) = 2k \in \llbracket 2, 32 \rrbracket$ et $k \in \llbracket 17, 32 \rrbracket$ implique que $\sigma(k) = 2k - 33 \in \llbracket 1, 31 \rrbracket$. En outre, on remarque que σ est une application injective. Pour le montrer, on note d'abord que, si $\sigma(k) = \sigma(k')$ avec $k, k' \in \llbracket 1, 32 \rrbracket$, 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 $k, k' \in \llbracket 1, 16 \rrbracket$ c'est clair que $2k = \sigma(k) = \sigma(k') = 2k'$ implique $k = k'$, et si $k, k' \in \llbracket 17, 32 \rrbracket$ 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

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

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

- 7. 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 .

Indication : on pourra distinguer deux cas, suivant que a possède ou non une racine carrée dans G .

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 $\sigma_a \circ \sigma_a = \text{id}_G$, vu que $a(ax^{-1})^{-1} = axa^{-1} = x$ 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

$$\sigma_a = \omega_1 \dots \omega_k \tag{2}$$

la décomposition de $\sigma_a \in \text{Aut}_{\text{Ens}}(G)$ en cycles disjoints de longueur supérieure ou égal à 1. On remarque que la longueur de chaque cycle ω_i dans (2) coïncide avec le cardinal de l'orbite $\#\mathcal{O}_{a,x}$, pour x dans le support de ω_i . On suppose alors que σ_i a longueur 1 pour $i \in \llbracket 1, k' \rrbracket$ et longueur 2 pour $i \in \llbracket k'+1, k \rrbracket$, où $k' \in \mathbb{N}$. Pour $i \in \llbracket 1, k' \rrbracket$, soit $\{x_i\}$ le support de ω_i . En conséquence, $X_a = \{x \in G : x^2 = a\} \subseteq G$ coïncide avec $\{x_1, \dots, x_{k'}\}$ et $k = (|G| - k')/2$. C'est clair que $k' < |G|$ si $a \neq 1_G$ car dans ce cas $a \notin X_a$. On voit bien que le type $\text{type}(\sigma_a)$ de σ_a est

donné par $\text{type}(\sigma_a)(i) = 0$ si $i \in \mathbb{N} \setminus \{1, 2\}$, $\text{type}(\rho_a)(1) = k'$ et $\text{type}(\rho_a)(2) = (|G| - k')/2$. En plus,

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

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

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 $\text{ord}(\sigma_{1_G}) = 1$ dans ce cas. Si $p > 3$, alors c'est clair qu'il existe $x \in G$ tel que $x^2 = 1_G$, vu que $2 \cdot \bar{1} = 2 \neq \bar{0}$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Par conséquent, $k' < |G|$ et $\text{ord}(\sigma_a) = 2$ pour tout $a \in G$ dans ce cas.

On continue avec le cas général d'un groupe quelconque G . On considère l'application de groupes

$$\rho : G \rightarrow \text{Aut}_{\text{Ens}}(G)$$

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

$$\rho_a = \sigma_1 \dots \sigma_k \tag{3}$$

la décomposition de $\rho_a \in \text{Aut}_{\text{Ens}}(G)$ en cycles disjoints de longueur supérieure ou égal à 1. Comme la longueur de chaque cycle σ_i dans (3) coïncide avec le cardinal de l'orbite $\#\mathcal{O}_{a,x}$, pour x dans le support de σ_i , on conclut que σ_i a longueur $\text{ord}(a)$ pour tout $i \in \llbracket 1, k \rrbracket$, ce qui nous dit en particulier que $k = |G|/\text{ord}(a)$. En conséquence, le type $\text{type}(\rho_a)$ de ρ_a est donné par $\text{type}(\rho_a)(i) = 0$ si $i \neq \text{ord}(a)$ et $\text{type}(\rho_a)(\text{ord}(a)) = |G|/\text{ord}(a)$. En plus, $\text{ord}(\rho_a) = \text{ord}(a)$ et $\epsilon(\rho_a) = (-1)^{(\text{ord}(a)+1)|G|/\text{ord}(a)}$.

8. Nombre d'orbites et signature d'une permutation. Soit E un ensemble fini de cardinal $n \geq 2$. Pour tout $\sigma \in \text{Aut}_{\text{Ens}}(E)$ 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 $\epsilon(\sigma) = (-1)^{n-N(\sigma)}$. On cherche à retrouver les principales propriétés de l'invariant $\epsilon(\sigma)$ à partir de cette définition.

- (a) Soient $\sigma \in \text{Aut}_{\text{Ens}}(E)$ et la transposition $\tau = (a \ b) \in \text{Aut}_{\text{Ens}}(E)$ 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 de 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 $\epsilon(\tau \circ \sigma)$ et $\epsilon(\sigma)$?
- (b) En déduire les conséquences suivantes :
- (i) $\min(\{k \in \mathbb{N} : \sigma = \tau_1 \dots \tau_k \in \mathcal{S}_n, \tau_1, \dots, \tau_k \text{ transpositions}\}) = n - N(\sigma)$;

- (ii) si $\sigma = \tau_1 \dots \tau_k \in \mathbb{S}_n$ est une composée de k transpositions τ_1, \dots, τ_k , alors $\varrho(\sigma) = (-1)^k$;
- (iii) $\varrho(\sigma)$ 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

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

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 $k \in \llbracket 1, \ell - 1 \rrbracket$ tel que $\sigma^k(a) = b$. Soit

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

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

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

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

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

et

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

ce qui nous dit que

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

et

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

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 $i' \in \llbracket 0, \ell_1 - 1 \rrbracket$ et $(\tau \circ \sigma)^{i''}(b) = \sigma^{i''}(b)$ pour $i'' \in \llbracket 0, \ell_2 - 1 \rrbracket$, car $\sigma^{i'}(a), \sigma^{i''}(b) \notin \{a, b\}$ pour $i' \in \llbracket 1, \ell_1 - 1 \rrbracket$ et $i'' \in \llbracket 1, \ell_2 - 1 \rrbracket$. On note en plus que

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

et

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

ce qui nous dit que

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

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

- (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 $\epsilon(\tau \circ \sigma) = -\epsilon(\sigma)$.

- (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 $\sigma = \tau_1 \dots \tau_\ell$ est une factorisation de σ comme produit de transpositions, alors $N(\sigma) \geq N(\text{id}_E) - \ell = n - \ell$, i.e. $\ell \geq n - N(\sigma)$. Par conséquent,

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

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

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

pour tout $\sigma \in \text{Aut}_{\text{Ens}}(E)$. 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 $\sigma = \text{id}_E$. Dans ce cas $N(\sigma) = n$ et $k = 0 = n - n$, ce qui montre le résultat. On suppose maintenant que $k > 0$. Comme $\sigma \neq \text{id}_E$, il existe $e \in E$ tel que $\sigma(e) \neq e$. Soit $\tau = (e \ \sigma(e)) \in \text{Aut}_{\text{Ens}}(E)$ et $E' = E \setminus \{e\}$. Alors, $(\tau \circ \sigma)(e) = e$, ce qui implique que $\sigma' = (\tau \circ \sigma)|_{E'} \in \text{Aut}_{\text{Ens}}(E')$. 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 $\tau'_1, \dots, \tau'_k \in \text{Aut}_{\text{Ens}}(E')$ des transpositions de et $k = n - N(\sigma) - 1$. On considère la transposition $\tau_i \in \text{Aut}_{\text{Ens}}(E)$ tel que $\tau_i|_{E'} = \tau'_i$ et $\tau_i(e) = e$ pour tout $i \in \llbracket 1, k \rrbracket$. 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 $\text{Aut}_{\text{Ens}}(E)$ et les morphismes de groupes ϵ et ϵ coïncident dans des transpositions, on conclut que $\epsilon = \epsilon$.

9. 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 $\sigma^2 = \text{id}_{\llbracket 1, n \rrbracket}$ 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 $i \in \llbracket 1, k \rrbracket$. En conséquence,

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

Alors, σ^2 est un cycle si et seulement il existe $i_0 \in \llbracket 1, k \rrbracket$ tel que $\sigma_{i_0}^2$ est un cycle et $\sigma_i^2 = \text{id}_{\llbracket 1, n \rrbracket}$ pour tout $i \in \llbracket 1, k \rrbracket \setminus \{i_0\}$. D'après le premier item, σ_i est un 2-cycle pour tout $i \in \llbracket 1, k \rrbracket \setminus \{i_0\}$, 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 $j \in \llbracket 1, \ell' + 1 \rrbracket$ et $b_{2j} = a_{\ell'+j+1}$ pour $j \in \llbracket 1, \ell' \rrbracket$.

- (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 $i \in \llbracket 1, k \rrbracket$. En conséquence,

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

D'après le premier item, on voit que $\sigma_i^2 = \text{id}_{\llbracket 1, n \rrbracket}$ pour tout $i \in \llbracket 1, k \rrbracket$ 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 $(\ell_i/2)$ -cycles 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 $i \in \llbracket 1, k \rrbracket$. On pose

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

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

$$\sigma' = \left(\prod_{\substack{i \in \llbracket 1, k \rrbracket \\ \ell_i \text{ impair}}} \rho_i \right)^2.$$

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

$$\sigma'' = \prod_{\substack{i \in \llbracket 1, k \rrbracket \\ \ell_i = \ell}} \sigma_i.$$

Si $\#(E_\ell)$ est pair, on pose $\bar{\sigma}_\ell'' = \sigma''$, et si $\#(E_\ell)$ est impair, on pose $\bar{\sigma}_\ell'' = \sigma'' \sigma_{i_\ell}^{-1}$, 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 seulement si

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

est un carré. D'après l'item précédent, $\bar{\sigma}''$ est un carré si et seulement si $\bar{\sigma}'' = \text{id}_{\llbracket 1, n \rrbracket}$, 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 $\text{type}(\sigma)$ satisfait que $\text{type}(\sigma)(2j)$ est pair pour tout $j \in \mathbb{N}^*$.

10. Classes de conjugaison de \mathbb{S}_n .

- Faire la liste des classes de conjugaison de \mathbb{S}_3 , \mathbb{S}_4 et \mathbb{S}_5 en indiquant leur cardinal ainsi que la signature et l'ordre des éléments appartenant à cette classe.
- En déduire les sous-groupes distingués de \mathbb{S}_5 .
- 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.

- On remarque d'abord que deux permutations σ et σ' dans \mathbb{S}_n sont conjugués si et seulement si $\text{type}(\sigma) = \text{type}(\sigma')$. 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 $i \in \llbracket 1, k \rrbracket$, 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 $i \in \llbracket 1, k \rrbracket$. 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 $i \in \llbracket 1, k \rrbracket$, et σ'_i est un cycle de longueur $\ell'_i \in \mathbb{N}^*$ et de support S'_i pour tout $i \in \llbracket 1, k' \rrbracket$, la condition $\text{type}(\sigma) = \text{type}(\sigma')$ et l'exercice 2 nous disent précisément qu'il existe des bijections $\varphi : \llbracket 1, k \rrbracket \rightarrow \llbracket 1, k' \rrbracket$ (et en particulier $k = k'$) et $\gamma : \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$ telles que $\gamma(S_i) = S'_{\varphi(i)}$ et $\sigma'_{\varphi(i)} = \gamma\sigma_i\gamma^{-1}$ pour tout $i \in \llbracket 1, k \rrbracket$. 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

$$\mathcal{F}_n = \left\{ f : \mathbb{N}^* \rightarrow \mathbb{N} \text{ telle que } f \text{ a support fini et } \sum_{i \in \mathbb{N}^*} if(i) = n \right\}.$$

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

$$\text{type} : \mathbb{S}_n \rightarrow \mathcal{F}_n$$

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

$$\overline{\text{type}} : \mathbb{S}_n / \sim \rightarrow \mathcal{F}_n,$$

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 $\text{cl}(\sigma) = \{\sigma' \in \mathbb{S}_n : \sigma' \sim \sigma\}$, ou $\text{cl}\sigma$, la classe d'équivalence de σ pour la relation d'équivalence donnée \sim par la conjugaison. En outre, étant donné $\vec{t} = (t_1, \dots, t_n) \in \mathbb{N}_0^n$ tel que $\sum_{i=1}^n it_i = n$, un argument combinatoire élémentaire nous dit que

$$\#\left(\left\{\sigma \in \mathbb{S}_n : \text{type}(\sigma)(i) = t_i \text{ pour tout } i \in \llbracket 1, n \rrbracket\right\}\right) = \frac{n!}{\prod_{i=1}^n i^{t_i} t_i!}.$$

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

$$\#\text{cl}(\sigma) = \frac{n!}{\prod_{i=1}^n i^{t_i} t_i!}, \tag{4}$$

si $\text{type}(\sigma)(i) = t_i$ pour tout $i \in \llbracket 1, n \rrbracket$.

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

$$\mathbb{S}_3 / \sim = \left\{ \text{cl}(\text{id}_{\llbracket 1,3 \rrbracket}), \text{cl}(1\ 2), \text{cl}(1\ 2\ 3) \right\},$$

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

De façon analogue, $\#(\mathcal{F}_4) = 5$,

$$\mathbb{S}_4 / \sim = \left\{ \text{cl}(\text{id}_{\llbracket 1,4 \rrbracket}), \text{cl}(1\ 2), \text{cl}(1\ 2\ 3), \text{cl}(1\ 2\ 3\ 4), \text{cl}(1\ 2)(3\ 4) \right\},$$

$\text{cl}(\text{id}_{\llbracket 1,4 \rrbracket}) = \{\text{id}_{\llbracket 1,4 \rrbracket}\}$ a cardinal 1, $\text{cl}(1\ 2) = \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}$ et $\text{cl}(1\ 2\ 3\ 4) = \{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$ possèdent 6 éléments,

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

a cardinal 8 et $\text{cl}(1\ 2)(3\ 4) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ possède 3 éléments. En plus, $\text{ord}(\text{id}_{\llbracket 1,4 \rrbracket}) = 1$, $\text{ord}(1\ 2) = \text{ord}(1\ 2)(3\ 4) = 2$, $\text{ord}(1\ 2\ 3) = 3$, $\text{ord}(1\ 2\ 3\ 4) = 4$ et $\epsilon(\text{id}_{\llbracket 1,4 \rrbracket}) = -\epsilon(1\ 2) = \epsilon(1\ 2\ 3) = -\epsilon(1\ 2\ 3\ 4) = 1$.

Finalement, $\#(\mathcal{F}_5) = 7$,

$$\mathbb{S}_5 / \sim = \left\{ \text{cl}(\text{id}_{\llbracket 1,5 \rrbracket}), \text{cl}(1\ 2), \text{cl}(1\ 2\ 3), \text{cl}(1\ 2\ 3\ 4), \text{cl}(1\ 2\ 3\ 4\ 5), \right. \\ \left. \text{cl}(1\ 2)(3\ 4), \text{cl}(1\ 2)(3\ 4\ 5) \right\},$$

$\text{cl}(\text{id}_{\llbracket 1,5 \rrbracket}) = \{\text{id}_{\llbracket 1,5 \rrbracket}\}$ a cardinal 1,

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

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

$$\epsilon(\text{id}_{\llbracket 1,5 \rrbracket}) = -\epsilon(1\ 2) = \epsilon((1\ 2)(3\ 4)) = \epsilon(1\ 2\ 3) = -\epsilon(1\ 2\ 3\ 4) \\ = \epsilon(1\ 2\ 3\ 4\ 5) = -\epsilon((1\ 2)(3\ 4\ 5)) = 1.$$

- (b) Les sous-groupes $\{1_G\}$ et G d'un groupe G sont toujours distingués. En particulier, $\text{cl}(\text{id}_{\llbracket 1,5 \rrbracket})$ 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 $\text{id}_{\llbracket 1,5 \rrbracket}$. 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 $\text{cl}(\text{id}_{\llbracket 1,5 \rrbracket}) \cup \text{cl}(x) \cup \text{cl}(y)$ n'est pas un diviseur de $|\mathbb{S}_5| = 120$ pour tous $x, y \in \mathbb{S}_5 \setminus \{\text{id}_{\llbracket 1,5 \rrbracket}\}$, sauf dans le cas $x = (1\ 2)(3\ 4)$ et $y = (1\ 2\ 3\ 4\ 5)$ à permutation près, mais $S = \text{cl}(\text{id}_{\llbracket 1,5 \rrbracket}) \cup \text{cl}(x) \cup \text{cl}(y)$ 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'ordre soit un diviseur de 120 sont $S = [\text{id}_{\llbracket 1,5 \rrbracket}] \cup \text{cl}(x) \cup \text{cl}(y) \cup \text{cl}(z)$ avec

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

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

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 $\{\text{id}_{\llbracket 1,5 \rrbracket}\}$, \mathbb{A}_5 et \mathbb{S}_5 .

De façon plus générale, on peut montrer que les sous-groupes distingués de \mathbb{S}_n sont $\{\text{id}_{\llbracket 1,n \rrbracket}\}$, \mathbb{A}_n et \mathbb{S}_n pour tout entier positif $n \neq 4$. Noter que les trois groupes coïncident si $n = 1$, $\{\text{id}_{\llbracket 1,2 \rrbracket}\} = \mathbb{A}_2 \neq \mathbb{S}_2$, et ils sont les trois différents si $n \geq 3$. Ce résultat suit facilement du résultat mentionné dans l'item suivant, 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 $H' = \{\text{id}_{\llbracket 1,n \rrbracket}\}$. 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. $H = \mathbb{A}_n$. Si $H' = \{\text{id}_{\llbracket 1, n \rrbracket}\}$ et $H \neq \{\text{id}_{\llbracket 1, n \rrbracket}\}$, alors $|H| = 2$, vu que l'application

$$H \simeq \frac{H}{H \cap \mathbb{A}_n} \simeq \frac{H \cdot \mathbb{A}_n}{\mathbb{A}_n} \rightarrow \frac{\mathbb{S}_n}{\mathbb{A}_n} \simeq \mathbb{Z}/2\mathbb{Z}$$

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 $H' = \{\text{id}_{\llbracket 1, n \rrbracket}\}$ on a $H = \{\text{id}_{\llbracket 1, n \rrbracket}\}$. On a donc prouvé le résultat suivant.

Pour tout entier positif $n \neq 4$, les sous-groupes distingués du groupe symétrique \mathbb{S}_n sont $\{\text{id}_{\llbracket 1, n \rrbracket}\}$, \mathbb{A}_n et \mathbb{S}_n .

Pour le cas $n = 4$, voir l'exercice 11, (b).

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

$$\sigma = \omega_1 \dots \omega_k \tag{5}$$

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 $i \in \llbracket 1, k \rrbracket$. Noter que $\ell_1 + \dots + \ell_k = n$.

On affirme que $\text{cl}_{\mathbb{A}_n}(\sigma) \neq \text{cl}_{\mathbb{S}_n}(\sigma)$ si et seulement si $\text{type}(\sigma)(2i - 1) \leq 1$ et $\text{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$. Pour le démontrer on note d'abord que $\text{cl}_{\mathbb{A}_n}(\sigma) = \text{cl}_{\mathbb{S}_n}(\sigma)$ 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 $\rho'\sigma\rho'^{-1} = \rho'\sigma\rho\rho^{-1}\rho'^{-1} = (\rho'\rho)\sigma(\rho'\rho)^{-1} \in \text{cl}_{\mathbb{A}_n}(\sigma)$, car $\rho'\rho \in \mathbb{A}_n$, ce qui nous dit que $\text{cl}_{\mathbb{A}_n}(\sigma) \supseteq \text{cl}_{\mathbb{S}_n}(\sigma)$. De façon réciproque, si $\text{cl}_{\mathbb{A}_n}(\sigma) \supseteq \text{cl}_{\mathbb{S}_n}(\sigma)$, 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 $\text{cl}_{\mathbb{A}_n}(\sigma) \neq \text{cl}_{\mathbb{S}_n}(\sigma)$ implique que $\text{type}(\sigma)(2i - 1) \leq 1$ et $\text{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$. Or, on note que $\text{type}(\sigma)(2i - 1) \leq 1$ et $\text{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$ équivaut à dire que les longueurs des cycles dans (5) satisfont que $\ell_i \neq \ell_j$ pour tous $i, j \in \llbracket 1, k \rrbracket$ différents et ℓ_1, \dots, ℓ_k sont impaires. La condition complémentaire équivaut donc à dire qu'il existe $i \in \llbracket 1, k \rrbracket$ tel que ℓ_i est pair, ou il existe $i, j \in \llbracket 1, k \rrbracket$ 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 permutation $\rho = (a_1 \ b_1) \dots (a_\ell \ b_\ell) \in \mathbb{S}_n \setminus \mathbb{A}_n$ commute avec σ , où $\ell = \ell_i = \ell_j$. On conclut que, s'il existe $i \in \llbracket 1, k \rrbracket$ tel que ℓ_i est pair, ou il existe $i, j \in \llbracket 1, k \rrbracket$ différents tels que $\ell_i = \ell_j$ est impair, alors $\text{cl}_{\mathbb{A}_n}(\sigma) = \text{cl}_{\mathbb{S}_n}(\sigma)$.

Finalement, on montre que $\text{type}(\sigma)(2i - 1) \leq 1$ et $\text{type}(\sigma)(2i) = 0$ pour tout $i \in \mathbb{N}^*$ implique que $\text{cl}_{\mathbb{A}_n}(\sigma) \neq \text{cl}_{\mathbb{S}_n}(\sigma)$. Dans ce cas, d'après l'exercice 13, 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 $\text{cl}_{\mathbb{A}_n}(\sigma) \neq \text{cl}_{\mathbb{S}_n}(\sigma)$.

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

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

qui associe $\tau\sigma'\tau^{-1}$ à $\sigma' \in \text{cl}_{\mathbb{A}_n}(\sigma)$ est bien définie et une bijection. En effet, la surjectivité est immédiate de la définition, et l'injectivité suit du fait que $\text{cl}_{\mathbb{A}_n}(\sigma) = \text{cl}_{\mathbb{A}_n}(\tau\sigma\tau^{-1})$ 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

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

En conséquence, à partir de l'identité précédente et (6) on conclut que, si $\sigma \in \mathbb{A}_n$, on a

$$\#(\text{cl}(\sigma)) = \begin{cases} \frac{n!}{2 \prod_{i=1}^n i^{t_i} t_i!}, & \text{si } t_{2i-1} \leq 1 \text{ et } t_{2i} = 0 \text{ pour tout } i \in \mathbb{N}^*, \\ \frac{n!}{\prod_{i=1}^n i^{t_i} t_i!}, & \text{sinon,} \end{cases} \quad (6)$$

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

On voit bien que

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

$\text{cl}(\text{id}_{[1,5]}) = \{ \text{id}_{[1,5]} \}$ a cardinal 1, $\text{cl}(1\ 2\ 3)$ possède 20 éléments, $\text{cl}(1\ 2)(3\ 4)$ a cardinal 15, et $\text{cl}(1\ 2\ 3\ 4\ 5)$ et $\text{cl}(2\ 1\ 3\ 4\ 5)$ 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 $\text{cl}(\text{id}_{[1,5]}) \cup \text{cl}(x) \cup \text{cl}(y) \cup \text{cl}(z)$ n'est pas un diviseur de $|\mathbb{A}_5| = 60$ pour tous $x, y, z \in \mathbb{A}_5 \setminus \{ \text{id}_{[1,5]} \}$. En conclusion, les sous-groupes distingués de \mathbb{A}_5 sont $\{ \text{id}_{[1,5]} \}$ 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 11, (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 démontrer 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 $\{a, b\} = \{c, d\}$, $\sigma = \text{id}_{[1,5n]}$, 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 sont 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 $\{ \text{id}_{[1,n]} \}$. 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 $\text{id}_{[1,n]}$ avec un quantité maximal de points fixes. Soit

$$\sigma = \omega_1 \dots \omega_k \quad (7)$$

la décomposition de σ en cycles disjoints de longueur strictement supérieure à 1. Si la longueur de tous les cycles précédents est 2, alors $k \geq 2$. Supposons 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 $\hat{\sigma} \neq \text{id}_{[1,n]}$, 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 (7) de longueur supérieure 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 $\hat{\sigma} \neq \text{id}_{\llbracket 1, n \rrbracket}$, 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.

11. 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 $K = E \cup \{\text{id}\}$. On rappelle que K est un sous-groupe distingué dans \mathbb{S}_4 .

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

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

Indication : discuter suivant que H contient ou non un 3-cycle.

(c) 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) Étant donné $\sigma \in \mathbb{S}_4$, on définit $\varphi_\sigma : \llbracket 1, 3 \rrbracket \rightarrow \llbracket 1, 3 \rrbracket$ via $s_{\varphi_\sigma(i)} = \sigma s_i \sigma^{-1}$ pour tout $i \in \llbracket 1, 3 \rrbracket$. 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 $i \in \llbracket 1, 3 \rrbracket$, on conclut que l'application $\varphi : \mathbb{S}_4 \rightarrow \mathbb{S}_3$ qui associe φ_σ à σ est un morphisme de groupes. En plus, comme K est un groupe abélien, c'est clair que $\varphi_\sigma = \text{id}_{\llbracket 1, 3 \rrbracket}$ pour tout $\sigma \in K$. Cela nous dit que $K \subseteq \text{Ker}(\varphi)$. 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 $\tilde{\varphi} : \mathbb{S}_4/K \rightarrow \mathbb{S}_3$. Comme les ensembles de départ et d'arrivée ont le même cardinal fini et $\tilde{\varphi}$ est surjectif, alors $\tilde{\varphi}$ est un isomorphisme de groupes.

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

$$\mathbb{A}_4 / \sim = \left\{ \text{cl}(\text{id}_{\llbracket 1, 4 \rrbracket}), \text{cl}(1\ 2\ 3), \text{cl}(1\ 3\ 2), \text{cl}(1\ 2)(3\ 4) \right\},$$

$\text{cl}(\text{id}_{\llbracket 1, 4 \rrbracket}) = \{\text{id}_{\llbracket 1, 4 \rrbracket}\}$ a cardinal 1, $\text{cl}(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$ et $\text{cl}(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)\}$ possède 4 éléments et $\text{cl}(1\ 2)(3\ 4) = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ a cardinal 3. On voit bien que $K = [\text{id}_{\llbracket 1, 4 \rrbracket}] \cup \text{cl}(1\ 2)(3\ 4)$ 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 $\text{cl}(\text{id}_{\llbracket 1, 4 \rrbracket}) \cup \text{cl}(x) \cup \text{cl}(y)$ n'est pas un diviseur de $|\mathbb{A}_4| = 12$ pour tous $x, y \in \mathbb{A}_4 \setminus \{\text{id}_{\llbracket 1, 4 \rrbracket}\}$ avec $x \notin \text{cl}(1\ 2)(3\ 4)$ ou $y \notin \text{cl}(1\ 2)(3\ 4)$. On a donc démontré le résultat suivant.

Les sous-groupes distingués du groupe alterné \mathbb{A}_4 sont $\{\text{id}_{\llbracket 1, 4 \rrbracket}\}$, $K = \text{cl}(\text{id}_{\llbracket 1, 4 \rrbracket}) \cup \text{cl}(1\ 2)(3\ 4)$ 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 $H' = \{\text{id}_{[1,4]}\}$. 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 $H' = \{\text{id}_{[1,4]}\}$ et $H \neq \{\text{id}_{[1,4]}\}$, alors $|H| = 2$, vu que l'application

$$H \simeq \frac{H}{H \cap \mathbb{A}_4} \simeq \frac{H \cdot \mathbb{A}_4}{\mathbb{A}_4} \rightarrow \frac{\mathbb{S}_4}{\mathbb{A}_4} \simeq \mathbb{Z}/2\mathbb{Z}$$

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 $H' = \{\text{id}_{[1,4]}\}$ on a $H = \{\text{id}_{[1,4]}\}$. 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 $\{\text{id}_{[1,3]}\}$, \mathbb{A}_3 et \mathbb{S}_3 , cela nous dit que $\varphi(K) = \{\text{id}_{[1,3]}\}$, $\varphi(K) = \mathbb{A}_3$ 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.

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

- (c) 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

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

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

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

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

Or, le morphisme surjectif de groupes $\varphi : \mathbb{S}_4 \rightarrow \mathbb{S}_3$ se restreint à un morphisme surjectif de groupes $\varphi' = \varphi|_{\mathbb{A}_4} : \mathbb{A}_4 \rightarrow \mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ dont le noyau est K . Comme $\mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien, $[\mathbb{A}_4, \mathbb{A}_4] \subseteq \text{Ker}(\varphi') = K$. En outre, comme $[\mathbb{A}_4, \mathbb{A}_4] \neq \{\text{id}_{[1,4]}\}$, 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 10, $[\mathbb{A}_n, \mathbb{A}_n] \neq \{\text{id}_{[1,n]}\}$, car \mathbb{A}_n n'est pas abélien, et $[\mathbb{A}_n, \mathbb{A}_n]$ est normal. On remarque que $[\mathbb{A}_3, \mathbb{A}_3] = \{\text{id}_{[1,3]}\}$, car $\mathbb{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien. On a donc démontré le résultat suivant.

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

12. Soient $n \geq 2$, G un groupe et $f : \mathbb{S}_n \rightarrow G$ 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 $\text{Im}(f)$ 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 $\text{Im}(f)$ est d'ordre 1, 2 ou $n!$. En déduire que si H est un sous-groupe de \mathbb{S}_n tel que $[\mathbb{S}_n : H] > 2$, alors $[\mathbb{S}_n : H] \geq n$.

Indication : utiliser l'action par translation à gauche de \mathbb{S}_n sur \mathbb{S}_n/H .

(d) 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 $\epsilon : \mathbb{S}_n \rightarrow \{\pm 1\}$ nous dit que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \text{Ker}(\epsilon) = \mathbb{A}_n$ pour tout $n \in \mathbb{N}^*$. Si $n \geq 3$, $[\mathbb{S}_n, \mathbb{S}_n] \neq \{\text{id}_{[1, n]}\}$, 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 $a, b, c \in \llbracket 1, n \rrbracket$ différents, ce qui nous dit que tous les 3-cycles sont dans $[\mathbb{S}_n, \mathbb{S}_n]$. Comme les 3-cycles engendrent \mathbb{A}_n pour tout $n \geq 3$, d'après l'exercice 10, on conclut que $\mathbb{A}_n \subseteq [\mathbb{S}_n, \mathbb{S}_n]$. On a donc démontré le résultat suivant.

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

Par ailleurs, on a montré dans l'exercice 11 que $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \text{Ker}(f)$ pour tout morphisme de groupes $f : \mathbb{S}_n, \mathbb{S}_n \rightarrow G$ avec G abélien, ce qui nous dit que $f = \bar{f} \circ p$, où $\bar{f} : \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n] \rightarrow G$ et $p : \mathbb{S}_n \rightarrow \mathbb{S}_n/[\mathbb{S}_n, \mathbb{S}_n]$ est la projection canonique. En particulier, comme a déjà expliqué, l'application

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

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

$$p_* : \text{Hom}_{\text{Gr}}(\mathbb{Z}/2\mathbb{Z}, G) \rightarrow \text{Hom}_{\text{Gr}}(\mathbb{S}_n, G)$$

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

$$\text{ev}_1 : \text{Hom}_{\text{Gr}}(\mathbb{Z}/2\mathbb{Z}, G) \rightarrow \{g \in G : g^2 = 1_G\}$$

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

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

qui associe $f(1 \ 2)$ à $f : \mathbb{S}_n \rightarrow G$ est un bijection. Si $G = \mathbb{C}^\times$, soient $t : \mathbb{S}_n \rightarrow G$ 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, $\varphi(t) = 1$ 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 $\pi : \mathbb{S}_n \rightarrow \mathbb{S}_n/H = G$. Comme tout groupe d'ordre 2 est abélien, $H = \text{Ker}(\pi) \supseteq [\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$, ce qui implique que $H = \mathbb{A}_n$.

(c) La première partie est une conséquence immédiate de la description de sous-groupes normales de \mathbb{S}_n pour $n \neq 4$ dans l'exercice 10. Soient $H \subseteq \mathbb{S}_n$ un sous-groupe, $X = \mathbb{S}_n/H$ l'ensemble de classes d'équivalence et

$$\rho : \mathbb{S}_n \rightarrow \text{Aut}_{\text{Ens}}(X)$$

le morphisme de groupes qui associe $g.g'.H$ à $g'.H$. Soit $K = \text{Ker}(\rho)$. On voit bien que $K \subseteq H$, car $\rho(g)(H) = H$ implique $g \in H$. Si $[\mathbb{S}_n : K] = 1$, alors $[\mathbb{S}_n : H] = 1$, tandis que si $[\mathbb{S}_n : K] = 2$, alors $[\mathbb{S}_n : H] \in \{1, 2\}$. 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

$$\rho' : H \rightarrow \text{Aut}_{\text{Ens}}(X \setminus \{H\})$$

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 $n \leq [\mathbb{S}_n : H]$.

- (d) 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 $[\mathbb{S}_n : H] = n$.

13. 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 $\gamma = (a_1 \dots a_\ell)$ 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 4 nous dit que $G_\ell = \langle S_\ell \rangle$ est un sous-groupe normal de \mathbb{S}_n , de cardinal strictement supérieur à $\#(S_\ell) \geq 1$. En particulier, $G_\ell \neq \{\text{id}_{[1,n]}\}$.
 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 10. 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 caractérisation des sous-groupes distingués de \mathbb{S}_n dans l'exercice 10.
 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 10, 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 $\sigma \circ (a_1 \dots a_\ell) \circ \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_\ell))$ pour $\sigma \in \mathbb{S}_n$, on voit que σ et γ commutent si et seulement si $(a_1 \dots a_\ell) = (\sigma(a_1) \dots \sigma(a_\ell))$, i.e. il existe $k \in \llbracket 0, \ell-1 \rrbracket$ tel que $\sigma(a_i) = a_{i+k}$ pour $i \in \llbracket 1, \ell-k \rrbracket$ et $\sigma(a_i) = a_{i-\ell+k}$ pour $i \in \llbracket \ell-k+1, \ell \rrbracket$. 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 $i \in \llbracket 1, \ell \rrbracket$. On fixe une bijection $f : \llbracket 1, n-\ell \rrbracket \rightarrow \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_\ell\}$ et on considère l'application

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

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

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

$$\text{Ad} : \mathbb{S}_n \rightarrow \text{Aut}_{\text{Gr}}(\mathbb{S}_n) \tag{8}$$

le morphisme qui associe à $\sigma \in \mathbb{S}_n$ l'automorphisme de groupes $\text{Ad}(\sigma) : \mathbb{S}_n \rightarrow \mathbb{S}_n$ donné par $\text{Ad}(\sigma)(\rho) = \sigma\rho\sigma^{-1}$, 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 $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$, et conclure que $\#[\sigma] = \#[\varphi(\sigma)]$.
- (d) On suppose désormais que $n \geq 3$. Soient $\sigma \in \mathbb{S}_n$ un 2-cycle, $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$ un automorphisme fixe et k la quantité d'orbites de $\varphi(\sigma)$ dans $\llbracket 1, n \rrbracket$. Montrer que

$$\#[\sigma] = \frac{n!}{2(n-2)!} \text{ et } \#[\varphi(\sigma)] = \frac{n!}{2^k k!(n-2k)!}. \quad (9)$$

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 $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$, alors $\varphi(\sigma)$ est un 2-cycle.
- (f) Soit $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$. Montrer qu'il existe $a, b_2, \dots, b_n \in \llbracket 1, n \rrbracket$ différents tels que $\varphi(1\ i) = (a\ b_i)$ pour tout $i \in \llbracket 2, n \rrbracket$. Soit $\gamma \in \mathbb{S}_n$ tel que $\gamma(1) = a$, $\gamma(i) = b_i$ pour $i \in \llbracket 2, n \rrbracket$. Montrer que $\varphi(\sigma) = \text{Ad}(\gamma)(\sigma)$, 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 est le seul morphisme intérieur, vu que \mathbb{S}_n est commutatif dans ce cas. C'est clair alors que (8) est bijectif pour $n = 1$ et surjectif pour $n = 2$.
- (b) On voit bien que (8) est injectif, vu que le noyau de Ad est le centre $\mathcal{Z}(\mathbb{S}_n)$, 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

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

pour tous $\sigma \in \mathbb{S}_n$ et $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$. 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 $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$. Par conséquent, $\#[\sigma] = \#[\varphi(\sigma)]$, pour tout $\varphi \in \text{Aut}_{\text{Gr}}(\mathbb{S}_n)$.

- (d) Soit

$$\varphi(\sigma) = \omega_1 \dots \omega_k \quad (10)$$

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 (10) est précisément la quantité d'orbites de $\varphi(\sigma)$ dans $\llbracket 1, n \rrbracket$. Comme σ a ordre 2, $\varphi(\sigma)$ a aussi ordre 2, ω_i est un 2-cycle pour tout $i \in \llbracket 1, k \rrbracket$. 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 $\llbracket 1, n \rrbracket$ de cardinalité 2. Cela nous donne la première identité de (9). Pour démontrer la dernière identité de (9) on procède de façon analogue.

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

$$2^{k-1} = \frac{(n-2)!}{(n-2k)!k!}. \quad (11)$$

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

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

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 facteur du membre de droite est divisible par $2k-3$, ce qui est impossible pour le membre de gauche. Si $k = 2$, (12) devient

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

qui est impossible. En conséquence, si $k \geq 2$ on doit avoir $k = 3$. Dans ce cas, (12) devient

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

ce qui est équivalent à $n = 6$. En conséquence, les seules solutions de (11) 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 $i \in \llbracket 3, n \rrbracket$, $\varphi(1\ i) = (a'\ b')$. Comme $(1\ 2)(1\ i) = (1\ 2\ i)$ pour $i \in \llbracket 3, n \rrbracket$, on conclut que l'ordre 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 $i \in \llbracket 2, n \rrbracket$, avec $b_2 = b$.

On voit bien que

$$\varphi(1\ i) = (a\ b_i) = (\gamma(1)\ \gamma(i)) = \gamma(1\ i)\gamma^{-1} \quad (13)$$

pour tout $i \in \llbracket 2, n \rrbracket$. Comme le sous groupe engendré par $\{(1\ i) : i \in \llbracket 2, n \rrbracket\}$ est \mathbb{S}_n , vu que $(1\ i) = (1\ j) = (i\ j)$ pour $i, j \in \llbracket 2, n \rrbracket$ différents, (13) nous dit que $\varphi(\sigma) = \text{Ad}(\gamma)(\sigma)$, pour tout $\sigma \in \mathbb{S}_n$.