Exercices groupe symétrique

1 Introduction

Ce document se veut être un ensemble d'exercices portant sur le groupe symétrique à n éléments et comportant des résultats sur ce dernier qu'il peut être intéressant de connaître avant d'entamer les oraux, notamment ceux de l'X en MP.

2 Exercices

Exercice 1 : Un calcul de puissance
Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 5 & 7 & 6 & 3 & 8 & 2 \end{pmatrix}$. Calculer σ^{2023}.

Exercice 2 : Caractères de degré 1 de S_n
Soit $n \geq 2$. Déterminer les morphismes de groupes de S_n dans $(\mathbb{C}^*, \times)$.

Exercice 3 : Autour des engendrements de S_n
Montrer que les transpositions $(1, k)$ avec $2 \leq k \leq n$ engendrent S_n, idem pour les $(k, k+1)$ avec $1 \leq k \leq n-1$, idem pour (1 2) et (1 2 ... n). Combien de transpositions au minimum suffisent pour engendrer S_n ?

Exercice 4 : Engendrement de S_n par les transpositions
Montrer par récurrence que les transpositions engendrent S_n pour $n \geq 2$.

Exercice 5 : Simplicité du groupe alterné d'ordre $n \geq 5$
D'abord quelques définitions : un sous-groupe H d'un groupe G est dit *distingué* si

$$\forall h \in H, \forall g \in G, ghg^{-1} \in H$$

Par exemple, si G est un groupe de neutre e_g, $\{e_g\}$ et G sont distingués.
Un groupe G est dit *simple* si ses seuls sous-groupes distingués sont $\{e_g\}$ et G.
Montrer que $\mathscr{A}_n$ (le groupe alterné d'ordre n, i.e les permutations dont la signature vaut 1) est simple pour $n \geq 5$.

Exercice 6 : Théorème de Cayley
Soit G un groupe. Montrer que G est isomorphe à un sous-groupe de $S(G)$ (les bijections de G dans G).

Exercice 7 : Sous-groupes de S_n d'indice au plus n quand $n \geq 5$
L'indice d'un sous-groupe H d'un groupe fini G, généralement noté $[G : H]$, est le cardinal de l'ensemble quotient G/H défini comme l'ensemble des classes d'équivalence sur G pour la relation définie par :

$$xRy \iff y \in xH$$

Montrer que si $n \geq 5$ et si H est un sous-groupe distingué de S_n d'indice $2 \leq r \leq n-1$ alors $r = 2$ et $H = \mathscr{A}_n$. Montrer que les sous-groupes d'indice n de S_n sont isomorphes à S_{n-1}. On pourra utiliser la simplicité de $\mathscr{A}_n$ quand $n \geq 5$ pour montrer que les seuls sous-groupes distingués de S_n quand $n \geq 5$ sont $S_n, \mathscr{A}_n$ et $\{id\}$.

Exercice 8 : Stabilité de $\mathscr{A}_n$ par tout automorphisme de S_n
Montrer que $\mathscr{A}_n$ est stable par tout automorphisme de S_n.

Exercice 9 : Automorphismes de S_n pour $n \neq 6$
L'objectif de cet exercice, qui m'a été posé aux oraux de l'X en 2023, est de montrer que quand $n \neq 6$, tout automorphisme de S_n est intérieur (i.e de la forme $u \mapsto \sigma \circ u \circ \sigma^{-1}$ pour une certaine permutation σ).
Question 1 Pour $\sigma \in S_n$ on note $Z(\sigma) = \{\tau \in S_n, \tau \circ \sigma = \sigma \circ \tau\}$ ($Z(\sigma)$ est appelé *centralisateur* de σ). Montrer que $Z(\sigma)$ est un sous-groupe de S_n et que pour tout $\varphi \in \mathrm{Aut}(S_n)$, $Z(\varphi(\sigma)) = \varphi(Z(\sigma))$.
Question 2 Calculer $|Z(\sigma)|$ (le cardinal de $Z(\sigma)$) quand σ est un produit de k transpositions à supports disjoints.
Question 3 On suppose $n \neq 6$. On se donne $\varphi \in \mathrm{Aut}(S_n)$ et τ une transposition. Montrer que $\varphi(\tau)$ est une transposition.
Question 4 En déduire que φ est intérieur.

Exercice 10 : Il n'existe pas de morphisme de groupes injectif de S_n dans $\mathscr{A}_{n+1}$ pour $n \geq 2$
Montrer qu'il n'existe pas de morphisme de groupes injectif de S_n dans $\mathscr{A}_{n+1}$ pour $n \geq 2$. On traitera d'abord les cas $n = 2$ et $n = 3$.

3 Indications

Indications pour l'exercice 1 :

Déterminer l'ordre de σ en la décomposant en produit de cycles à supports disjoints.

Indications pour l'exercice 2 :

S'intéresser aux images des transpositions, utiliser le fait qu'elles engendrent S_n.

Indications pour l'exercice 3 :

Écrire les transpositions (i, j) à l'aide des $(1, k)$, puis écrire les $(1, k)$ à l'aide des $(k, k+1)$, puis écrire les $(k, k+1)$ à l'aide de $(1, 2)$ et de $(1, \ldots, n)$. Pour se donner une idée de la réponse à la dernière question, regarder ce qu'il se passe si on enlève une des $(1, k)$: les transpositions restantes engendrent-elles toujours S_n ?

Indications pour l'exercice 4 :

Raisonner par récurrence sur n.

Indications pour l'exercice 5 :

L'exercice est difficile, il faut plusieurs connaissances intermédiaires. Commencer par montrer que les 3-cycles engendrent $\mathscr{A}_n$, puis que deux 3-cycles sont toujours conjugués dans $\mathscr{A}_n$. Ensuite, se donner un sous-groupe distingué H de $\mathscr{A}_n$ non réduit à l'identité et montrer qu'il contient un 3-cycle en raisonnant sur la décomposition en produits de cycles à supports disjoints d'un élément σ de H différent de l'identité maximisant le nombre de points fixes parmi les éléments de H.

Indications pour l'exercice 6 :

Considérer

$$\begin{aligned} \varphi \ : G &\to S(G) \\ g &\mapsto \varphi(g) \end{aligned}$$

où :

$$\begin{aligned} \varphi(g) \ : G &\to G \\ h &\mapsto gh \end{aligned}$$

φ est appelé *action de translation à gauche de G sur lui-même*. Quand on ne sait pas quoi faire, il est parfois intéressant de s'intéresser à ce morphisme.

Indications pour l'exercice 7 :

S'inspirer de l'exercice 6 en faisant cette fois agir S_n sur S_n/H par translation à gauche. Remarquer que le noyau d'un morphisme de groupes est toujours un sous-groupe distingué de l'ensemble de départ.

Indications pour l'exercice 8 :

S'intéresser aux ordres des images des 3-cycles.

Indications pour l'exercice 9 :

Pour la dernière question, s'intéresser aux images par φ des $(1,k), 2 \leq k \leq n$. Montrer par récurrence qu'il existe $x_1, \ldots, x_n$ deux-à-deux distincts tels que $\forall k \in \{2, \ldots, n\}, \varphi((1,k)) = (x_1, x_k)$.

Indications pour l'exercice 10 :

Remarquer que deux conditions nécessaires à l'existence d'un morphisme de groupes injectif entre deux groupes finis est que le cardinal du premier divise celui du second, et qu'il existe un sous-groupe du groupe d'arrivée de cardinal celui de l'ensemble de départ. Utiliser la première condition pour traiter le cas $n = 2$, et la seconde pour le cas $n = 3$.
Pour le cas général, raisonner par l'absurde en supposant qu'il existe un tel morphisme φ et s'inspirer de l'exercice 7.

4 Solutions

Solution de l'exercice 1 :

La méthode est toujours la même pour ce genre d'exercices : on commence par **déterminer l'ordre de l'élément étudié dans le groupe dans lequel on travaille**, ici l'ordre de σ dans S_8.

Pour ce faire, on commence par décomposer σ en produit de cycles à supports disjoints, dont le cours nous renseigne sur l'existence et l'unicité à l'ordre près des facteurs. En effet, ces cycles commutent (car leurs supports sont disjoints), et on sait que si g et h sont deux éléments d'ordre fini d'un groupe G et qui commutent, alors gh est d'ordre fini dans G divisant le PPCM des ordres de g et h.

Pour calculer la décomposition en produit de cycles à supports disjoints de $\sigma \in S_n$, on commence par calculer $\sigma(1)$, puis $\sigma(\sigma(1))$,..., jusqu'à retomber sur 1 : cela nous donne un premier cycle. On réitère ensuite en calculant $\sigma(k)$, $\sigma(\sigma(k))$... où k est le plus petit nombre de $\{1, ..., n\}$ que l'on n'a pas encore croisé dans nos calculs, cela nous donne un deuxième cycle. On s'arrête quand tous les éléments de $\{1, \ldots, n\}$ ont été rencontrés.

Dans notre cas $\sigma(1) = 4$, $\sigma(4) = 7$, $\sigma(7) = 8$, $\sigma(8) = 2$, $\sigma(2) = 1$: on a trouvé le cycle (14782) que l'on notera γ. Ensuite : $\sigma(3) = 5$, $\sigma(5) = 6$, $\sigma(6) = 3$, on a donc trouvé le cycle (356) noté τ.
Ainsi, $\sigma = \tau\gamma$ avec τ et γ commutant donc l'ordre de σ divise le PPCM des ordres de τ et γ, respectivement 3 et 5, donc l'ordre de σ divise 15. De $2023 = 15 \times 134 + 13$ on obtient :

$$\sigma^{2023} = \sigma^{13} = \tau^{13}\gamma^{13} = \tau\gamma^{-2}$$

Pour calculer γ^{-2}, il suffit de calculer γ^2 en parcourant les éléments du cycle en en sautant un à chaque fois, on trouve (1 7 2 4 8), puis à inverser l'ordre du cycle.
Ainsi,

$$\sigma^{2023} = (356)(84271) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 2 & 6 & 3 & 1 & 4 \end{pmatrix}$$

Solution de l'exercice 2 :

Cet exercice est l'occasion de voir plusieurs résultats importants. Mais avant, il est intéressant d'avoir à l'idée que si G et H sont deux groupes tels qu'existe une partie $S \subset G$ telle que $G = \langle S \rangle$ (le groupe engendré par S), alors tout homomorphisme φ de G vers H est entièrement déterminé par l'image des éléments de S. Par ailleurs, si H est commutatif (comme c'est le cas pour $(\mathbb{C}^*, \times)$), φ est constant sur les classes de conjugaison, car

$$\forall (g, g') \in G^2, \varphi(g^{-1}g'g) = \varphi(g)^{-1}\varphi(g')\varphi(g) = \varphi(g')\varphi(g)^{-1}\varphi(g) = \varphi(g')$$

Dans notre cas, on va s'intéresser à la partie S des transpositions de S_n. On raisonne par analyse-synthèse en supposant donné un homomorphisme φ de S_n dans $(\mathbb{C}^*, \times)$. Il faut tout d'abord remarquer que **les transpositions engendrent** S_n. Pour le montrer, il suffit de montrer qu'elles engendrent les cycles, car ceux-ci engendrent déjà S_n (toute permutation peut s'écrire comme produit de cycles). Or si $\tau = (x_1 \dots x_p)$ est un p-cycle, on a clairement $\tau = (x_1\ x_2) \dots (x_{p-1}\ x_p)(x_p\ x_1)$ ce qui prouve que tout cycle s'écrit comme produit de transpositions, et donc toute permutation également.

Ensuite, il faut remarquer que **les transpositions, et en général les cycles de même longueur sont conjugués dans** S_n. Cela vient du fait que si $\tau = (x_1 \dots x_p)$ est un p-cycle et σ une permutation, σ o $(x_1 \dots x_p)$ o $\sigma^{-1} = (\sigma(x_1) \dots \sigma(x_p))$ (on remarque que **le conjugué d'un p-cycle en est un**), donc si $\tau' = (y_1 \dots y_p)$ est un p-cycle, il suffit de prendre σ qui envoie x_i sur y_i pour i allant de 1 à p et qui permute les éléments restants pour avoir $\sigma\tau\sigma^{-1} = \tau'$.

On sait maintenant que les transpositions sont conjuguées, et qu'elles engendrent S_n. Or, si τ est une transposition (existe si $n \geq 2$), τ est d'ordre 2 donc

$$\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(id) = 1$$

donc φ est à valeurs dans $\{-1, 1\}$. Par ailleurs, φ est constant sur les transpositions. Dès lors, s'il vaut 1 sur ces dernières, φ est le morphisme trivial valant constamment 1, et s'il vaut -1 sur les transpositions, c'est la signature, car il coïncide avec celle-ci sur les transpositions, qui engendrent S_n

Ainsi, si $n \geq 2$, **les homomorphismes de S_n dans $\mathbb{C}^*$ sont le morphisme trivial et la signature**. Dans le langage des représentations de groupes, on aurait dit que *les caractères de degré 1 de S_n sont le caractère trivial et la signature.*

Solution de l'exercice 3 :

Pour montrer que les $(1,k)$ engendrent S_n, il suffit de montrer que les transpositions en sont des produits, puisque celles-ci engendrent déjà S_n comme on l'a vu. Soit donc (i,j) une transposition ($i \neq j$, et $i,j \neq 1$ sinon (i,j) est déjà de la forme $(1,k)$). Il suffit de remarquer que $(i,j) = (1,i)(1,j)(1,i)$, et c'est tout ! Cette écriture est très pratique et à garder à l'esprit, on s'en sert dans l'exercice 9.
Ainsi, **les transpositions** $(1,k)$ **avec** $2 \leq k \leq n$ **engendrent** S_n.

On sait maintenant que les $(1,k)$ $(2 \leq k \leq n)$ engendrent S_n, donc pour montrer qu'il en est de même pour les $(k,k+1)$ $(1 \leq k \leq n-1)$, il suffit de montrer que les $(1,k)$ en sont des produits. Pour $3 \leq k \leq n$, on a en vertu de la formule mise en exergue dans le troisième paragraphe (conjugaison des cycles) :

$$(k-1,k)(1,k-1)(k-1,k)^{-1} = (1,k)$$

Ainsi, si $k = 3$, c'est terminé. Sinon, on recommence avec $(1,k-1)$. La propriété étant vraie pour $k = 2$ ($(1,2)$ est déjà de la forme $(k,k+1)$), le principe de récurrence permet de conclure que les $(1,k)$ $(2 \leq k \leq n)$ s'écrivent comme produit de $(k,k+1)$ $(1 \leq k \leq n-1)$ et donc que **les transpositions** $(k,k+1)$ $(1 \leq k \leq n-1)$ **engendrent** S_n.

On commence à connaître la chanson : pour montrer que $\tau = (1,2)$ et $\gamma = (1,2,\ldots,n)$ engendrent S_n, il suffit de montrer que les $(k,k+1)$ $(1 \leq k \leq n-1)$ en sont des produits. On a déjà τ de la forme voulue. Par ailleurs, la formule de conjugaison des cycles nous donne :

$$\forall k \in \{1,\ldots,n-2\}, \gamma \circ (k,k+1) \circ \gamma^{-1} = (\gamma(k),\gamma(k+1)) = (k+1,k+2)$$

et donc :

$$\forall k \in \{1,\ldots,n-2\}, (k,k+1) = \gamma^{k-1} \circ (1,2) \circ (\gamma^{k-1})^{-1}$$

Ainsi, $(1,2)$ **et** $(1,2,\ldots,n)$ **engendrent** S_n.

Répondons maintenant à la question du nombre minimal de transpositions engendrant S_n. Les deux premiers exemples que l'on a traités montrent que $n-1$ transpositions suffisent. On va en réalité montrer qu'on ne peut pas faire moins. Pour se forger l'intuition, on peut imaginer que l'on enlève une des transpositions $(1,k)$, notons $(1,j)$ la transposition que l'on enlève. Puisque toutes les $(1,k)$, $2 \leq k \leq n$, $k \neq j$ laissent fixe j, si ces transpositions engendraient S_n, tout les permutations fixeraient j, ce qui n'est bien sûr pas le cas quand $n \geq 3$ (considérer $(1,j')$ avec $j' \neq j$).
De manière générale, considérons $\tau_1,\ldots,\tau_l$ des transpositions. Imaginons qu'il existe $i,j \in \{1,\ldots,n\}$ tels que j ne soit pas atteignable en "utilisant les τ_k sur i", c'est-à-dire que :

$$\forall m \in \mathbb{N}, \forall (j_1,\ldots,j_m) \in [\![1;l]\!]^m, (\prod_{q=1}^{m} \tau_{j_q})(i) \neq j$$

Alors toute permutation envoyant i sur j, par exemple (i,j) ne pourra pas s'écrire comme produit des τ_k, qui donc n'engendreront pas S_n. Ainsi, une condition nécessaire pour qu'un

ensemble de transpositions engendre S_n est qu'en partant de n'importe quel élément de $\{1, \ldots, n\}$ on puisse atteindre n'importe quel élément de $\{1, \ldots, n\}$ en utilisant ces transpositions.
Pour formaliser cela, imaginons un graphe dont les sommets soient $\{1, \ldots, n\}$ et dans lequel deux sommets différents i et j sont reliés si et seulement si l'une des τ_k s'écrit (i, j). La condition nécessaire que l'on a mise en exergue traduit que, pour que les τ_k engendrent S_n, il est nécessaire que pour toute paire de sommet, il existe au moins un chemin joignant les deux sommets. Un tel graphe est dit **connexe**.

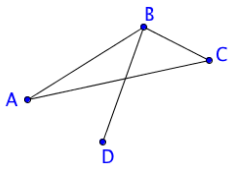

FIGURE 1 – Graphe connexe

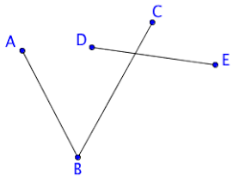

FIGURE 2 – Graphe non connexe

Montrons par récurrence sur $n \geq 2$ que si G est un graphe connexe à n sommets, alors il a au moins $n-1$ arêtes.
C'est clair pour $n = 2$.
Supposons le résultat vrai à l'ordre $n \geq 2$. Soit G un graphe à $n+1$ sommets. Puisque chaque arête correspond à exactement 2 sommets, on a en notant A le nombre d'arêtes de G, S l'ensemble de ses sommets et $\delta(x)$ le nombre d'arêtes arrivant en $x \in S$:

$$\sum_{x \in S} \delta(x) = 2A$$

Alors, si $\forall x \in S, \delta(x) \geq 2$, on a directement $A \geq n+1$ avec l'égalité ci-dessus.
Sinon, il existe un sommet x sur lequel n'arrive qu'une arête : imaginons que l'on retire ce sommet et l'arête qui lui est incidente, on obtient un graphe G' à n sommets et $A-1$ arêtes. D'après l'hypothèse de récurrence appliquée à G', $A - 1 \geq n$: ce qu'il fallait montrer.
Ainsi, pour que le graphe à n sommets créé à partir des τ_k $(1 \leq k \leq l)$ soit connexe, il faut qu'il ait au moins $n-1$ arêtes, donc que $l \geq n-1$: **il faut donc au moins** $n-1$ **transpositions pour engendrer** S_n.

Solution de l'exercice 4 :

L'idée générale de cet exercice peut s'appliquer également pour montrer que les réflexions engendrent $O(E)$ où E est un espace euclidien. En effet, le but va être de **fixer**. Ici, on va se donner une permutation $\sigma \neq id$, fixer un élément de $\{1, \ldots, n\}$ qui n'est pas déjà laissé fixe par notre permutation en la composant par une transposition τ bien léchée, puis appliquer l'hypothèse de récurrence à $\tau\sigma$, écrire $\tau\sigma$ comme un produit de transpositions et enfin "faire passer τ de l'autre côté" en se servant du fait que $\tau^2 = id$.
On établit pour $n \geq 2$ la propriété :

Pour tout ensemble E de cardinal n et toute permutation σ des éléments de E, il existe des transpositions telles que σ en soit le produit.
Si E est un ensemble de cardinal 2, de la forme $\{x_1, x_2\}$, alors $S(E)$ (les permutations des éléments de E) est égal à $\{id, (x_1, x_2)\}$ et la propriété est vraie (id est un produit vide de transpositions par convention).
Supposons la propriété vraie à l'ordre $n \geq 2$. Soit E un ensemble de cardinal $n+1$ et soit $\sigma \in S(E)$.
Si $\sigma = id$ il n'y a rien à faire.
Sinon, $\exists x \in E, \sigma(x) \neq x$. On pose $y = \sigma(x)$ et $\tau = (x, y)$ de sorte que $\tau\sigma(x) = x$ et que $\tau\sigma$ induise une permutation des éléments de $E - \{x\}$, qui est de cardinal au moins 2. D'après l'hypothèse de récurrence, il existe des transpositions $\tau_1, \ldots, \tau_l$ telles que $\tau\sigma = \prod_{k=1}^{l} \tau_k$. En composant cette égalité par τ on obtient, puisque $\tau^2 = id$, $\sigma = \tau \prod_{k=1}^{l} \tau_k$: la propriété est vraie à l'ordre $n+1$.
Ainsi, le principe de récurrence permet de conclure que **si E est de cardinal au moins 2, les transpositions engendrent** $S(E)$.

Solution de l'exercice 5 :

Cet exercice est très abrupt et nécessite des connaissances sur $\mathscr{A}_n$. Bien qu'il soit posé tel quel aux oraux, il est je pense impossible de s'en sortir sans la connaissance de certains lemmes "sortis du chapeau", c'est d'ailleurs pour cette raison que j'écris ces lignes. De manière générale, quand on veut montrer qu'un groupe G est simple, on commence par s'en donner un sous-groupe distingué H différent du singleton neutre, et on cherche à montrer que H **contient un élément d'une partie stable par conjugaison et qui engendre** G. En effet, H étant distingué, il est stable par conjugaison : il contiendra donc toute la partie en question, et puisque c'est un groupe, il est stable par produit, et puisque cette partie engendre G, H contiendra G, donc ce sera G. Par exemple, on peut montrer que $SO_3(\mathbb{R})$ est simple en utilisant le fait que les retournements, i.e les matrices semblables à $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & -1 & -1 \end{pmatrix}$, l'engendrent.
Seulement voilà, reste à trouver une partie de $\mathscr{A}_n$ qui convienne... Je sais pas vous, mais moi je parierai bien sur les 3 - cycles... Vous l'aurez compris, nous allons montrer les résultats suivants : **les 3 - cycles engendrent** $\mathscr{A}_n$, et **pour** $n \geq 5$**, deux 3-cycles sont conjugués dans** $\mathscr{A}_n$.

Montrons que les 3-cycles engendrent $\mathscr{A}_n$. Par définition, les éléments de $\mathscr{A}_n$ sont les permutations de signature 1. Puisque la signature d'une transposition vaut -1 et que toute permutation peut s'écrire comme un produit de transpositions, les éléments de $\mathscr{A}_n$ sont donc exactement les permutations qui sont le produit d'un nombre pair de transpositions. Pour montrer que les 3-cycles engendrent $\mathscr{A}_n$, il suffit donc de montrer qu'un produit de deux transpositions est en fait un produit de 3-cycles. Soient donc (i, j) et (k, l) des transpositions.
Si ces deux transpositions sont égales, leur produit vaut l'identité, qui est un produit vide de

3-cycles.
Si un des éléments permutés est commun aux deux transpositions, disons que $j = k$, alors $(i, j)(k, l) = (i, j, l)$ qui est un 3-cycle.
Sinon, on remarque que $(i, j)(k, l) = (i, l, k)(i, j, k)$ (pour le trouver, écrire le deuxième 3-cycle et trafiquer le premier jusqu'à ce que ça fonctionne).
Ainsi, **les 3-cycles engendrent** $\mathscr{A}_n$.

Montrons maintenant que pour $n \geq 5$, deux 3-cycles sont conjugués dans $\mathscr{A}_n$. Soient (i, j, k) et (i', j', k') deux 3-cycles, soit $\sigma \in S_n$ qui envoie i sur i', j sur j' et k sur k'. D'après la formule de conjugaison des cycles (c.f solution de l'exercice 2), $\sigma \circ (i, j, k) \circ \sigma^{-1} = (i', j', k')$
.
Si σ est paire c'est fini.
Sinon, on peut considérer p et q deux éléments de $\{1, \ldots, n\} - \{i, j, k\}$ (car $n \geq 5$) et remplacer σ par $\tau\sigma$ où $\tau = (p, q)$, ce qui ne change pas l'égalité du dessus. L'avantage est qu'alors, $\tau\sigma$ est paire et qu'on a fini. Ainsi, **pour** $n \geq 5$**, deux 3-cycles sont conjugués dans** $\mathscr{A}_n$.

Passons maintenant à la preuve du résultat : soit H un sous-groupe distingué de $\mathscr{A}_n$ différent du singleton identité. Comme expliqué ci-dessus, on veut montrer que H contient un 3-cycle, et on pourra conclure que $H = \mathscr{A}_n$. H n'est pas réduit à l'identité donc on peut se donner une permutation $\sigma \in H$ ayant le plus de points fixes parmi tous les éléments de H qui ne sont pas l'identité. Notons N son nombre de points fixes. On va montrer que σ est un 3-cycle en raisonnant par l'absurde sur la décomposition de cycles à supports disjoints de σ en fabriquant, à l'aide d'un 3-cycle bien léché (pour rester dans $\mathscr{A}_n$), un élément de H qui ait strictement plus de points fixes que σ.

Si cette décomposition n'est composée que de transpositions, alors il y en a au moins 2 car σ est paire, sans perte de généralité on peut supposer que ces transpositions sont $(1, 2)$ et $(3, 4)$, et donc que σ s'écrit $(1, 2)(3, 4)\tau_1 \ldots \tau_r$ où les τ_k ont des supports disjoints de $\{1, 2, 3, 4\}$. On note $\gamma = (3, 4, 5)$, on peut car $n \geq 5$. Alors, d'après la formule de conjugaison des cycles :

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma \circ (1,2) \circ \gamma^{-1})(\gamma \circ (3,4) \circ \gamma^{-1})(\gamma \circ \tau_1 \circ \gamma^{-1}) \ldots (\gamma \circ \tau_r \circ \gamma^{-1})$$

$$= (\gamma(1), \gamma(2))(\gamma(3), \gamma(4))\tau_1' \ldots \tau_r' = (1, 2)(4, 5)\tau_1' \ldots \tau_r'$$

où on a noté $\tau_i' = \gamma \circ \tau_i \circ \gamma^{-1}$.
Posons alors $\rho = \gamma \circ \sigma \circ \gamma^{-1} \circ \sigma^{-1}$. On remarque que :

$$\rho(1) = \gamma \circ \sigma \circ \gamma^{-1}(2) = \gamma \circ \sigma(2) = \gamma(1) = 1$$

Et que idem, $\rho(2) = 2$.
Par ailleurs, si i est un point fixe de σ strictement supérieur à 5, $\rho(i) = i$ donc i est encore un point fixe de ρ.
Or, puisque 1, 2, 3, 4 ne sont pas fixés par σ, ses N points fixes sont dans $\{5, \ldots, n\}$. Alors, si 5 n'est pas fixé par σ, tous les points fixes de σ sont points fixes de ρ, ainsi que 1 et 2, donc ρ a au moins $N + 2$ points fixes. Sinon, les $N - 1$ autres points fixes de σ différents de 5 sont points fixes de ρ, et en comptant 1 et 2, ρ a au mois $N + 1$ points fixes.
Par ailleurs, $\rho \neq id$ car $\gamma \circ \sigma \circ \gamma^{-1} \neq \sigma$ (regarder la décomposition en produit de cycles et

invoquer l'unicité de celle-ci).
Or, $\gamma \circ \sigma \circ \gamma^{-1} \in H$ car H est distingué et γ est un 3-cycle donc est dans $\mathscr{A}$, et donc $\rho = \gamma \circ \sigma \circ \gamma^{-1} \circ \sigma^{-1} \in H$: c'est absurde car ρ a strictement plus de points fixes que σ.

On en déduit qu'il y a au moins un cycle dans la décomposition de σ qui n'est pas une transposition, sans perte de généralité on peut supposer qu'il s'écrit $(1, 2, 3, \dots)$. Supposons encore, par l'absurde, que σ ne soit pas un 3-cycle. On va appliquer la même idée en cherchant encore deux éléments qui ne sont pas fixés par σ, ces éléments étant 4 et 5 dans le paragraphe précédent. S'il y a un autre cycle dans la décomposition, l'existence de deux éléments différents de 1, 2, 3 qui ne sont pas fixés par σ est claire. Sinon, σ est un cycle pair, de longueur au moins 3 mais qui n'est pas un 3-cycle par hypothèse, c'est donc un cycle de longueur au moins 5 et dans ce cas l'existence de deux éléments différents de 1, 2, 3 qui ne sont pas fixés par σ est encore claire. Quitte à renuméroter on peut supposer que ces éléments sont 4 et 5. Là encore, on pose $\gamma = (3, 4, 5)$. Alors, si on note $c_1 \dots c_r$ la décomposition de σ en produit de cycles à supports disjoints, et $c_1 = (1, 2, 3, \dots)$ on a par la formule de conjugaison des cycles :

$$\begin{aligned}\gamma \circ \sigma \circ \gamma^{-1} &= (\gamma \circ (1, 2, 3, \dots) \circ \gamma^{-1})(\gamma \circ c_2 \circ \gamma^{-1}) \dots (\gamma \circ c_r \circ \gamma^{-1}) \\ &= (\gamma(1), \gamma(2), \gamma(3), \dots) c_2' \dots c_r' = (1, 2, 4, \dots) c_2' \dots c_r'\end{aligned}$$

où l'on a noté, $c_i' = \gamma \circ c_i \circ \gamma^{-1}$ pour $i \in \{2, \dots, r\}$. Posons encore $\rho = \gamma \circ \sigma \circ \gamma^{-1} \circ \sigma^{-1}$. Pour les mêmes raisons, $\rho \in H$ et $\rho \neq id$. De plus,

$$\rho(2) = \gamma \circ \sigma \circ \gamma^{-1}(1) = \gamma \circ \sigma(1) = \gamma(1) = 2$$

Et enfin, tout point fixe de σ strictement supérieur à 5 est fixé par ρ. Puisque σ ne fixe pas 1, 2, 3, 4, 5, on en déduit que ρ a au moins $N + 1$ points fixes, donc strictement plus que σ : c'est absurde !

Plus de doute possible, σ est un 3-cycle, et au vu des remarques préliminaires, $H = \mathscr{A}_n$ et ainsi, $\mathscr{A}_n$ **est simple pour** $n \geq 5$.

On ne saurait résister à l'idée de faire quelques remarques. Si G est un groupe, on appelle *groupe dérivé* de G, noté $D(G)$ le groupe engendré par les commutateurs, i.e les éléments de la forme $[g, g']= gg'g^{-1}g'^{-1}$. C'est toujours un sous-groupe distingué de G, et le groupe quotient $G/D(G)$, appelé *l'abélianisé de* G, est un groupe abélien.
Un corollaire de l'exercice que l'on vient de voir est que **si** $n \geq 5$**, le groupe dérivé de** S_n **est** $\mathscr{A}_n$.

Solution de l'exercice 6 :

On définit :

$$\begin{aligned}\varphi : G &\to S(G) \\ g &\mapsto \varphi(g)\end{aligned}$$

où :

$$\begin{aligned}\varphi(g) \ : G &\to G \\ h &\mapsto gh\end{aligned}$$

Difficile de justifier pourquoi on en vient à poser ce morphisme (car oui, cela en est un) sans parler d'actions de groupe, on peut en avoir l'intuition en se souvenant que les translations (ici à gauche) sont parmi les plus simples permutations des éléments de G.
En tout cas, il est bon de connaître l'existence de ce morphisme, qualifié d'*action par translation à gauche*, dont on se sert dans les exercices suivants.
Tout d'abord, φ est bien défini, car quelque soit g dans G, $\varphi(g)$ est une bijection, de réciproque $\varphi(g^{-1})$. Ensuite, $\forall g, g' \in G, \forall h \in G$,

$$\varphi(gg')(h) = gg'h = g(g'h) = \varphi(g)(g'h) = \varphi(g)(\varphi(g')(h)) = (\varphi(g) \text{ o } \varphi(g'))(h)$$

Et donc $\forall g, g' \in G, \varphi(gg') = \varphi(g) \text{ o } \varphi(g')$: φ est un homomorphisme.
Montrons que φ est injectif : si $g \in \ker(\varphi), \varphi = id$ on a $\forall g' \in G, gg' = g'$. En prenant $g' = e_G$, on obtient $g = e_G$: φ est injectif.
Puisque φ est un homomorphisme, $\text{Im}(\varphi)$ est un sous-groupe de $S(G)$. On a ainsi $G \simeq \text{Im}(\varphi) \subset S(G)$: **ce que l'on voulait montrer**.

En particulier, si G est un groupe fini de cardinal n, G est isomorphe à un sous-groupe de S_n. Les sous-groupes de S_n peuvent donc servir de "modèles" pour la classification à isomorphisme près des groupes finis.

Solution de l'exercice 7 :

Soit H un sous-groupe d'indice $2 \leq r \leq n-1$ de S_n (avec $n \geq 5$). On peut s'inspirer de la preuve du théorème de Cayley et définir :

$$\begin{aligned}\varphi \ : S_n &\to S(S_n/H) \\ \sigma &\mapsto \varphi(\sigma)\end{aligned}$$

où :

$$\begin{aligned}\varphi(\sigma) \ : S_n/H &\to S_n/H \\ \tau H &\mapsto \sigma\tau H\end{aligned}$$

C'est l'action de S_n sur S_n/H par translation à gauche.
Montrons que φ est bien à valeurs dans $S(S_n/H)$: on se donne $\sigma \in S_n$ et il s'agit de montrer que $\varphi(\sigma)$ est bien bijective. Commençons par l'injectivité : soient $\tau H, \tau' H \in S_n/H$ telles que $\sigma\tau H = \sigma\tau' H$. Si $x \in \tau H$, $\sigma(x) \in \sigma\tau H = \sigma\tau' H$ donc $\exists y \in \tau' H, \sigma(x) = \sigma(y)$, et puisque σ est injective, $x = y \in \tau' H$ donc $\tau H \subset \tau' H$ et idem, $\tau' H \subset \tau H$ donc $\tau H = \tau' H$ et $\varphi(\sigma)$ est injective. Pour la surjectivité, il suffit de voir que si $\tau H \in S_n/H$, $\tau H = \sigma\sigma^{-1}\tau H = \varphi(\sigma)(\sigma^{-1}\tau H)$

donc $\varphi(\sigma)$ est surjective : c'est bien une bijection.

On montre de manière analogue à l'exercice 6 que φ est un morphisme de groupes. Intéressons-nous à son noyau. Il est bon de connaître le résultat suivant : **si G et G' sont deux groupes et $\psi : G \to G'$ un morphisme de groupes, $\ker(\psi)$ est un sous-groupe distingué de G**. En effet, si $g \in \ker(\psi)$ et $h \in G$, $\psi(hgh^{-1}) = \psi(h)\psi(g)\psi(h^{-1}) = \psi(h)\psi(h)^{-1} = e_{G'}$ donc $hgh^{-1} \in \ker(\psi)$ et ce quelque soient $g \in \ker(\psi)$ et $h \in G$: c'est la définition d'un sous-groupe distingué. Ainsi, dans notre cas, $\ker(\varphi)$ est un sous-groupe distingué de S_n.

On va montrer le résultat suggéré dans la consigne, en s'appuyant sur la simplicité de $\mathscr{A}_n$ quand $n \geq 5$ (c.f exercice 5) : **quand $n \geq 5$, les seuls sous-groupes distingués de S_n sont S_n, $\mathscr{A}_n$ et $\{id\}$**. Soit G un sous-groupe distingué de S_n. Alors, $G \bigcap \mathscr{A}_n$ est un sous-groupe distingué de $\mathscr{A}_n$, lequel est simple ($n \geq 5$) donc G est soit égal à $\mathscr{A}_n$ soit à $\{id\}$.
Si $G \bigcap \mathscr{A}_n = \mathscr{A}_n$, $\mathscr{A}_n$ est un sous-groupe de G, donc son cardinal divise celui de G (théorème de Lagrange), qui lui-même divise $n\,! = |S_n|$. Or, le cardinal de $\mathscr{A}_n$ vaut $\frac{n!}{2}$. En effet, en notant ε le morphisme signature, le théorème du rang pour les groupes donne $|S_n| = |\mathrm{Im}(\varepsilon)||\ker(\varepsilon)| = 2|\mathscr{A}_n|$ d'où le résultat. On a donc $\frac{n!}{2} \mid |\mathrm{G}| \mid n\,!$, donc $\exists k, k' \in \mathbb{N}, |G| = \frac{n!}{2}k$ et $n\,! = |G|k'$ donc $n\,! = \frac{n!}{2}kk'$ puis $kk' = 2$ donc $k' \in \{1, 2\}$ donc $|G|$ ne peut valoir que $n\,!$, auquel cas $G = S_n$, ou $\frac{n!}{2} = |\mathscr{A}_n|$ et auquel cas $G = \mathscr{A}_n$.
Si $G \bigcap \mathscr{A}_n = \{id\}$, on suppose par l'absurde que G contient un élément σ différent de l'identité. Soit γ un élément de G différent de l'identité. Alors, ni σ ni γ ne sont paires, car sinon elles seraient dans $G \bigcap \mathscr{A}_n = \{id\}$ ce qui n'est pas. Leur produit est donc pair : c'est un élément de $G \bigcap \mathscr{A}_n = \{id\}$, donc $\gamma = \sigma^{-1}$ et ce quelque soit $\gamma \in G - \{id\}$. Cela implique que $G = \{id, \sigma\}$ et que $\sigma = \sigma^{-1}$ donc σ est d'ordre 2. Or, **l'ordre d'une permutation est le PPCM des longueurs des cycles qui interviennent dans sa décomposition**, on en déduit que ceux-ci sont tous des transpositions, et donc que σ est un produit de $r \geq 1$ ($r \neq 0$ car $\sigma \neq id$) transpositions. Or, en utilisant la formule de conjugaison des cycles, on constate que **si σ et σ' sont deux permutations de décomposition en produits de cycles $c_1 \dots c_r$ et $c'_1 \dots c'_k$ telles que $r = k$ et la longueur de c_i soit égale à celle de c'_i quelque soit i** (après un éventuel ré-arrangement de l'ordre des c'_i), **alors σ et σ' sont conjuguées**. Une conséquence est que **tous les produits de r transpositions sont conjugués**, et puisque G est distingué, il les contient tous. Or, le nombre de produits de $r \geq 1$ transpositions est plus grand que le nombre de transpositions, qui vaut $\binom{n}{2} = \frac{n(n-1)}{2} \geq 10$ (car $n \geq 5$), bref il en existe au moins 1 qui n'est pas σ mais qui pourtant est dans G : c'est absurde car $G = \{id, \sigma\}$. Ainsi, $G = \{id\}$.

Ainsi, $\ker(\varphi)$ est soit égal à S_n, soit à $\{id\}$, soit à $\mathscr{A}_n$. Or, φ ne peut pas être injectif, car $|S_n| = n\,! > |S(S_n/H)| = r\,!$ (car H est d'indice $2 \leq r \leq n-1$), donc $\ker(\varphi) \neq \{id\}$. Par ailleurs, si $\sigma \in \ker(\varphi)$, $\forall \tau \in S_n, \sigma\tau H = \tau H$ ce qui implique en prenant $\tau = \sigma^{-1}$ que $\sigma^{-1}H = H$ donc $\sigma^{-1} \in H$ puis $\sigma \in H$ et donc $\ker(\varphi) \subset H$. Puisque H est d'indice au moins 2, ce n'est pas S_n, donc $\ker(\varphi)$ est forcément différent de S_n et donc $\ker(\varphi) = \mathscr{A}_n \subset H$. Mais alors, par le théorème de Lagrange, $|\mathscr{A}_n| = \frac{n!}{2}||H| = \frac{n!}{r}$ donc a fortiori $\frac{n!}{2} \leq \frac{n!}{r}$ d'où $r \leq 2$ et alors $r = 2$ puis $H = \mathscr{A}_n$.

Si cette fois H est d'indice n, alors $|H| = (n-1)\,!$. Tout d'abord, $\ker(\varphi) \subset H$ ne peut pas être égal à S_n. Il ne peut pas non plus être égal à $\mathscr{A}_n$ puisque sinon on aurait $\frac{n!}{2}|(n-1)\,!$ par le théorème de Lagrange, donc a fortiori $n \leq 2$ ce qui n'est pas. Ainsi, φ est injectif, donc $\varphi(H)$ est un sous-groupe de $S(S_n/H)$ isomorphe à H. Or, on remarque que tout élément de $\varphi(H) \subset S(S_n/H)$ laisse fixe $H \in S_n/H$ et réciproquement, puisque si $\sigma \in H$, $\varphi(\sigma)(H) = \sigma H = H$. Ainsi, tout élément $\varphi(\sigma)$ de $\varphi(H)$ est entièrement déterminé par la permutation $\widetilde{\varphi(\sigma)}$ des éléments de $S_n/H - \{H\}$ qu'il induit, et l'application $\varphi(\sigma) \mapsto \widetilde{\varphi(\sigma)}$ est clairement un isomorphisme (elle est bijective comme expliqué ci-dessus, et le caractère de morphisme est clair). Enfin, puisque $|S_n/H - \{H\}| = n-1$, on a $|S(S_n/H - \{H\})| \simeq S_{n-1}$.
Ainsi :

$$H \simeq \varphi(H) \simeq S(S_n/H - \{H\}) \simeq S_{n-1}$$

Ce qui prouve le résultat annoncé.

Solution de l'exercice 8 :

Cet exercice est l'occasion de faire la remarque suivante qui sera utile dans les prochains exercices : **soient G, G' deux groupes, $\varphi : G \to G'$ un homomorphisme et $x \in G$ d'ordre n fini. Alors, $\varphi(g)$ est d'ordre fini divisant n.** En effet, $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_{G'}$. Cette remarque s'avère particulièrement utile dans l'étude des morphismes de S_n dans lui-même, car l'image d'éléments de petit ordre ou d'ordre premier (typiquement des transpositions, d'ordre 2, ou des 3-cycles, d'ordre 3) ne peuvent avoir que peu d'ordres possibles.

Soit $\varphi \in S_n$. On sait que $\mathscr{A}_n$ **est engendré par les 3-cycles** (c.f exercice 5), donc pour que φ stabilise $\mathscr{A}_n$, il suffit que l'image des 3-cycles en fasse partie. Or si γ est un 3-cycle, γ est d'ordre 3, donc $\varphi(\gamma)$ est d'ordre divisant 3, mais ce n'est pas l'identité car φ est injectif et $\gamma \neq id$, donc $\varphi(\gamma)$ est d'ordre 3. Or **l'ordre d'une permutation est le PPCM des longueurs des cycles qui interviennent dans sa décomposition**, on en déduit que tous les cycles intervenant dans la décomposition de $\varphi(\gamma)$ sont des 3-cycles, donc que $\varphi(\gamma) \in \mathscr{A}_n$. **Ainsi, tout automorphisme de S_n stabilise $\mathscr{A}_n$.**

$\mathscr{A}_n$ est un sous-groupe distingué de S_n (c'est le noyau du morphisme signature), il est donc **stable par tout automorphisme intérieur de** S_n (c.f définition d'un sous-groupe distingué). Le résultat que l'on vient de prouver est donc un corollaire de celui de l'exercice suivant, bien plus puissant et difficile.

Solution de l'exercice 9 :

Question 1 : Soit $\sigma \in S_n$. Montrons que $Z(\sigma)$ est un sous-groupe de S_n. Tout d'abord, $Z(\sigma) \subset S_n$ et $id \in Z(\sigma)$ donc $Z(\sigma) \neq \emptyset$. Ensuite, si $\tau, \tau' \in Z(\sigma)$ alors $\sigma \circ (\tau \circ \tau') = \sigma \circ \tau \circ \tau' = \tau \circ \sigma \circ \tau' = \tau \circ \tau' \circ \sigma = (\tau \circ \tau') \circ \sigma$ donc $\tau \circ \tau' \in Z(\sigma)$. Enfin, si $\tau \in Z(\sigma)$, $\sigma \circ \tau = \tau \circ \sigma$ donc en composant chaque membre par τ^{-1} à droite et à gauche on obtient $\tau^{-1} \circ \sigma = \sigma \circ \tau^{-1}$ i.e $\tau^{-1} \in Z(\sigma)$.

Ensuite, soit $\varphi \in Aut(S_n)$. Soit $\tau \in \varphi(Z(\sigma))$. Il existe $\tau' \in Z(\sigma)$ telle que $\tau = \varphi(\tau')$ et alors, $\tau \circ \varphi(\sigma) = \varphi(\tau') \circ \varphi(\sigma) = \varphi(\tau' \circ \sigma) = \varphi(\sigma \circ \tau') = \varphi(\sigma) \circ \varphi(\tau') = \varphi(\sigma) \circ \tau$ donc $\tau \in Z(\varphi(\sigma))$ et ainsi $\varphi(Z(\sigma)) \subset Z(\varphi(\sigma))$. Or, si $\tau \in Z(\varphi(\sigma))$ alors $\tau \circ \varphi(\sigma) = \varphi(\sigma) \circ \tau$. En prenant l'image de chacun des membres par φ^{-1} on obtient $\varphi^{-1}(\tau) \circ \sigma = \sigma \circ \varphi^{-1}(\tau)$ donc $\varphi^{-1}(\tau) \in Z(\sigma)$ puis
$\tau = \varphi(\varphi^{-1}(\sigma)) \in \varphi(Z(\sigma))$ d'où $Z(\varphi(\sigma)) \subset \varphi(Z(\sigma))$ et ainsi, $Z(\varphi(\sigma)) = \varphi(Z(\sigma))$.

Question 2 : Supposons que σ s'écrive $\tau_1 \dots \tau_k$ où les τ_i sont des transpositions à supports disjoints.
$\forall \gamma \in S_n, \gamma \in Z(\sigma) \iff \gamma \circ \sigma \circ \gamma^{-1} = \sigma$. Or, si on note $\tau_i = (x_1^{(i)}, x_2^{(i)})$ pour $i \in \{1, \dots, k\}$ alors d'après la formule de conjugaison des cycles, $\gamma \circ \sigma \circ \gamma^{-1} = (\gamma(x_1^{(1)}), \gamma(x_2^{(1)})) \dots (\gamma(x_1^{(r)}), \gamma(x_2^{(r)}))$.
Notons $\tau_i' = (\gamma(x_1^{(i)}), \gamma(x_2^{(i)}))$. Pour que γ soit dans $Z(\sigma)$, il faut et il suffit que $\{\tau_1, \dots, \tau_k\} = \{\tau_1', \dots, \tau_k'\}$. Il y a $(n-2k)\,!$ possibilités de permuter les $n-2k$ éléments de S_n autres que les $x_1^{(i)}, x_2^{(i)}$, il y a $k\,!$ correspondances bijectives entre $\{\tau_1, \dots, \tau_k\}$ et $\{\tau_1', \dots, \tau_k'\}$, i.e $k\,!$ d'appareiller chaque τ_i avec un τ_j' mais pour chaque τ_i que l'on appareille avec un τ_j' on a deux possibilités : soit on envoie $x_1^{(i)}$ sur $x_1^{(j)}$ et $x_2^{(i)}$ sur $x_2^{(j)}$, soit on envoie $x_1^{(i)}$ sur $x_2^{(j)}$ et $x_2^{(i)}$ sur $x_1^{(j)}$.
Dès lors, si $\sigma = \tau_1 \dots \tau_k$ alors $|Z(\sigma)| = 2^k k\,!(n-2k)\,!$.

Question 3 : Soit τ une transposition, on écrit $\varphi(\tau)$ comme produit de k transpositions $\tau_1 \dots \tau_k$. L'objectif est de montrer que $k = 1$. D'après la question 1, $Z(\varphi(\tau)) = \varphi(Z(\tau))$. Or, puisque φ est bijective, $|\varphi(Z(\tau))| = |Z(\tau)|$, donc en utilisant la question 2, $|Z(\varphi(\tau))| = 2^k k\,!(n-2k)\,! = |Z(\tau)| = 2(n-2)\,!$ d'où $2^{k-1} k\,! = (n-2)\dots(n-2k+1)$.
Si $k = 2$, l'équation s'écrit $(n-2)(n-3) = 4$, équation qui n'a pas de solution dans $\mathbb{N}$ puisque le membre de gauche a un facteur impair.
Si $k \geq 3$ on peut écrire :

$$2^{k-1} = \frac{(n-2)\dots(n-2k+1)}{k\,!} = (n-2)\dots(n-k+1)\frac{(n-k)\dots(n-2k+1)}{k!} = (n-2)\dots(n-k+1)\binom{n-k}{k}$$

Pour que le membre de droite n'ait pas de facteur impair, il est nécessaire que $n-2 = n-k+1$ soit $k = 3$, mais alors on obtient $(n-2)\binom{n-3}{3} = 4$ c'est-à-dire $(n-2)(n-3)(n-4)(n-5) = 24$. On remarque que seul $n = 6$ convient mais ce cas est exclu.
Ainsi, $k = 1$ et $\varphi(\tau)$ est une transposition.

Question 4 : Pour montrer que φ est intérieur, il faut trouver σ telle que $\forall u \in S_n$, $\varphi(u) = \sigma \circ u \circ \sigma^{-1}$. Cela semble compliqué. Pour s'aider, il faut se rappeler qu'un morphisme de groupes partant de S_n est entièrement déterminé par l'image des $(1,k), 2 \leq k \leq n$ car celles-ci engendrent S_n. Il suffit donc que σ coïncide avec φ sur ces transpositions pour convenir ! Par ailleurs, il est facile d'exprimer $\sigma \circ u \circ \sigma^{-1}$ quand u est une transposition.

On va s'intéresser aux images des $(1,k), 2 \leq k \leq n$. Tout d'abord, ce sont des transpositions d'après la question 3, notons (x_1, x_2) et (y_1, y_2) les images de $(1,2)$ et $(1,3)$. Alors, (x_1, x_2) et (y_1, y_2) ne peuvent pas commuter, sinon l'injectivité de φ permettrait de conclure que c'est aussi le cas pour $(1,2)$ et $(1,3)$ ce qui n'est pas. Dès lors, $\{x_1, x_2\} \cap \{y_1, y_2\} \neq \emptyset$: sans perte de généralité on peut supposer que $y_1 = x_1$ et on note $y_2 = x_3$. L'objectif est de montrer que $\forall i \in \{2, \ldots, n\}, \exists x_i \in \{1, \ldots, n\}, \varphi((1,i)) = (x_1, x_i)$ où les x_i sont deux-à-deux distincts puisqu'alors, en notant σ la permutation qui à i associe x_i pour $i \in \{1, \ldots, n\}$, la formule de conjugaison des transpositions montrera que φ coïncide avec $u \mapsto \sigma \circ u \circ \sigma^{-1}$ sur les $(1,k), 2 \leq k \leq n$ et on aura fini.

On établit donc pour $i \in \{2, \ldots, n\}$ la propriété suivante :

Il existe $x_1, \ldots, x_i$ deux-à-deux distincts tels que $\forall k \in \{2, \ldots, i\}, \varphi((1,k)) = (x_1, x_k)$

La propriété est vraie pour $i = 2$ et $i = 3$ comme on l'a montré.
Soit $i > 3$, supposons la propriété vraie à l'ordre $i-1$. Puisque $(1,i)$ ne commute avec aucun des $(1,k), 2 \leq k \leq i-1$, $\varphi((1,i))$ est une transposition qui ne commute avec aucun des $\varphi((1,k)) = (x_1, x_k)$, donc son support rencontre chacun des $(x_1, x_k), 2 \leq k \leq i-1$. Supposons par l'absurde que x_1 ne soit pas dedans. Puisque le support de $\varphi((1,i))$ rencontre chacun des (x_1, x_k), tous les x_k sont dedans. Puisque il y en a $i - 2 \geq 2$ (car $i > 3$), et que le support en question ne peut contenir que deux éléments, on a forcément $i = 4$. Alors, puisque x_1 n'est pas dans le support, on en déduit que $\varphi((1,4)) = (x_2, x_3)$.
Or on remarque que $(x_2, x_3) = (x_1, x_3)(x_1, x_2)(x_1, x_3) = \varphi((1,3))\varphi((1,2))\varphi((1,3)) = \varphi((1,3)(1,2)(1,3))$.
Par injectivité, on a alors $(1,4) = (1,3)(1,2)(1,3)$: c'est faux. Ainsi, x_1 est dans le support de $\varphi((1,i))$, reste à nommer x_i l'autre élément pour conclure que la propriété est vraie à l'ordre i.

Dès lors, comme expliqué plus haut, il reste à définir σ la permutation qui à i associe x_i pour $i \in \{1, \ldots, n\}$, la formule de conjugaison des transpositions montre que φ coïncide avec $u \mapsto \sigma \circ u \circ \sigma^{-1}$ sur les $(1,k), 2 \leq k \leq n$ qui engendrent S_n, donc lui est égale. Ainsi, **si $n \neq 6$, tout automorphisme de S_n est intérieur.**

Solution de l'exercice 10 :

Montrons qu'il n'existe pas de morphisme de groupes injectif de S_2 dans $\mathscr{A}_3$. Remarquons que, si G et G' sont deux groupes finis et $\varphi : G \to G'$ un morphisme injectif de groupes, alors $\mathrm{Im}(\varphi)$ est un sous-groupe de G' donc par le théorème de Lagrange, son cardinal divise celui de G'. Or, φ induit un isomorphisme de G vers $\mathrm{Im}(\varphi)$, donc ces deux ensembles sont de même cardinal. Ainsi, **une condition nécessaire pour qu'il existe un morphisme de groupes injectif d'un groupe fini G vers un autre groupe fini G' est que $|G| \mid |G'|$.** Une autre condition nécessaire est qu'**il existe un sous-groupe de G' de même cardinal que G.** Puisque 2 ne divise pas $3 = |\mathscr{A}_3|$, il n'existe pas de morphisme de groupes injectif de S_2 dans $\mathscr{A}_3$.

Pour le cas $n = 3$, on va montrer que $\mathscr{A}_4$ n'a pas de sous-groupe d'ordre $6 = |S_6|$, ainsi la deuxième condition nécessaire ne sera pas validée. On va en fait montrer le résultat plus fort suivant : **si G est un groupe fini d'ordre $2n$ et H un sous-groupe de G d'ordre n, alors pour tout $g \in G$, $g^2 \in H$.** En effet, donnons-nous $g \in G$. Si $g \in H$, $g^2 \in H$. Sinon, $H \neq gH$ donc $G/H = \{H, gH\}$ car H est de cardinal n donc d'indice 2. On a donc la partition $G = H \bigcup gH$. Dès lors, si $g^2 \in gH$, $\exists h \in H$, $g^2 = gh$ et donc $g = h \in H$: absurde par hypothèse. Ainsi, $g^2 \in H$.
Dans notre cas, $\mathscr{A}_4$ est d'ordre $12 = 2 \times 6$. S'il existait H un sous-groupe de $\mathscr{A}_4$ de cardinal 6, alors H contiendrait tous les carrés d'éléments de $\mathscr{A}_4$. Or, si τ est un 3-cycle, $\tau = (\tau^{-1})^2$ car τ est d'ordre 3, donc H contient tous les 3-cycles de $\mathscr{A}_4$, au nombre de 8 : c'est absurde. (Au fait, combien y a-t-il de r-cycles, $2 \leq r \leq n$, dans S_n ?). Ainsi, il n'existe pas de morphisme de groupes injectif de S_3 dans $\mathscr{A}_4$.

Revenons au cas général où $n \geq 4$. On a vu qu'une condition nécessaire pour qu'il existe un morphisme de groupes injectif de S_n dans $\mathscr{A}_{n+1}$ était que $|S_n| = n\,!$ divise $|\mathscr{A}_{n+1}| = \frac{(n+1)\,!}{2}$. Or, si tel était le cas, il existerait un entier k tel que $\frac{(n+1)\,!}{2} = n\,!k$ et donc $n = 2k + 1$: une condition nécessaire est que n soit impair. On supposera dorénavant que c'est le cas et on notera $n = 2k + 1$.

Raisonnons par l'absurde en supposant qu'il existe un morphisme de groupes injectif φ de S_{2k+1} vers $\mathscr{A}_{2k+2}$. Il est temps de ressortir le super-morphisme qui nous a sauvés dans l'exercice 7 :

$$\begin{aligned} \psi \ : \mathscr{A}_{2k+2} &\to S(\mathscr{A}_{2k+2}/\mathrm{Im}(\varphi)) \\ \sigma &\mapsto \psi(\sigma) \end{aligned}$$

où :

$$\begin{aligned} \psi(\sigma) \ : \mathscr{A}_{2k+2}/\mathrm{Im}(\varphi) &\to \mathscr{A}_{2k+2}/\mathrm{Im}(\varphi) \\ \tau H &\mapsto \sigma\tau H \end{aligned}$$

On montre de même qu'en exercice 7 que ψ est bien défini et que c'est un morphisme de groupes. Son noyau est un sous-groupe distingué de $\mathscr{A}_{2k+2}$. Or, nous considérons le cas $n \geq 5$,

donc $\mathscr{A}_{2k+2}$ est simple d'après l'exercice 5 : $\ker(\psi)$ est donc soit égal à $\{id\}$, soit à $\mathscr{A}_{2k+2}$. Mais :

$$|S(\mathscr{A}_{2k+2}/\mathrm{Im}(\varphi))| = \left(\frac{(2k+2)\,!}{2(2k+1)\,!}\right)\,! = (k+1)\,!$$

et $|\mathscr{A}_{2k+2}| = \frac{(2k+2)\,!}{2} = (k+1)(2k+1)\,! > (k+1)\,!$ donc ψ ne peut pas être injectif. On en déduit que $\ker(\psi) = \mathscr{A}_{2k+2}$. Mais comme on a pu le voir dans l'exercice 7, $\mathscr{A}_{2k+2} = \ker(\psi) \subset \mathrm{Im}(\varphi)$ ($= H$ dans le contexte de l'exercice 7). Puisque $\mathrm{Im}(\varphi) \subset \ker(\psi)$, on en déduit que $H = \mathscr{A}_{2k+2}$. En passant aux cardinaux, on obtient $(2k+1)\,! = (k+1)(2k+1)\,!$: c'est absurde.

Ainsi, **il n'existe pas de morphisme de groupes injectif de S_n dans $\mathscr{A}_{n+1}$ pour** $n \geq 2$.