DM n° 14 : Groupes, anneaux

Correction du problème 1 –

1. Soit A un pseudo-anneau
   (a) • Par définition, $C(A) \subset A$, et de façon évidente, $O \in C(A)$.
   • Étant donné $(x, y) \in C(A)$, pour tout $z \in A$,
   $$(x-y)z = xz - yz = zx - yx = (z-y)x,$$
   donc $x - y \in C(A)$.
   Ainsi, $\boxed{C(A) \text{ est un sous-groupe de } (A, +).}$
   (b) Soit I un idéal bilatère de A. Par définition, I est un sous-groupe additif de A. Par ailleurs, pour tout $(x, y) \in I$, $xy \in I$. Ainsi, I est stable par $\times$, ce qui permet de définir une loi de multiplication induite par *times* sur I. L'associativité de cette loi et sa distributivité sur $+$ découlent alors des propriétés similaires sur A.
   Ainsi, $\boxed{I \text{ est un pseudo-anneau.}}$
   Remarquez qu'en revanche, si A est un anneau, I n'est en général pas un anneau, mais seulement un pseudo-anneau.
2. Soit A un pseudo-anneau vérifiant : $\forall x \in A, \quad x^2 - x \in C(A)$.
   (a) Soit $(x, y) \in A^2$. On a :
   $$(x+y)^2 - (x+y) = (x^2 - x) + (y^2 - y) + xy + yx.$$
   Comme $(x+y)^2 - (x+y) \in C(A)$, $x^2 - x \in C(A)$, $y^2 - y \in C(A)$, et comme $C(A)$ est un sous-groupe additif de A, il en résulte que $\boxed{xy + yx \in C(A).}$
   (b) En particulier, $xy + yx$ commute avec x, donc
   $$x(xy + yx) = (xy + yx)x \qquad \text{puis:} \qquad x^2y + xyx = xyx + yx^2,$$
   donc $x^2y = yx^2$.
   Par ailleurs, puisque $x^2 - x \in C(A)$,
   $$(x^2 - x)y = y(x^2 - x) \qquad \text{donc:} \qquad x^2y - xy = yx^2 - yx,$$
   ce qui amène enfin, après simplifications : $xy = yx$
   Ainsi, $\boxed{A \text{ est commutatif}}$.

Dans la suite, A désigne un anneau *tel que pour tout $x \in A$, $x^3 = x$. On veut prouver que A est commutatif.*

2. On a $(2 \cdot 1_A)^3 = 2 \cdot 1_A$ par hypothèse, donc $8 \cdot 1_A = 2 \cdot 1_A$ donc $\boxed{6 \cdot 1_A = 0}$.
3. On note $2A = \{2 \cdot a \mid a \in A\}$ et $3A = \{3 \cdot a \mid a \in A\}$. Prouver les assertions suivantes :
   (a) Soit $x \in 3A \cap 2A$. Il existe donc deux éléments a et b de A tels que $x = 3a$ et $x = 2b$. On a donc :
   $$2x = 6a = 0 \qquad \text{et} \qquad 3x = 6b = 0,$$
   d'après la question précédente, donc $x = 3x - 2x = 0$. Comme réciproquement $0 \in 3A \cap 2A$, on obtient bien $\boxed{3A \cap 2A = \{0\}}$.
   (b) Montrons que $3A$ est un sous-groupe additif de A.

- Par stabilité de A, $3A \subset A$ et de façon évidente, $0 \in 3A$.
- Soit $(x, y) \in (3A)^2$. Il existe a et b dans A tels que $x = 3a$, $y = 3b$, donc

$$x - y = 3(a - b) \in 3A.$$

Ainsi, $3A$ est un sous-groupe additif de A. Par ailleurs, pour tout $x \in A$ et $y \in 3A$, soit a tel que $y = 3a$. On a alors :

$$xy = 3xa \in 3A \qquad \text{et} \qquad yx = 3ax \in 3A.$$

Ainsi, $\boxed{3A \text{ est un idéal bilatère de } A}$.

Évidemment la même preuve montre que $\boxed{2A \text{ est un idéal bilatère de } A}$.

(c)
- Pour tout $a \in A$, $a = 3a + 2(-a)$, donc a s'écrit comme somme d'un élément de $3A$ et d'un élément de $2A$.
- Supposons que $a = 3b + 2c$ et $a = 3b' + 2c'$, où a, b, c, b', c' sont des éléments de A. On a alors, en effectuant la différence :

$$3(b - b') = 2(c' - c) \in 3A \cap 2A = \{0\},$$

donc $3(b - b') = 0$ et $2(c - c') = 0$, d'où $3b = 3b'$ et $2c = 2c'$, ce qui prouve l'unicité de la décomposition.

Ainsi, $\boxed{\text{tout } a \text{ de } A \text{ s'écrit de façon unique comme somme d'un élément de } 3A \text{ et d'un élément de } 2A.}$

(d) Soit $x \in 3A$ et $y \in 2A$. Écrivons $x = 3a$ et $y = 2b$. On a alors

$$xy = 6ab = 0 \qquad \text{et} \qquad yx = 6ba = 0.$$

Donc : $\boxed{\forall x \in 3A,\ \forall y \in 2A,\ xy = yx = 0}$.

4. (a)
- Soit $x \in 3A$. Écrivons $x = 3a$. On a alors

$$2x = 6a = 0.$$

- On en déduit en particulier que pour tout $x \in 3A$, $x = 3x$, donc, en utilisant la formule du binôme (x et 1_A commutent), et la stabilité de $3A$ par produit :

$$x - 1 = (x - 1)^3 = x^3 - 3x^2 + 3x - 1 = x^3 - x^2 + x - 1 = x - x^2 + x - 1,$$

d'où : $x - x^2 = 0$, soit $\boxed{x = x^2.}$

(b) Soit $(x, y) \in (3A)^2$. On a donc $(x + y) \in 3A$, donc

$$x + y = (x + y)^2 = x^2 + y^2 + xy + yx = x + y + xy + yx,$$

et après simplifications, $xy + yx = 0$. Or, $3A$ étant un idéal, $yx \in 3A$, donc $2yx = 0$, d'où $\boxed{xy = yx}$.

On aurait aussi pu répondre à cette question en remarquant que l'égalité $x^2 - x = 0$ entraîne $x^2 - x \in C(3A)$, puis appliquer la question 2 au pseudo-anneau $3A$.

5. Soit x et y dans $2A$. On a :

$$(x + y)^3 = x^3 + x^2y + xyx + yx^2 + xy^2 + yxy + y^2x + y^3$$

et de même :

$$(x - y)^3 = x^3 - x^2y - xyx - yx^2 + xy^2 + yxy + y^2x - y^3$$

En effetuant la somme des deux expressions, il vient :

$$2(x^3 + xy^2 + yxy + y^2x) = 0.$$

Comme par ailleurs, $2A$ est un idéal, $x^3 + xy^2 + yxy + y^2x \in 2A$, donc peut s'écrire sous la forme $2a$, ce qui implique

$$3(x^3 + xy^2 + yxy + y^2x) = 6a = 0.$$

Ainsi, en faisant la différence des deux expressions obtenues,

$$x^3 + xy^2 + yxy + y^2x = 0.$$

On en déduit que $x + xy^2 + yxy + y^2x = 0$. En multipliant cette expression d'une part à gauche, d'autre part à droite par y, on obtient d'une part :

$$0 = xy + xy^3 + yxy^2 + y^2xy = 2xy + yxy^2 + y^2xy,$$

et d'autre part :

$$0 = yx + yxy^2 + y^2xy + y^3x = 2yx + yxy^2 + y^2xy.$$

On en déduit que $2xy = 2yx$, et comme xy et yx sont éléments de $2A$, on obtient, par un argument déjà utilisé, $\boxed{xy = yx}$.

6. Soit a et b dans A. On décompose $a = x + y$, où $x \in 3A$ et $y \in 2A$, et $b = x' + y'$ où $x' \in 3A$ et $y' \in 2A$. On a alors d'après 4(d), $xy' = yx' = 0 = x'y = y'x$, et d'après 5(b) et 6, $xx' = x'x$ et $yy' = y'y$. Ainsi :

$$ab = (x + y)(x' + y') = xx' + yy' + xy' + yx' = x'x + y'y + x'y + y'x = (x' + y')(x + y) = ba.$$

Ainsi, $\boxed{A \text{ est commutatif.}}$

Correction du problème 2 – Simplicité de $\mathfrak{A}_n$

Préliminaire

1. Soit τ_1 et τ_2 deux transpositions.
   - Si elles ont même support, alors $\tau_1 = \tau_2$ donc $\tau_1 \circ \tau_2 = \mathrm{id}$, qui peut être vu par exemple comme la composée $(1\ 2\ 3) \circ (1\ 3\ 2)$.
   - Si l'intersection de leur support est un singleton, il existe i, j et k deux à deux distincts tels que

     $$\tau_1 = (i\ j) \qquad \text{et} \qquad \tau_2 = (i\ k).$$

     Alors

     $$\tau_1 \circ \tau_2 = (i\ j) \circ (i\ k) = (i\ k\ j).$$

   - Si les supports de τ_1 et τ_2 sont disjoints, il existe i, j, k ℓ deux à deux distincts tels que

     $$\tau_1 = (i\ j) \qquad \text{et} \qquad \tau_2 = (k\ \ell).$$

     On vérifie facilement que

     $$(i\ j) \circ (k\ \ell) = (i\ j\ k) \circ (k\ \ell\ j).$$

   Ainsi, $\boxed{\text{toute composition de 2 transpositions est un 3-cycle ou une composée de deux 3-cycles.}}$
2. Soit $\sigma \in \mathfrak{A}_n$. Il existe une décomposition de σ en un nombre pair de transpositions :

   $$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2k}.$$

   Chaque composée $\tau_{2i-1} \circ \tau_{2i}$, pour $i \in [\![1, k]\!]$, s'écrit comme produit de 3-cycles, donc σ s'écrit également comme produit de 3-cycles.
   Ainsi, $\boxed{\text{les 3-cycles engendrent } \mathfrak{A}_n.}$

Partie I – Conjugaison

On dit que deux permutations τ_1 et τ_2 de $\mathfrak{S}_n$ sont conjuguées s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$.

1. - Soit $\sigma \in \mathfrak{S}_n$. On a alors $\mathrm{id} \circ \sigma \circ \mathrm{id}^{-1} = \sigma$, donc σ est conjuguée avec elle-même. La relation de conjugaison est donc réflexive.
   - Soit τ_1 et τ_2 tels que τ_2 soit conjugué à τ_1, c'est-à-dire qu'il existe σ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$. On a alors $\tau_1 = \sigma^{-1} \circ \tau_2 \circ \sigma$, donc τ_1 est conjugué de τ_2 (par $\sigma' = \sigma^{-1}$). Ainsi, la relation de conjugaison est symétrique.
   - Soit τ_1, τ_2 et τ_3 tels que τ_1 et τ_2 sont conjugués ainsi que τ_2 et τ_3. Il existe donc σ_2 et σ_2 tels que

     $$\tau_2 = \sigma_1\tau_1\sigma_1^{-1} \qquad \text{et} \qquad \tau_3 = \sigma_2\tau_2\sigma_2^{-1} \qquad \text{donc:} \qquad \tau_3 = (\sigma_2\sigma_1)\tau_1(\sigma_2\sigma_1)^{-1},$$

     donc τ_3 est conjugué de τ_1 (par $\sigma_2\sigma_1$). Ainsi la relation est transitive.

   $\boxed{\text{La relation de conjugaison est donc une relation d'équivalence.}}$

2. Soit $\tau_1 = (i_1\ i_2\ \cdots\ i_k)$ un cycle, et $\tau_2 = \sigma\tau_1\sigma^{-1}$.
   - Soit $\ell \in [\![1,k]\!]$. On a alors (en notant par convention $i_{k+1} = i_1$

$$\tau_2(\sigma(i_\ell)) = \sigma \circ \tau_1 \circ \sigma^{-1} \circ \sigma(i_\ell) = \sigma \circ \tau_1(ß_\ell)\sigma(i_{\ell+1}).$$

     Ainsi, $(\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$ est un cycle de τ_2.
   - Montrons qu'il s'agit du seul cycle non trivial. Soit pour cela $i \notin \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)\}$. On en déduit que $\sigma^{-1}(i) \notin \{i_1, i_2, \ldots, i_k\}$, et donc $\sigma^{-1}(i)$ est un point fixe de τ_1. Ainsi,

$$\tau_2(i) = \sigma\tau_1(\sigma^{-1}(i)) = \sigma(\sigma^{-1}(i)) = i.$$

     Ainsi, i est un point fixe de σ.
   - On en déduit que $(\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$ est le seul sycle non trivial de τ_2, donc

$$\boxed{\tau_2 = \sigma\tau_1\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))}.$$

3. - Soit τ_1 et τ_2 deux permutations, conjuguées par σ. Soit $\tau_1 = C_1 \circ \cdots \circ C_s$ la décomposition en cycles à supports disjoints de τ_1. On a alors :

$$\tau_2 = \sigma\tau_1\sigma^{-1} = (\sigma C_1\sigma^{-1}) \circ (\sigma C_2\sigma^{-1}) \circ \cdots \circ (\sigma C_s\sigma^{-1}).$$

     D'après la question précédente, les $\sigma C_i\sigma^{-1}$ sont des cycles de même longueur que C_i, et, σ étant bijective, l'expression trouvée dans la question précédente pour ces cycles montrent que leurs supports forment aussi une partition de $[\![1,n]\!]$. Ainsi, il s'agit de la décomposition en cycles à supports disjoints de τ_2. Les longueurs de ces cycles étant les mêmes que ceux de τ_1, on en déduit que τ_1 et τ_2 ont même type cyclique.
   - Réciproquement, soit τ_1 et τ_2 deux permutations de même type cyclique. Comme les produits de cycles à supports disjoints sont commutatifs, on peut alors trouver deux décompositions en cycles à supports disjoints (et formant une partition de $[\![1,n]\!]$:

$$\tau_1 = C_1 \circ \cdots \circ C_k \qquad \text{et} \qquad \tau_2 = D_1 \circ \cdots \circ D_k$$

     tels que pour tout $i \in [\![1,k]\!]$, les cycles C_i et D_i soient de même longueur. On peut donc trouver une suite $0 = \ell_1 < \ell_1 < \ell_2 < \cdots < \ell_k = n$ et deux suites finies d'éléments de $[\![1,n]\!]$: $i_1, \ldots, i_n$ et $j_1, \ldots, j_n$ tels que pour tout ß $\in [\![1,k]\!]$,

$$C_i = (i_{\ell_{i-1}+1}\ \cdots\ i_{\ell_i}) \qquad \text{et} \qquad D_i = (j_{\ell_{i-1}+1}\ \cdots\ j_{\ell_i}).$$

     Comme par ailleurs, les supports des C_i forment une partition de $[\![1,n]\!]$, la suite $(i_s)_{s\in[\![1,n]\!]}$ représente en fait une permutation des éléments de $[\![1,n]\!]$. De même pour $(j_s)_{s\in[\![1,n]\!]}$. On définit alors de façon unique une permutation σ de $[\![1,n]\!]$, en posant, pour tout $s \in [\![1,n]\!]$, $\sigma(i_s) = j_s$. La description de la question précédente permet alors d'affirmer que pour tout $i \in [\![1,k]\!]$,

$$D_i = \sigma C_i\sigma^{-1}, \qquad \text{puis:} \qquad \tau_2 = (\sigma C_1\sigma^{-1}) \cdots (\sigma C_k\sigma^{-1}) = \sigma\tau_2\sigma^{-1}.$$

     Ainsi, τ_1 et τ_2 sont conjugués.

Ainsi, $\boxed{\text{deux permutations sont conjuguées dans } \mathfrak{S}_n \text{ si et seulement si elles ont même type cyclique.}}$

Partie II – Simplicité de $\mathfrak{A}_5$

1. On pose σ' dans $\mathfrak{S}_n$ définie pour tout $i \in [\![1,n]\!]$ par $\sigma'(a_i) = b_i$. Si σ' est pair, on pose $\sigma = \sigma'$ et sinon, $\sigma = \sigma' \circ (a_{n-1}\ a_n)$. Alors $\boxed{\sigma \text{ est paire}}$ et

$$\boxed{\forall i \in [\![1,n-2]\!],\ \ \sigma(a_i) = b_i}.$$

2. Soit $(a_1\ a_2\ a_3)$ et $(b_1\ b_2\ b_3)$ deux 3-cycle de $\mathfrak{A}_5$. En appliquant la question précédente, il existe σ paire telle que $\sigma(a_1) = b_1$, $\sigma(a_2) = b_2$ et $\sigma(a_3) = b_3$. On a alors

$$\sigma(a_1\ a_2\ a_2)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \sigma(a_3)) = (b_1\ b_2\ b_3).$$

   Ainsi, les cycles $(a_1\ a_2\ a_3)$ et $(b_1\ b_2\ b_3)$ sont conjugués dans $\mathfrak{A}_5$ (σ étant paire).
   On en déduit que $\boxed{\text{les 3-cycles sont 2 à 2 conjugués dans } \mathfrak{A}_5}$.

3. Soit $\sigma_1 = (i_1\ j_1) \circ (k_1\ \ell_1)$ et $\sigma_2 = (i_2\ j_2) \circ (k_2\ \ell_2)$ deux compositions de deux transpositions à supports disjoints. Les entiers i_1, j_1, k_1 et ℓ_1 sont donc deux à deux distincts dans $[\![1, 5]\!]$. Soit m_1 le dernier élément de $[\![1, 5]\!]$. On définit de même m_2. Soit alors σ définie par $\sigma(i_s) = j_s$, pour tout $s \in [\![1, 5]\!]$. Quitte à considérer $\sigma \circ (i_1\ j_1)$ au lieu de σ, on peut supposer σ est paire, et la description de la conjugaison sur les cycles amène :

$$\sigma\sigma_1\sigma^{-1} = (\sigma(i_1)\ \sigma(j_1)) \circ (\sigma(k_1)\ \sigma(\ell_1)) = (i_2\ j_2) \circ (k_2\ \ell_2) = \sigma_2,$$

la composition éventuelle par $(i_1\ j_1)$ n'ayant pas d'incidence (on trouve $(j_2\ i_2)$ au lieu de $(i_2\ j_2)$, mais c'est la même transposition !). Ainsi, σ étant paire, σ_1 et σ_2 sont conjuguées dans $\mathfrak{A}_5$.

Ainsi les composées de deux transpositions à supports disjoints sont conjuguées dans $\mathfrak{A}_5$.

4. Soit $c_0 = (1\ 2\ 3\ 4\ 5)$, et $c = (a_1\ a_2\ a_3\ a_4\ a_5)$ un 5-cycle, et $\sigma \in \mathfrak{S}_5$ définie par $\sigma(k) = a_k$. On a donc $c = \sigma c_0 \sigma^{-1}$. On en déduit que

$$c^2 = \sigma c_0 \sigma^{-1} \sigma c_0 \sigma^{-1} = \sigma c_0^2 \sigma^{-1} = \sigma(1\ 3\ 5\ 2\ 4)\sigma^{-1}.$$

Or,

$$(1\ 3\ 5\ 2\ 4) = \tau c_0 \tau^{-1},$$

où $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} = (2\ 3\ 5\ 4)$.

On en déduit que $c^2 = (\sigma \circ \tau) \circ c_0 \circ (\sigma \circ \tau)^{-1}$.

5. La permutation τ ci-dessus est impaire (cycle de longueur 4). Ainsi, soit σ soit $\sigma \circ \tau$ est paire. On en déduit que soit c soit c^2 est conjugué dans $\mathfrak{A}_5$ à c_0.

6. Soit H un sous-groupe distingué de $\mathfrak{A}_5$. Puisque H est stable par conjugaison, et puisque les 3-cycles sont deux-à-deux conjugués, si H contient un 3-cycle, il les contient tous.

Le même argument montre que si H contient un produit de 2 transpositions disjointes, il les contient tous.

En ce qui concerne les 5-cycles, si H contient un 5-cycle c, il contient aussi c^2. Ainsi, d'après la question précédente, par stabilité par conjugaison, il contient c_0 (notations de la question écédente). Or, étant donné un autre 5-cycle c', soit c' soit c'^2 est conjugué à c_0, donc c' est dans H ou c'^2 est dans H. Or, si $c'^2 \in H$, $c'^6 = c'^{2^3} \in H$, et comme c' est d'ordre 5, $c' \in H$. Dans tous les cas, le 5-cycle c', choisi quelconque, est dans H.

Ainsi, si H contient un 5-cycle, il les contient tous.

7. - Un 3-cycle est obtenu par le choix d'un sous-ensemble $\{i_1, i_2, i_3\}$ de $[\![1, 5]\!]$, puis le choix d'un des deux 3-cycles de support $\{i_1, i_2, i_3\}$, à savoir $(i_1\ i_2\ i_3)$ ou $(i_1\ i_3\ i_2)$. Il y a donc $\binom{3}{5} \times 2 = 20$ 3-cycles.
   - Une composition de deux transpositions disjointes est la donnée d'un sous-ensemble $\{i_1\ i_2\ i_3\ i_4\}$ de $[\![1, 5]\!]$ (ou de façon équivalente, le choix du point fixe i_5), ce qui se fait de 5 façons possibles. Étant fixé arbitrairement un point par exemple i_1 de cet ensemble, on choisit son image (de 3 façons possibles), à savoir i_2. Cela détermine toute la permutation, les deux derniers éléments s'échangeant l'un l'autre. Ainsi, il y a 15 compositions de 2 transpositions disjointes.
   - Le choix d'un 5-cycle est obtenu en choisissant les u images successives de 1, d'abord parmi 4 éléments, puis pour la suivante parmi les 3 restants, etc. Il y a donc $4! = 24$ 5-cycles.
   - Les seuls types cycliques possibles dans $\mathfrak{A}_5$ sont 1^5 (c'est l'identité), $1^2 3^1$, $1^1 2^2$ et 1^5 (car il faut un nombre impair de cycles dans la décomposition en produit de cycles à supports disjoints). Ainsi, si $H \neq \{\mathrm{id}\}$, il contient au moins une permutation du type étudié précédemment, donc toutes les permutations de ce type (en plus de l'identité). Il ne peut pas contenir que des permutations d'un seul type (en plus de l'identité), sinon son cardinal serait 21, 16 ou 25, qui ne divise pas $|\mathfrak{A}_5| = 60$ (la moitié des permutations sont paires : la composition par une transposition fixée donne une bijection entre l'ensemble des permutations paires et l'ensemble des permutations impaires) ; cela contredit le théorème de Lagrange. H contient alors nécessairement, en plus de id, des permutations de deux types cycliques différents. Mais alors, un décompte rapide amène de façon immédiate $|H| > 30$. Comme $|H|$ doit diviser 60, il vient donc $|H| = 60$, donc $H = \mathfrak{A}_5$.
   - Ainsi, les seuls groupes distingués de $\mathfrak{A}_5$ sont $\{0\}$ et $\mathfrak{A}_5$. Autrement dit, $\mathfrak{A}_5$ est simple.

Partie III – Simplicité de $\mathfrak{A}_n$, $n > 5$

Soit $n > 5$, et soit H un sous-groupe distingué de $\mathfrak{A}_n$, différent de $\{\mathrm{id}\}$. Soit $\sigma \neq \mathrm{id}$ dans H

1. Soit a tel que $\sigma(a) \neq a$. On pose $b = \sigma(a)$, et on considère c différent de a, b et $\sigma(b)$. Soit τ le 3-cycle $(a\ b\ c)$.
   La conjugaison préservant le type cyclique, $\boxed{\sigma\tau^{-1}\sigma^{-1} \text{ est un 3-cycle.}}$
   Plus précisément, $\sigma\tau^{-1}\sigma^{-1} = (\sigma(a)\ \sigma(c)\ \sigma(b)) = (b\ \sigma(c)\ \sigma(b))$
   Les entiers qui ne sont ni dans le support du cycle $\sigma\tau^{-1}\sigma^{-1}$ ni dans le support du cycle τ sont des points fixes de la composée $\tau\sigma\tau^{-1}\sigma^{-1}$. Or, l'union de ces deux supports est $\{a, b, c, \sigma(b), \sigma(c)\}$.
   Ainsi, $\boxed{\tau\sigma\tau^{-1}\sigma^{-1} \text{ admet au moins } n-5 \text{ points fixes}}$.
2. Soit F un sous-ensemble de $[\![1, n]\!]$ de cardinal 5, contenant l'ensemble des points non fixes de $\sigma\tau^{-1}\sigma^{-1}$. Soit $\mathfrak{A}(F)$ l'ensemble des permutations de $\mathfrak{A}_n$ laissant tous les points extérieurs à F fixes. On a alors pour tout $\sigma \in \mathfrak{A}(F)$, $\sigma(F) = F$ (car σ est bijective). Donc σ induit une bijection $\tilde{\sigma}$ de F dans F
   Soit $\varphi : [\![1, 5]\!] \longrightarrow F$ une bijection (numérotation des éléments de F). On définit alors :
   $$\Phi :\ \mathfrak{A}(F) \longrightarrow \mathfrak{A}_5,$$
   par $\Phi(\sigma) = \varphi^{-1} \circ \tilde{\sigma} \circ \varphi$.
   - $\mathfrak{A}(F)$ est un sous-groupe de $\mathfrak{A}_n$. En effet :
     * il contient id
     * si σ et τ sont dans $\mathfrak{A}(F)$, alors tous les points hors de F sont points fixes de σ et τ, donc aussi de $\sigma \circ \tau$, et par conséquent, $\sigma \circ \tau \in \mathfrak{A}(F)$.
     * Si $\sigma \in \mathfrak{A}(F)$, alors pour tout $x \notin F$, $\sigma(x) = x$, donc $\sigma^{-1}(x) = x$. Ainsi, l'ensemble des points non fixes de σ^{-1} est dans F, donc σ^{-1} est dans $\mathfrak{A}(F)$.
   - Φ est un morphisme de groupes : en effet, soit σ et τ dans $\mathfrak{A}(F)$. Alors
     $$\Phi(\sigma \circ \tau) = \varphi^{-1} \circ (\sigma \circ \tau) \circ \varphi = \varphi^{-1} \circ \sigma\varphi \circ \varphi^{-1} \circ \tau \circ \varphi = \Phi(\sigma) \circ \Phi(\tau).$$
   - Φ est un isomophisme, sa réciproque étant l'application qui à $\sigma \in \mathfrak{A}_5$ associé le prolongement (par l'identité) à $[\![1, n]\!]$ de la bijection de F définie par $\varphi \circ \sigma \circ \varphi^{-1}$.

   Ainsi, $\boxed{\mathfrak{A}(F) \text{ est isomorphe, en tant que groupe, à } \mathfrak{A}_5}$.
   Soit K un sous-groupe distingué de $\mathfrak{A}(F)$. On a alors pour tout $x \in \Phi(K)$ et tout $y \in \mathfrak{A}_5$, en posant $y' = \Phi^{-1}(y)$, et $x' = \Phi^{-1}(x)$,
   $$yxy^{-1} = \Phi(y')\Phi(x')\Phi(y')^{-1} = \Phi(y'x'y'^{-1}).$$
   Or, K étant distingué, et $x' \in H$, on a $y'x'y'^{-1} \in K$, donc $yxy^{-1} \in \Phi(K)$. On en déduit que $\Phi(K)$ est ditingué dans $\mathfrak{A}_5$, puis que $\Phi(K) = \{0\}$ ou $\mathfrak{A}_5$, donc que $H = \{0\}$ ou $\mathfrak{A}(F)$.
   Ainsi, $\boxed{\mathfrak{A}(F) \text{ est simple.}}$
3. Soit $K = H \cap \mathfrak{A}(F)$. Soit $x \in K$ et $y \in \mathfrak{A}(F)$. On a alors $yxy^{-1} \in \mathfrak{A}(F)$ (stabilité) et $yxy^{-1} \in H$ (car H est distingué dans $\mathfrak{A}_n$, et $x \in \mathfrak{A}_n$). Ainsi, $yxy^{-1} \in K$, d'où on tire que $\boxed{K \text{ est distingué dans } \mathfrak{A}(F).}$
   Or, $\sigma \in H$, donc, H étant distingué, $\tau\sigma\tau^{-1} \in H$, et par stabilité par produit et inverse, $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Or $\tau\sigma\tau^{-1}\sigma^{-1} \in \mathfrak{A}(F)$, et cette permutation n'est pas l'identité. En effet, l'égalité
   $$\tau\sigma\tau^{-1}\sigma^{-1} = (a\ b\ c) \circ (b\ \sigma(c)\ \sigma(b))$$
   permet de se rendre compte que l'image de $\sigma(b)$ est c, qui est différent de $\sigma(b)$ par construction.
   Ainsi, $K \neq \{\text{id}\}$. Étant distingué dans $\mathfrak{A}(F)$ qui est simple, on a donc $K = \mathfrak{A}(F)$, donc contient les 3-cycles de $\mathfrak{A}(F)$. Ainsi $\boxed{H \text{ contient au moins un 3-cycle de } \mathfrak{A}_n}$.
4. Les 3-cycles de $\mathfrak{A}_n$ étant 2 à 2 conjugués, le fait que H soit distingué implique donc que tous les 3-cycles de $\mathfrak{A}_n$ sont dans H. Puisque les 3-cycles engendrent $\mathfrak{A}_n$, il en résulte que $\mathfrak{A}_n \subset H$, l'autre inclusion provenant de la définition de H.
   Ainsi, $H = \mathfrak{A}_n$.
   Nous avons donc montré que tout sous-groupe distingué autre que $\{\text{id}\}$ de $\mathfrak{A}_n$ est égal à $\mathfrak{A}_n$ lui-même. Ceci équivaut à affirmer que $\boxed{\mathfrak{A}_n \text{ est simple (pour } n \geqslant 5)}$.