L3 Mathématiques – Site Nancy, S5 – 2021/22

Algèbre 2 – Feuille 5

Groupes de permutations

Exercice 1. On considère la permutation $\sigma \in \mathcal{S}_{10}$ définie par

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 8 & 7 & 2 & 5 & 10 & 3 & 1 & 9 \end{smallmatrix}\right).$$

(a) Décomposer σ en produit de cycles disjoints.
(b) Calculer l'ordre de σ dans $\sigma \in \mathcal{S}_{10}$.
(d) Calculer σ^{4781}.
(d) Calculer la signature de σ.

Corrigé l'exercice 1. (a) On trouve

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

et on note $\sigma_1 = (1\ 4\ 7\ 10\ 9)$, $\sigma_2 = (2\ 6\ 5)$ et $\sigma_3 = (3\ 8)$. Les trois cycles sont deux à deux disjoints d'ordre respectivement 5, 3 et 2.

(b) Puisque les cycles σ_1, σ_2 et σ_2 sont disjoints,

$$o(\sigma) = \operatorname{ppcm}(o(\sigma_1), o(\sigma_2), o(\sigma_3)) = 30$$

(b) Comme $4781 \equiv 1 \mod 5$, $4781 \equiv 2 \mod 3$ et $4781 \equiv 1 \mod 2$, on a

$$\begin{aligned} \sigma^{4781} &= \sigma_1^{4781}\sigma_2^{4781}\sigma_3^{4781} \\ &= \sigma_1\sigma_2^2\sigma_3 \\ &= \sigma_1\sigma_2^{-1}\sigma_3 \\ &= (1\ 4\ 7\ 10\ 9)(5\ 6\ 2)(3\ 8) \end{aligned}$$

(c) On a

$$\varepsilon(\sigma) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)\varepsilon(\sigma_3) = (-1)^{5-1} \times (-1)^{3-1} \times (-1)^{2-1} = -1$$

Exercice 2. Soit $\sigma \in \mathcal{S}_n$ définie par

$$\forall k \in \{1, 2, \cdots, n\},\ \sigma(k) = n + 1 - k.$$

Décomposer σ en produit de cycles deux à deux disjoints.

Corrigé l'exercice 2. La permutation σ est

$$\left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{smallmatrix}\right)$$

Si $n = 2p$ pair, alors

$$\begin{cases} \sigma(k) = 2p + 1 - k \\ \sigma^2(k) = \sigma(2p + 1 - k) = k \end{cases}$$

pour $k = 1, \cdots, p$ et $2p + 1 - k = 2p, \cdots, p + 1$. Donc

$$\sigma = (1\ 2p)(2\ 2p - 1) \cdots (p\ p + 1)$$

Si $n = 2p + 1$ impair, alors

$$\begin{cases} \sigma(k) = 2p + 2 - k \\ \sigma^2(k) = \sigma(2p + 2 - k) = k \end{cases}$$

pour $k = 1, \cdots, p$ et $2p + 2 - k = 2p + 1, \cdots, p + 2$. Donc

$$\sigma = (1\ 2p + 1)(2\ 2p) \cdots (p\ p + 2)$$

Exercice 3. On considère les deux permutations suivantes de $\mathcal{S}_8$

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{smallmatrix}\right) \text{ et } \tau = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 5 & 2 & 7 & 4 & 1 & 6 \end{smallmatrix}\right).$$

(a) Montrer que σ et τ sont conjugués.
(b) Trouver une permutation γ telle que $\tau = \gamma \circ \sigma \circ \gamma^{-1}$; combien y-a-t-il de telles permutations dans $\gamma \in \mathcal{S}_8$.

Corrigé l'exercice 3. (a) On a

$$\begin{aligned} \sigma &= (1\,2\,3\,4)(5\,6\,7\,8) \\ \tau &= (1\,3\,5\,7)(2\,8\,6\,4) \end{aligned}$$

Pour construire la permutation γ, verifiant $\tau = \sigma \circ \sigma \circ \sigma^{-1}$, il suffit de prendre par exemple

$$\begin{array}{ccc} \sigma & = & (1\,2\,3\,4)(5\,6\,7\,8) \\ \gamma & & \downarrow\downarrow\downarrow\downarrow\ \downarrow\downarrow\downarrow\downarrow \\ \tau & = & (1\,3\,5\,7)(2\,8\,6\,4) \end{array}$$

autrement dit

$$\gamma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 5 & 7 & 2 & 8 & 6 & 4 \end{smallmatrix}\right)$$

Il faut remarquer que γ n'est pas unique, En effet, si $\gamma(1\ 2\ 3\ 4)\gamma^{-1} = (1\ 3\ 5\ 7)$ alors $\gamma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 5 & 7 \end{smallmatrix}\right)$ (c-à-d-. $\gamma(1) = 1$, $\gamma(2) = 3$, $\gamma(3) = 5$ et $\gamma(4) = 7$). Or il y a 4 façon différentes d'écrires le cycle $(1\,3\,5\,7)$, soit

$$(1\,3\,5\,7) = (3\,5\,7\,1) = (5\,7\,1\,3) = (7\,1\,3\,5)$$

Il en résulte qu'il y a 4 permutations qui conjuguent les cycles $(1\,2\,3\,4)$ et $(1\,3\,5\,7)$; ce sont

$$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 5 & 7 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 5 & 7 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 5 & 7 & 1 & 3 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 7 & 1 & 3 & 5 \end{smallmatrix}\right).$$

De même, il y a 4 façons de conjuguer les cycles $(5\,6\,7\,8)$ et $(2\,8\,6\,4)$.
A toutes ce possibilités il faut ajouter 2 autres possibilités liées à l'ordre d'écriture des cycles dans la décomposition de σ. Donc au total il y a $4 \times 4 \times 2 = 32$ permutations γ possibles.

Exercice 4. Soit p un nombre premier et soit $\sigma \in \mathcal{S}_n$ d'ordre p.
(a) Montrer que les σ-orbites sont de cardinal 1 ou p.
(b) En déduire que si $n < 2p$, alors σ est un cycle.

Corrigé l'exercice 4. Soit $\sigma \in \mathcal{S}_n$ avec $o(\sigma) = p$ premier.
(a) Le sous-groupe $H = \langle\sigma\rangle$ engendré par σ est un groupe cyclique d'ordre p. On fait agir H sur l'ensemble $E = \{1, \cdots, n\}$ par $\sigma^k \cdot j = \sigma^k(j)$. Pour $j = 1, \cdots, n$ l'orbite de j est

$$\mathrm{Orb}_\sigma(j) = H \cdot j = \{\sigma^k(j), k = 0, \cdot, p-1\}$$

Donc $\mathrm{card}(\mathrm{Orb}_\sigma(j))$ divise $|H| = p$ ce qui conduit à $\mathrm{card}(\mathrm{Orb}_\sigma(j)) = 1$ ou $\mathrm{card}(\mathrm{Orb}_\sigma(j)) = p$.
(b) Supposons $n < 2p$. L'équation des classes donne

$$\begin{aligned} n &= \sum \mathrm{card}(\mathrm{Orb}_\sigma(j)) \\ &= a \times 1 + b \times p \end{aligned}$$

où a est le nombre des orbites de cardinal 1 et b celui des orbites de cardinal p. On doit avoir donc

$$n = a + bp < 2p$$

d'où $b = 0$ ou $b = 1$.
Si $b = 0$ alors toutes les orbites sont réduite à un point et $\sigma = Id$. Cas à exclure car l'ordre de σ est p. Donc $b = 1$ et il y a une seule orbite non réduite à un point ce qui conduit à dire que σest un cycle.

Exercice 5. Soit $n \geq 3$. Montrer que pour toute permutation $\sigma \in \mathcal{S}_n \setminus \{\mathrm{Id}\}$, il existe une transposition qui ne commute pas à σ.
En déduire que le centre de $\mathcal{S}_n$ est $Z(\mathcal{S}_n) = \{\mathrm{Id}\}$.

Corrigé l'exercice 5. (a) Soit $\sigma \in \mathcal{S}_n \setminus \{Id\} \simeq \mathcal{S}(E) \setminus \{Id\}$ où E est un ensemble de cardinal n. Comme $n \geq 3$, il existe $x \in E$ tel que $y := \sigma(x) \neq x$ et il existe $z \in E$ tel que $z \notin \{x, y\}$. Considérons la transposition $\tau = (y\ z)$. On a $\sigma\tau(x) = \sigma(x) = y$ et $\tau\sigma(x) = \tau(y) = z$. Donc $\sigma\tau(x) \neq \tau\sigma(x)$ et par suite $\sigma\tau \neq \tau\sigma$. Cette égalité montre que $\sigma \notin Z(\mathcal{S}_n)$. Par conséquent $Z(\mathcal{S}_n) = \{Id\}$.

Exercice 6. On se proposer de montrer que $\mathcal{S}_3$ est, à isomorphisme près, le seul groupe d'ordre 6 non abélien.
(a) Verifier que $\mathcal{S}_3$ n'est pas abélien.
(b) Montrer que $\mathcal{S}_3 = \{\tau_1^i \sigma_1^j;\ \ i = 0, 1 \text{ et } j = 0, 1, 2\}$, où $\tau_1 = (1, 2)$ et $\sigma_1 = (1, 2, 3)$.
Soit G un groupe non abélien d'ordre 6.
(c) Montrer qu'il existe $a, b \in G$ tels que $G = \{a^i b^j;\ \ i = 0, 1 \text{ et } j = 0, 1, 2\}$.
(d) Montrer que $ba = ab^2$ et $b^2 a = ab$.
(e) En déduire que l'application φ de G dans $\mathcal{S}_3$ définie par

$$\forall (i, j) \in \{0, 1\} \times \{0, 1, 2\},\ \ \varphi(a^i b^j) = \tau_1^i \sigma_1^j$$

est un isomorphisme.

Corrigé l'exercice 6. (a) $\mathcal{S}_3 = \{Id, \tau_1 := (1\ 2), \tau_2 := (1\ 3), \tau_3 := (2\ 3), \sigma_1 := (1\ 2\ 3), \sigma_2 := 1, 3, 2\}$. On remarque que $\tau_1\tau_2 = \sigma_2$ tandisque $\tau_2\tau_1 = \sigma_1$ Donc $\mathcal{S}_3$ n'est pas abélien.
(b) En dressant la table de $\mathcal{S}_3$, on peut remarquer que

$$\mathcal{S}_3 = \{\tau_1^i \sigma_1^j,\ i = 0, 1 \text{ et } j = 0, 1, 2\}$$

(c) Soit G un groupe non-abélien d'ordre 6. D'après le théorème de Cauchy, il existe $a, b \in G$ tels que $o(a) = 2$ et $o(b) = 3$. On vérifie que

$$G = \{a^i b^j,\ i = 0, 1 \text{ et } j = 0, 1, 2\}$$

En effet, les $a^i b^j$ sont deux à deux distincts : si $a^i b^j = a^{i'} b^{j'}$ alors $a^{i-i'} = b^{j'-j} \in \langle a\rangle \cap \langle b\rangle = \{e\}$ car ces deux sous-groupes ont des ordres premiers entre eux. On en déduit que $a^{i-i'} = e$ et $b^{j'-j} = e$, d'où 2 divise $i - i' \in \{-1, 0, 1\}$ et 3 divise $j' - j \in \{-2, -1, 0, 1, 2\}$ ce qui conduit à $i - i' = 0$ et $j - j' = 0$.

(d) On a $ba \in G = \{e, a, b, b^2, ab, ab^2\}$ mais $ba \notin \{e, a, b, b^2, ab\}$, donc $ba = ab^2$. En effet :
si $ba = e$, alors $b = a^{-1} = a$, ce qui n'est pas possible pour raison d'ordre;
si $ba = a$, alors $b = e$ ce qui n'est pas possible;
si $ba = b$, alors $a = e$ ce qui n'est pas possible non plus;
si $ba = b^2$, alors $a = b$, ce qui n'est pas possible pour raison d'ordre;
si $ba = ab$ alors G est abélien ce qui contredit l'hypothèse G non-abélien.

On montre de même en distinguant tous les cas que $b^2a = ab$.
(e) Soit l'application

$$\begin{array}{rccc} \varphi : & G & \to & \mathcal{S}_3 \\ & a^ib^j & \mapsto & \tau_1^i\sigma_1^j \end{array}$$

φ est surjective par définition. Comme les deux groupes G et $\mathcal{S} - n$ sont de même ordre, φ est bijective. Montrons maintenant que c'est un morphisme de groupes.
Soit $a^ib^j, a^{i'}b^{j'} \in G$. Alors d'après la question précédente,

$$(a^ib^j)(a^{i'}b^{j'}) = a^i(b^ja^{i'})b^{j'} \begin{cases} a^ib^{j+j'} & \text{si } \ i' = 0 \\ a^{i+1}b^{j'} & \text{si } \ i' = 1, j = 0 \\ a^{i+1}b^{j'+2} & \text{si } \ i' = 1, j = 1 \\ a^{i+1}b^{j'+1} & \text{si } \ i' = 1, j = 2 \end{cases}$$

donc

$$\begin{aligned} \varphi\big((a^ib^j)(a^{i'}b^{j'})\big) &= \begin{cases} \tau_1^i\sigma_1^{j+j'} & \text{si } \ i' = 0 \\ \tau_1^{i+1}\sigma_1^{j'} & \text{si } \ i' = 1, j = 0 \\ \tau_1^{i+1}\sigma_1^{j'+2} & \text{si } \ i' = 1, j = 1 \\ \tau_1^{i+1}\sigma_1^{j'+1} & \text{si } \ i' = 1, j = 2 \end{cases} \\ &= \begin{cases} \varphi(a^ib^j)\varphi(b^{j'}) & \text{si } \ i' = 0 \\ \varphi(a^i)\varphi(ab^{j'}) & \text{si } \ i' = 1, j = 0 \\ \varphi(a^ib)\varphi(ab^{j'}) & \text{si } \ i' = 1, j = 1 \\ \varphi(a^ib^2)\varphi(ab^{j'}) & \text{si } \ i' = 1, j = 2 \end{cases} \\ &= \varphi\big(a^ib^j\big)\varphi\big(a^{i'}b^{j'}\big) \end{aligned}$$

Les même propriétés sont aussi valables pour le produit $(\tau_1^i\sigma_1^j)(\tau_1^{i'}\sigma_1^{j'})$. Ce qui permet, en distinguant les 4 cas que

$$\varphi((a^ib^j)(a^{i'}b^{j'})) = (\tau_1^i\sigma_1^j)(\tau_1^{i'}\sigma_1^{j'}) = \varphi((a^ib^j))\varphi((a^{i'}b^{j'}))$$

En conclusion, φ est un isomorphisme, et $G \simeq \mathcal{S}_3$: tout groupe **non-abélien** d'ordre 6 est isomorphe à $\mathcal{S}_3$.
Notons qu'un groupe **abélien** d'ordre 6 est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Exercice 7. Soit $(i_1 \ i_2 \ \cdots \ i_r)$ un cycle de longueur paire. Montrer que σ^2 n'est pas un cycle.

Corrigé l'exercice 7. Soit $\sigma = (i_1 \ i_2 \ \cdots \ i_r)$ un cycle de longueur par $r = 2k$ avec $k \geq 1$.
Si $k = 1$, alors $r = 2$ et σ est une transposition dont le carrée est l'identité, donc pas un cycle.
Si $k \geq 2$, alors

$$\begin{aligned} \mathrm{Orb}_{\sigma^2}(i_1) &= \{i_1, i_3, \cdots, i_{2k-1}\} \\ \mathrm{Orb}_{\sigma^2}(i_2) &= \{i_2, i_4, \cdots, i_{2k}\} \end{aligned}$$

La permutation σ^2 admet donc deux orbites non-réduite à un point, et par conséquent ce n'est pas un cycle.

Exercice 8. Soit $\sigma = (x_1, x_2, \cdots, x_r)$ un r-cycle de longueur $r \geq 2$.
(a) Montrer que, pour $x \in \mathrm{Supp}(\sigma)$ et $j \in \mathbb{Z}$, on a

$$\sigma^j(x) = x \iff r \text{ divise } j$$

(b) Montrer que pour tout entier $m \in \mathbb{Z}$, on a

$$\mathrm{Supp}(\sigma^m) = \begin{cases} \emptyset & \text{si } r \text{ divise } m \\ \mathrm{Supp}(\sigma) & \text{sinon} \end{cases}$$

(c) Montrer que, pour $x \in \mathrm{Supp}(\sigma)$ et $m \in \mathbb{Z}$, on a

$$\mathrm{card}(Orb_{\sigma^m}(x)) = \frac{r}{r \wedge m}$$

(d) Montrer que pour $m \in \mathbb{Z}$ non multiple de r, σ^m est un cycle si, et seulement si, m est premier avec r.

Corrigé l'exercice 8. (a) Si r divise j, alors $\sigma^j = Id$ et $\sigma^j(x) = x$ pour tout $x \in E$.
Réciproquement, supposons $\sigma^j(x) = x$ pour $x = x_k \in \mathrm{Supp}(\sigma)$. On a

$$x_k = \sigma^j(x_k) = \sigma^{j+k+1}(x_1)$$

et en effectuant la division euclidienne de $j+k+1$ par r, on a $j+k+1 = qr+p$ avec $0 \leq p < r$, donc

$$x_k = \sigma^{qr+p}(x_1) = \sigma^p(x_1) = x_{p+1}$$

d'où $k = p+1$. Il en résulte que

$$j+k = qr+p+1 = qr+k$$

soit $j = qr$ et r divise j.

(b) Si r divise m, on a $\sigma^m = Id$ et $\mathrm{Supp}(\sigma^m) = \emptyset$.
S'il existe $x \in \mathrm{Supp}(\sigma)$ tel que $x \notin \mathrm{Supp}(\sigma^m)$ alors $\sigma^m(x) = x$ et d'après (a) r divise m. Il en résulte que si r ne divise par m, alors $\mathrm{Supp}(\sigma) \subset \mathrm{Supp}(\sigma^m)$, d'où $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^m)$ car l'autre inclusion est toujours vérifiée.

(c) Si r divise m, alors $\sigma^m = Id$ et $\mathrm{Orb}_{\sigma^m}(x) = \{x\}$ pour tout $x \in E$. Comme $r \wedge m = r$, l'égalité

$$\mathrm{card}\,(\mathrm{Orb}_{\sigma^m}(x)) = 1 = \frac{r}{r \wedge m}$$

est triviale.
Sinon, pour tout $x \in \mathrm{Supp}(\sigma)$, $\sigma^m(x) \neq x$ et $\mathrm{card}\,(\mathrm{Orb}_{\sigma^m}(x)) \geq 2$.
Soit $d = r \wedge m$, alors il existe des entiers m_1, r_1 tels que $m = dm_1$, $r = qr_1$ et $r_1 \wedge m_1 = 1$. Donc

$$(\sigma^m)^{r_1}(x) = \sigma^{m_1 d r_1}(x) = \sigma^{m_1 r}(x) = (\sigma^r)^{m_1}(x) = x$$

Soit maintenant un entier k compris entre 1 et $r_1 - 1$. Si $(\sigma^m)^k(x) = x$ alors $\sigma^{mk} = x$, donc $r = dr_1$ divise $mk = dm_1 k$ ce qui entraîne r_1 divise $m_1 k$ et r_1 divise k puisque $r_1 \wedge m_1 = 1$, ce qui est incompatible avec $1 \leq k \leq r_1 - 1$. Ainsi $(\sigma^m)^k(x) \neq x$. Il en résulte que

$$\mathrm{Orb}_{\sigma^m}(x) = \{x, \sigma^m(x), \cdots, (\sigma^m)^{r_1-1}(x)\}$$

et cette orbite est de cardinal $r_1 = \frac{r}{r \wedge m}$.

(d) Si $m \wedge r = 1$, alors

$$\begin{aligned}
&\mathrm{Supp}(\sigma^m) = \mathrm{Supp}(\sigma)\\
&\mathrm{card}\,(\mathrm{Orb}_{\sigma^m}(x_1)) = r = \mathrm{Card}\,(\mathrm{Supp}(\sigma^m))\\
&\mathrm{Orb}_{\sigma^m}(x_1) \subset \mathrm{Supp}(\sigma^m)
\end{aligned}$$

donc $\mathrm{Orb}_{\sigma^m}(x_1) \subset \mathrm{Supp}(\sigma^m)$ et σ^m est un cycle.
Sinon,

$$2 \leq \mathrm{card}\,(\mathrm{Orb}_{\sigma^m}(x_1)) = \frac{r}{r \wedge m} < r = \mathrm{card}\,(\mathrm{Supp}(\sigma^m))$$

et il y a aumoins deux σ^m-orbites non réduites à un point, donc σ^m n'est pas un cycle.

Exercice 9. Déterminer l'ordre maximal d'un élément de $\mathcal{S}_5$.

Corrigé l'exercice 9. La décomposition en cycles disjoints d'un élément de $\mathcal{S}_5 \backslash \{Id\}$ (Id est d'ordre 1) est formée soit d'un r-cycle avec $2 \leq r \leq 5$, soit d'un 2-cycle et d'un cycle d'ordre 2 ou 3 et cet ordre est au maximum 6, qui est atteint pour $(1,2)(3,4,5)$.

Exercice 10. (a) Soit G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n (donc d'indice 2). Montrer que pour tout $g \in G$, $g^2 \in H$.

(b) Montrer que $\mathcal{A}_4$ (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.

Corrigé l'exercice 10. On note τ_{ij} la transposition (i,j) dans $\mathcal{S}_4$ pour $1 \leq i \neq j \leq 4$ On a dans le groupe $\mathcal{A}_4$ les 12 éléments distincts suivants :

- l'identité ;
- les 3 éléments d'ordre 2 : $\tau_{12} \circ \tau_{34}, \tau_{13} \circ \tau_{24}, \tau_{23} \circ \tau_{14}$ (le produit de deux transpositions de supports disjoints est d'ordre 2 puisque ces transpositions commutent) ;
- les 8 éléments d'ordre 3 : $(2,3,4), (2,4,3), (1,3,4), (1,4,3),$
$(1,2,4), (1,4,2), (1,2,3)$ $(1,3,2)$ (un 3-cycle fixe un élément de $\{1,2,3,4\}$ et il y en a deux qui fixent k, pour $k = 1,2,3,4$) et on a ainsi tous les éléments puisque $\mathcal{A}_4$ est de cardinal $\frac{4!}{2} = 12$.

(a) Soit $g \in G$. Si $g \in H$, on a alors $g^2 \in H$ puisque H est un groupe. Si $g \notin H$, on a alors $gH \neq H$ et $G/H = \{H, gH\}$, ce qui nous donne la partition $G = H \cup gH$. Si $g^2 \notin H$, il est alors dans gH et s'écrit $g^2 = gk$ avec $k \in H$, ce qui entraine $g = k \in H$ qui est en contradiction avec $g \notin H$.

(b) Si H est un sous-groupe de $\mathcal{A}_4$ d'ordre 6 , on a alors $\sigma^2 \in H$ pour tout $\sigma \in \mathcal{A}_4$. Si $\sigma \in \mathcal{A}_n$ est un 3-cycle, il est alors d'ordre 3 et $\sigma^4 = \sigma$, c'est-à-dire que $\sigma = \gamma^2$ avec $\gamma = \sigma^2 = \sigma^{-1} \in \mathcal{A}_n$. Donc H va contenir tous les 3 -cycles, soit 8 éléments, ce qui n'est pas possible.

Exercice 11. Montrer que $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathcal{S}_n$ (c-à-d. stable par tout automorphisme de $\mathcal{S}_n$).

Corrigé l'exercice 11. Si φ est un automorphisme de $\mathcal{S}_n$, alors pour tout 3-cycle $\sigma \in \mathcal{A}_n, \varphi(\sigma)$ est d'ordre 3 dans $\mathcal{S}_n$. Comme $\varphi(\sigma)$ est produit de cycles et l'ordre de $\varphi(\sigma)$ est le ppcm des longueurs de ces cycles, ils sont nécessairement tous d'ordre 3 et $\varphi(\sigma) \in \mathcal{A}_n$. Comme $\mathcal{A}_n$ est engendré par les 3-cycles, on déduit que, $\varphi(\sigma) \in \mathcal{A}_n$ pour tout $\sigma \in \mathcal{A}_n$.

Exercice 12. Soit E un ensemble de cardinal $n \geq 4$. Montrer que les produits de deux transpositions disjointes sont conjugués dans $\mathcal{A}(E)$.

Corrigé l'exercice 12. Soient $\sigma = (x_1, x_2)(x_3, x_4)$ et $\sigma' = (x'_1, x'_2)(x'_3, x'_4)$ deux produits de deux transpositions disjointes. En désignant par τ une permutation dans $\mathcal{S}(E)$ telle que $\tau(x_k) = x'_k$ pour $1 \leq k \leq 4$, on a :

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau(x_1, x_2)\tau^{-1}\tau(x_3, x_4)\tau^{-1} = (\tau(x_1), \tau(x_2))(\tau(x_3), \tau(x_4)) \\ &= (x'_1, x'_2)(x'_3, x'_4) = \sigma'\end{aligned}$$

(ce qui prouve que σ et σ' sont conjuguées dans $\mathcal{S}(E)$). Si $\tau \in \mathcal{A}(E)$ c'est terminé, sinon $\gamma = (x'_3, x'_4)\tau$ est dans $\mathcal{A}(E)$ et :

$$\begin{aligned}\gamma\sigma\gamma^{-1} &= (\gamma(x_1), \gamma(x_2))(\gamma(x_3), \gamma(x_4)) \\ &= (x'_1, x'_2)(x'_4, x'_3) = \sigma'\end{aligned}$$

Exercice 13. Décomposer en produit de 3-cycle dans $\mathcal{A}_7$ la permutation

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{smallmatrix}\right).$$

Corrigé l'exercice 13. On a la décomposition en produit de transpositions :

$$\sigma = (1,2)(2,3)(3,4)(4,5)(5,6)(6,7)$$

donc $\varepsilon(\sigma) = 1$ et $\sigma \in \mathcal{A}_7$. Puis :

$$\sigma = (2,3,1)(4,5,3)(6,7,5) = (1,2,3)(3,4,5)(5,6,7)$$

Exercice 14. Le groupe $\mathcal{S}_n$ est-il isomorphe au produit direct $\mathcal{A}_n \times \{-1, 1\}$.

Corrigé l'exercice 14. Pour $n = 2$, on a $\mathcal{S}(E) \cong \{-1, 1\}$ et $\mathcal{A}(E) = \{Id_E\}$, donc $\mathcal{S}(E)$ est isomorphe au produit direct $\mathcal{A}(E) \times \{-1, 1\}$.

Pour $n = 3, \mathcal{A}(E)$ est d'ordre 3, donc cyclique et $\mathcal{A}(E) \times \{-1, 1\}$ qui est commutatif ne peut être isomorphe à $\mathcal{S}(E)$ qui ne l'est pas.

Pour $n \geq 4, \gamma = (Id, -1)$ est dans le centre de $\mathcal{A}(E) \times \{-1, 1\}$, il est d'ordre 2, donc si φ est un isomorphisme de $\mathcal{A}(E) \times \{-1, 1\}$ sur $\mathcal{S}(E)$, l'élément $\varphi(\gamma)$ serait d'ordre 2 dans le centre de $\mathcal{S}(E)$, ce qui contredit le fait que $Z(\mathcal{S}(E)) = \{Id\}$. Donc $\mathcal{S}(E)$ n'est pas isomorphe au produit direct $\mathcal{A}(E) \times \{-1, 1\}$.

Exercice 15. Soit $n \geq 5$.

(a) Montrer que deux 3-cycles sont conjugués dans $\mathcal{A}_n$.

(b) Vérifier que ce résultat n'est pas vrai pour $\mathcal{A}_4$ et $\mathcal{A}_3$.

(c) En déduire que le groupe dérivé $D(\mathcal{A}_n)$ de $\mathcal{A}_n$ (c-à-d. le groupe engendré par les commutateurs $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ où $\sigma, \tau \in \mathcal{A}_n$) est $\mathcal{A}_n$.

Corrigé l'exercice 15. (a) On sait déjà que deux 3-cycles sont conjugués dans $\mathcal{S}(E)$ (exercice 3.2). Soient $\gamma = (x_1, x_2, x_3)$ et $\gamma' = (x'_1, x'_2, x'_3)$ deux 3 -cycles. On se donne une permutation $\sigma \in \mathcal{S}(E)$ telle que $\sigma(x_k) = x'_k$ pour $k = 1, 2, 3$ et on a alors $\gamma' = \sigma\gamma\sigma^{-1}$. Si $\sigma \in \mathcal{A}(E)$, c'est terminé, sinon en prenant x_4, x_5 dans $E \backslash \{x_1, x_2, x_3\}$ (E a au moins 5 éléments), la permutation $\sigma' = (x_4, x_5)\sigma$ est dans $\mathcal{A}(E)$ avec $\sigma'(x_k) = x'_k$ pour $k = 1, 2, 3$ et on est ramené au cas précédent.

(b) Ce résultat n'est pas valable pour $n = 4$. Si $\gamma = (1, 2, 3)$ et $\gamma' = (2, 3, 4)$ sont conjugués dans $\mathcal{A}_4$, il existe $\sigma \in \mathcal{A}_4$ telle que $(2, 3, 4) = \sigma\gamma\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ et on a nécessairement $\sigma(4) = 1$. On parcourant la liste des éléments de $\mathcal{A}_4$ (exercice 3.18), on voit que $\sigma = \tau_{23} \circ \tau_{14}$, ou $\sigma = (1, 3, 4)$, ou $\sigma = (1, 2, 4)$ et $\sigma\gamma\sigma^{-1} = (4, 3, 2) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (3, 2, 4) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (2, 4, 3) \neq \gamma'$. Les cycles γ et γ' ne sont pas conjugués dans $\mathcal{A}_4$

(c) Comme $\mathcal{A}(E)$ est engendré par les 3 -cycles, il suffit de montrer que tout 3 -cycle est dans $D(\mathcal{A}(E))$. Si γ est un 3 -cycle, il en est de même de $\gamma^{-1} = \gamma^2$, donc γ^2 est conjugué à γ dans $\mathcal{A}(E), c'$ est-à-dire qu'il existe $\sigma \in \mathcal{A}(E)$ tel que $\gamma^2 = \sigma^{-1}\gamma\sigma$ et $\gamma = \gamma^{-1}\sigma^{-1}\gamma\sigma \in D(\mathcal{A}(E))$

Exercice 16. Déterminer, pour $n \geq 4$, le centre $Z(\mathcal{A}_n)$ de $\mathcal{A}_n$.

Corrigé l'exercice 16. Soit E un ensemble de cardinal $n \geq 4$.

Si $\sigma \in \mathcal{A}(E) \backslash \{ \text{ Id } \}$, il existe $x \in E$ tel que $y = \sigma(x) \neq x$. On se donne $z \in E \backslash \{x, y, \sigma(y)\}$ (E a au moins 4 éléments) et γ est le 3-cycle $\gamma = (x, y, z) \in \mathcal{A}(E)$. On a alors :

$$\sigma\gamma(x) = \sigma(y) \text{ et } \gamma\sigma(x) = \gamma(y) = z \neq \sigma(y)$$

donc $\sigma\gamma \neq \gamma\sigma$ et $\sigma \notin Z(\mathcal{A}(E))$. Le centre de $\mathcal{A}(E)$ est donc réduit à $\{Id\}$.

Pour $n = 3$, $\mathcal{A}(E)$ est cyclique (d'ordre 3), donc commutatif et $Z(\mathcal{A}(E)) = \mathcal{A}(E)$.

Exercice 17. Soit $n \geq 5$. Montrer que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\text{Id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Corrigé l'exercice 17. Voir Théorème 6.6 du chapitre 5.

Exercice 18. On se propose de montrer que le groupe alterné $\mathcal{A}_5$ est simple (c-à-d. n'a pas de sous-groupes distingués autres que lui même et $\{\text{Id}\}$).

(a) Donner une description de $\mathcal{A}_5$ en classant ses éléments en fonction de leur ordre.

(b) Montrer que $\mathcal{A}_5$ est un groupe simple.

Corrigé l'exercice 18. Voir Théorème 6.8 du chapitre 5.