Recasages possibles : 103, 105, 108
Référence : Algèbre et géométrie, Rombaldi (p. 49-51) - Cours d'algèbre, Perrin (p. 28-30).

Développement Soit $n \in \mathbb{N}_{\geqslant 5}$

Lemme 1 $\mathfrak{A}_n$ est engendré par les 3-cycles, et les 3-cycles sont $\mathfrak{A}_n$-conjugués.

Théorème 2 Pour $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.

Corollaire 3 Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}, \mathfrak{A}_n$ et $\mathfrak{S}_n$.

- *Preuve du Lemme 1* : Notons $G \subset \mathfrak{S}_n$ le sous-groupe engendré par les 3-cycles. Comme un 3-cycle est une permutation paire, (car $3 - 1 = 2$ est pair !), on a immédiatement $G \subset \mathfrak{A}_n$. Réciproquement si $\sigma \in \mathfrak{A}_n$, on sait que σ est produit de p transpositions (car les transpositions engendrent $\mathfrak{S}_n$). Or, $\varepsilon(\sigma) = 1$ donc p est nécessairement pair. Montrons alors que le produit de deux tranpositions est toujours un produit de 3-cycles. Pour $i, j, k, l \in [\![1, n]\!]$ deux à deux distincts, on a

$$(i\ j)(j\ k) = (i\ j\ k) \quad \text{puis} \quad (i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l).$$

  Enfin on a $(i\ j)(i\ j) = \mathrm{id}$ qui est le cube de n'importe quel 3-cycle. Ainsi, que les supports des deux transpositions que l'on compose soient disjoints ou non, on obtient dans tous les cas un produit de (un ou deux ou trois) 3-cycles. Ainsi, σ est produit de 3-cycles, ce qui montre bien que $G = \mathfrak{A}_n$. Montrons alors que les 3-cycles sont bien $\mathfrak{A}_n$-conjugués, en utilisant le fait qu'ils sont $\mathfrak{S}_n$-conjugués, car ont même type. Soient $(a\ b\ c)$ et $(d\ e\ f)$ deux 3-cycles, et soit $\sigma \in \mathfrak{S}_n$ telle que

$$\sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f).$$

  Si $\sigma \in \mathfrak{A}_n$, les deux 3-cycles en présence sont bien $\mathfrak{A}_n$-conjugués, donc on a fini. Sinon, σ est de signature -1. Comme $n \geqslant 5$, on peut se donner deux entiers $i, j \in [\![1, n]\!]$ distincts de a, b et c et poser $\sigma' = \sigma \circ (i\ j)$. Alors, $\sigma' \in \mathfrak{A}_n$ et on a

$$\sigma'(a\ b\ c)\sigma'^{-1} = \sigma(i\ j)(a\ b\ c)(i\ j)\sigma^{-1} = \sigma(a\ b\ c)\sigma^{-1} = (d\ e\ f)$$

  car $(i\ j)$ et $(a\ b\ c)$ étant à supports disjoints, elles commutent, et $(i\ j)^{-1} = (i\ j)$. Ainsi, on a dans tous les cas $(a\ b\ c)$ et $(d\ e\ f)$ qui sont $\mathfrak{A}_n$-conjugués, ce qui termine la preuve du **Lemme 1**.

- *Preuve du Théorème 2* : Soit H un sous-groupe distingué de $\mathfrak{A}_n$ non réduit à $\{\mathrm{id}\}$. On veut montrer que $H = \mathfrak{A}_n$, mais remarquons qu'il suffit de montrer que $\mathfrak{A}_n$ contient un 3-cycle. En effet, si $(a\ b\ c) \in H$, et si $(d\ e\ f)$ est un autre 3-cycle, alors $(a\ b\ c)$ et $(d\ e\ f)$ sont $\mathfrak{A}_n$ conjugués d'après le **Lemme 1**, *i.e* il existe $\sigma \in \mathfrak{A}_n$ telle que

$$(d\ e\ f) = \sigma(a\ b\ c)\sigma^{-1}.$$

  Alors, comme H est distingué dans $\mathfrak{A}_n$, $(d\ e\ f) \in H$, et ainsi H contient tous les 3-cycles. Par suite, H contient le sous-groupe engendré par les 3-cycles, qui n'est autre que $\mathfrak{A}_n$ d'après le **Lemme 1**. Ainsi, on a bien $H = \mathfrak{A}_n$ dès que H contient un 3-cycle.

  Montrons alors que H contient bel et bien un 3-cycle. Fixons $\sigma \in H \setminus \{\mathrm{id}\}$, et $x \in [\![1, n]\!]$ tel que $y := \sigma(x) \neq x$. On choisit alors $z \in [\![1, n]\!]$ distinct de x,y et $\sigma(y)$ de sorte que le 3-cycle $\gamma = (x\ z\ y)$ ne commute pas avec σ. En effet, on a alors par injectivité de γ

$$\sigma\gamma(y) = \sigma(x) = y = \gamma(z) \neq \gamma\sigma(y).$$

  On considère alors le commutateur σ' de σ et γ : $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1}$. On a $\sigma' \neq \mathrm{id}$ car σ et γ ne commutent pas par construction. Par associativité de la composition, on a d'une part $\sigma' = \sigma(\gamma\sigma^{-1}\gamma^{-1}) \in H$ car $\sigma^{-1} \in H$, $\gamma \in \mathfrak{A}_n$ et H est distingué dans $\mathfrak{A}_n$, et d'autre part $\sigma' = (\sigma\gamma\sigma^{-1})\gamma^{-1}$, ce qui montre que σ' est un produit de deux 3-cycles. Plus précisément,

$$\begin{aligned} \sigma' = \big(\sigma(x\ z\ y)\sigma^{-1}\big)\gamma^{-1} &= \big(\sigma(x)\ \sigma(z)\ \sigma(y)\big)(x\ y\ z) \\ &= \big(y\ \sigma(z)\ \sigma(y)\big)(x\ y\ z) \end{aligned}$$

  Ainsi, on voit que le support de σ' est inclus dans l'ensemble

$$F = \{x, y, z, \sigma(y), \sigma(z)\}$$

  qui est de cardinal $\leqslant 5$. On considère alors la décomposition de σ' en produit de cycles à supports disjoints : $\sigma' = c_1 \cdots c_k$. On a nécessairement $k \geqslant 1$ car $\sigma' \neq \mathrm{id}$, et $k \geqslant 2$ car sinon, le support de σ' serait au moins de cardinal 6 (le support minimal d'un produit de trois cycles à supports disjoints, en l'occurrence celui d'une triple transposition), contredisant le fait qu'il est inclus dans F. Il n'y a donc que trois cas possibles : ou bien $k = 2$ et σ' est une bitransposition, ou bien $k = 1$ et σ' est un 3-cycle ou un 5-cycle. Si σ' est un 3-cycle, on a trouvé un 3-cycle dans H, donc on a terminé. Traitons les deux autres cas :

· Si $\sigma' = (a\ b)(c\ d)$, on choisit $e \notin \{a, b, c, d\}$ et on pose $\tau = (a\ b\ e) \in \mathfrak{A}_n$. Alors le commutateur $\sigma'' = \sigma'\tau\sigma'^{-1}\tau^{-1}$ est dans H (pour les mêmes raisons que σ') et on a

$$\begin{aligned}\sigma'' &= \big(\sigma'(a\ b\ e)\sigma'^{-1}\big)(a\ e\ b)\\ &= \big((\sigma'(a)\ \sigma'(b)\ \sigma'(e)\big)(a\ e\ b)\\ &= \big(b\ a\ e)(a\ e\ b)\\ &= (a\ b\ e)\end{aligned}$$

On a donc trouvé un 3-cycle dans H et on a terminé.

· Si $\sigma' = (a\ b\ c\ d\ e)$, alros on pose $\tau = (a\ b\ c) \in \mathfrak{A}_n$ et on considère à nouveau le commutateur $\sigma'' = \sigma'\tau\sigma'^{-1}\tau^{-1} \in H$. On a

$$\begin{aligned}\sigma'' &= \big(\sigma'(a\ b\ c)\sigma'^{-1}\big)(a\ c\ b)\\ &= \big(\sigma'(a)\ \sigma'(b)\ \sigma'(c)\big)(a\ c\ b)\\ &= (b\ c\ d)(a\ c\ b)\\ &= (a\ d\ b)\end{aligned}$$

On a encore trouvé un 3-cycle dans H et on a terminé.
Dans tous les cas H contient bel et bien un 3-cycle et donc par l'argument vu précédemment, $H = \mathfrak{A}_n$, ce qui montre que $\mathfrak{A}_n$ est simple, et achève la preuve du **Théorème 2**.

- *Preuve du Corollaire 3* : Soit H un sous-groupe distingué de $\mathfrak{S}_n$. On considère alors $H \cap \mathfrak{A}_n$ qui est un sous-groupe distingué de $\mathfrak{A}_n$. D'après le **Théorème 2**, on a alors $H \cap \mathfrak{A}_n = \mathfrak{A}_n$ ou $H \cap \mathfrak{A}_n = \{\mathrm{id}\}$. Dans le premier cas, on obtient $\mathfrak{A}_n \subset H$, et donc $H = \mathfrak{A}_n$ ou $\mathfrak{S}_n$ (qui sont les seuls sous-groupes de $\mathfrak{S}_n$ contenant $\mathfrak{A}_n$ pour des raisons d'indice). Dans le deuxième cas, on considère le morphisme signature restreint $\varepsilon_{|H} : H \to \{\pm 1\}$. Ce morphisme est injectif car

$$\mathrm{Ker}(\varepsilon_{|H}) = H \cap \mathrm{Ker}(\varepsilon) = H \cap \mathfrak{A}_n = \{\mathrm{id}\}.$$

Il induit donc un isomorphisme $H \simeq \varepsilon(H) \subset \{\pm 1\}$ de sorte que $\#H \leqslant 2$. Supposons que $H = \{\mathrm{id}, \sigma\}$ avec $\sigma \neq \mathrm{id}$. Alors, pour $\tau \in \mathfrak{S}_n$, comme H est distingué, on a $\tau\sigma\tau^{-1} \in H$, donc $\tau\sigma\tau^{-1} = \mathrm{id}$ ou $\tau\sigma\tau^{-1} = \sigma$. Si $\tau\sigma\tau^{-1} = \mathrm{id}$, alors $\tau\sigma = \tau$, ce qui implique $\sigma = \mathrm{id}$ et est absurde. Ainsi pour tout $\tau \in \mathfrak{S}_n$, on a $\tau\sigma\tau^{-1} = \sigma$, *i.e* $\tau\sigma = \sigma\tau$ et donc σ est dans le centre de $\mathfrak{S}_n$. Or, ce centre est trivial car $n \geqslant 5$, donc $\sigma = \mathrm{id}$, ce qui est absurde. On a donc $\#H = 1$ et $H = \{\mathrm{id}\}$, ce qui conclut la preuve du **Corollaire 3**.