Recasages possibles : 101, 103, 104, 105, 108.
Référence : Cours d'algèbre, Perrin (p. 30-32).

Développement 1

Lemme 1 Soient $n \in \mathbb{N}_{\geqslant 2}$ et $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ envoie toute transposition sur une transposition, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

Théorème 2 Si $n \neq 6$, alors $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

- *Preuve du Lemme 1* : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ envoyant toute transposition sur une transposition. On va utiliser le fait que les tranpositions $\tau_i = (1\ i)$, pour $i \geqslant 2$, engendrent $\mathfrak{S}_n$. Par hypothèse, pour tout $i \geqslant 2$, $\varphi(\tau_i)$ est une transposition. Par ailleurs, si $i \neq j$, les transpositions τ_i et τ_j ne commutent pas. En effet,

$$\tau_i\tau_j = (1\ i)(1\ j) = (1\ j\ i) \neq (1\ i\ j) = (1\ j)(1\ i) = \tau_j\tau_i.$$

Par conséquent, comme φ est un automorphisme, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas non plus (sinon en appliquant φ^{-1}, on obtiendrait que τ_i et τ_j commutent). En particulier, les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas disjoints. Écrivons donc $\varphi(\tau_2) = (\alpha_1\ \alpha_2)$ et $\varphi(\tau_3) = (\alpha_1\ \alpha_3)$, où $\alpha_1, \alpha_2, \alpha_3 \in [\![1, n]\!]$ sont deux à deux distincts. On sait alors que pour tout $i \in [\![4, n]\!]$, le support de $\varphi(\tau_i)$ intersecte $\{\alpha_1, \alpha_2\}$ et $\{\alpha_1, \alpha_3\}$. Montrons que dans tous les cas, α_1 est dans le support de $\varphi(\tau_i)$ pour tout i. Si ce n'était pas le cas, on aurait pour un $i \geqslant 4$, $\varphi(\tau_i) = (\alpha_2\ \alpha_3)$. Mais alors de l'égalité $(\alpha_1\ \alpha_2)(\alpha_1\ \alpha_3)(\alpha_2\ \alpha_3) = (\alpha_1\ \alpha_3)$, en appliquant φ^{-1}, on obtiendrait

$$(1\ 2)(1\ 3)(1\ i) = (1\ i\ 3\ 2) = (1\ 3)$$

ce qui est manifestement faux. Ainsi, pour tout $i \in [\![2, n]\!]$, il existe $\alpha_i \in [\![1, n]\!]$ tel que $\alpha_i \neq \alpha_1$ et $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. Les α_i sont nécessairement distincts deux à deux par injectivité de φ, donc on a par cardinalité

$$\{\alpha_2, \ldots, \alpha_n\} = [\![1, n]\!] \backslash \{\alpha_1\} \implies \{\alpha_1, \ldots, \alpha_n\} = [\![1, n]\!].$$

On a donc construit une permutation $\alpha \in \mathfrak{S}_n$. Or, par définition, $\forall i \geqslant 2$, on a $\varphi(\tau_i) = (\alpha_1\ \alpha_i) = \alpha\tau_i\alpha^{-1} = i_\alpha(\tau_i)$, où i_α est l'automorphisme intérieur de conjugaison par α. Ainsi, φ et i_α coïncident sur une partie génératrice de $\mathfrak{S}_n$, donc sur $\mathfrak{S}_n$. En particulier $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$, ce qui termine la preuve du **Lemme 1**.

- *Preuve du Théorème 2* : Supposons $n \neq 6$. On va utiliser l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison. Si $\sigma \in \mathfrak{S}_n$, on note $c(\sigma)$ son centralisateur, *i.e* son stabilisateur pour cette action. Montrons tout d'abord que $D(\mathfrak{S}_n) = \mathfrak{A}_n$. La signature d'un commutateur $\sigma\tau\sigma^{-1}\tau^{-1}$ est clairement 1 (car la signature est un morphisme de groupes de $\mathfrak{S}_n$ dans $\{\pm 1\}$ qui est abélien), donc l'inclusion $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ est claire. Pour montrer l'inclusion réciproque, il suffit de montrer que tout 3-cycle appartient à $D(\mathfrak{S}_n)$, puisque les 3-cycles engendrent $\mathfrak{S}_n$. Soit donc $\sigma = (a\ b\ c)$ un 3-cycle. On a $\sigma^2 = (a\ c\ b)$ qui est encore un 3-cycle, donc σ et σ^2 sont $\mathfrak{S}_n$-conjugués. Il existe donc $\tau \in \mathfrak{S}_n$ tel que $\sigma^2 = \tau\sigma\tau^{-1}$, d'où $\sigma = \tau\sigma\tau^{-1}\sigma^{-1} \in D(\mathfrak{S}_n)$. On a bien montré que $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Comme $\mathfrak{A}_n = D(\mathfrak{S}_n)$ est un sous-groupe caractéristique de $\mathfrak{S}_n$, on a $\varphi(\mathfrak{A}_n) = \mathfrak{A}_n$. Ainsi, l'imagine par φ d'une transposition est une permutation impaire, et d'ordre 2, donc est un produit d'un nombre impair k de transpositions à supports disjoints. Si pour toute les transpositions $k = 1$, alors on a terminé d'après le **Lemme 1**. Sinon, il existe une transposition telle que $k \geqslant 3$, auquel cas on a nécessairement $n \geqslant 7$, ce que l'on suppose désormais. Soit $\tau = (a\ b)$ une telle transposition, et soit $\tau' = \varphi(\tau)$. Notons $F = [\![1, n]\!] \backslash \{a, b\}$. Pour $\sigma \in \mathfrak{S}_n$, on a

$$\sigma \in c(\tau) \Leftrightarrow \sigma\tau\sigma^{-1} = (\sigma(a)\ \sigma(b)) = (a\ b) \Leftrightarrow \sigma(F) = F.$$

Ainsi, l'action naturelle de $c(\tau)$ sur $[\![1, n]\!]$, induit par restriction une action sur F. Autrement dit, on dispose du morphisme de groupes

$$r : \left| \begin{array}{ccc} c(\tau) & \longrightarrow & \mathfrak{S}_F \simeq \mathfrak{S}_{n-2} \\ \sigma & \longmapsto & \sigma_{|F} \end{array} \right.$$

Par ailleurs, ce morphisme est surjectif car étant donné $\widetilde{\sigma} \in \mathfrak{S}_F$, en prolongeant $\widetilde{\sigma}$ à $[\![1, n]\!]$ par l'identité sur $\{a, b\}$, on obtient un antécédent de $\widetilde{\sigma}$ par r. Enfin, son noyau est $\mathrm{Ker}(\tau) = \{1, \tau\}$. Notons $\tau' = \tau_1 \cdots \tau_k$ où les $\tau_i = (a_{2i-1}\ a_{2i})$ sont des transpositions à supports disjoints. Étant à supports disjoints, les τ_i commutent

deux à deux, donc on a pour tout $i \in [\![1,k]\!]$,

$$\tau_i \tau' \tau_i^{-1} = \tau_i \tau_1 \cdots \tau_k \tau_i = \tau_1 \cdots \tau_i^3 \cdots \tau_k = \tau_1 \cdots \tau_i \cdots \tau_k = \tau'.$$

Ainsi, $\tau_i \in c(\tau')$ donc $N = \left\langle (\tau_i)_{i\in[\![1,k]\!]} \right\rangle$ est un sous-groupe de $c(\tau')$. Comme tous ses éléments sont d'ordre 2, et que $\#N = 2^k$, on a $N \simeq (\mathbb{Z}/2\mathbb{Z})^k$. C'est de plus un sous-groupe distingué de $c(\tau')$: si $\sigma \in c(\tau')$, il suffit de montrer que $\sigma\tau_i\sigma^{-1} \in N$ pour tout i. Or, par définition,

$$\sigma\tau'\sigma = \tau' = \tau_1 \cdots \tau_k.$$

Par ailleurs,

$$\sigma\tau'\sigma^{-1} = (\sigma\tau_1\sigma^{-1}) \cdots (\sigma\tau_k\sigma^{-1}) = \big(\sigma(a_1)\ \sigma(a_2)\big) \cdots \big(\sigma(a_{2n-1})\ \sigma(a_{2n})\big)$$

Par unicité de la décomposition en produit de cycles à supports disjoints, on obtient que pour tout $i \in [\![1,k]\!]$, il existe $j \in [\![1,k]\!]$ tel que $\sigma\tau_i\sigma^{-1} = \tau_j \in N$. Ainsi, comme les τ_i engendrent N, on a bien $\sigma N \sigma^{-1} \subset N$ pour tout σ, *i.e* $N \lhd c(\tau')$. Or, φ induit un isomorphisme de groupes entre $c(\tau)$ et $c(\tau')$, donc via cet isomorphisme, N est envoyé sur $N' \lhd c(\tau)$, toujours isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. Alors, $r(N')$ est un sous-groupe distingué de $\mathfrak{S}_{n-2}$, *i.e* comme $n-2 \geqslant 5$ c'est nécessairement $\{\mathrm{id}\}$, $\mathfrak{A}_{n-2}$ ou $\mathfrak{S}_{n-2}$. Or, en considérant le morphisme de groupes surjectif $\tilde{r} : N' \to r(N')$ induit par r, on a un isomorphisme $r(N') \simeq N'/(N' \cap \mathrm{Ker}(r))$. En particulier, on a $\#r(N') = 2^k$ ou 2^{k-1} selon que $N' \cap \mathrm{Ker}(r) = \{\mathrm{id}\}$ ou $\mathrm{Ker}(r)$. Or, $k \geqslant 3$, donc $r(N') \neq \{\mathrm{id}\}$ et les cardinaux $\#\mathfrak{A}_{n-2} = \frac{(n-2)!}{2}$ et $\#\mathfrak{S}_{n-2} = (n-2)!$ ne sont pas des puissances de 2 (car sont par exemple divisible par 3). Le sous-groupe distingué $r(N')$ de $\mathfrak{S}_{n-2}$ est donc distinct de $\{\mathrm{id}\}$, $\mathfrak{A}_{n-2}$ et $\mathfrak{S}_{n-2}$, ce qui est absurde.

Ceci nous assure que toutes les transpositions de $\mathfrak{S}_n$ sont envoyées par φ sur des transpositions ($k = 1$), donc par le **Lemme 1**, φ est un automorphisme intérieur, ce qui achève la preuve du **Théorème 2**.

Commentaires et prolongements :

- Ce développement est plus technique qu'il n'y parait, mais reste faisable en 15 minutes à condition de bien connaître les différents pièges et les quelques astuces de raisonnement. J'ai l'impression que le fait que N soit isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ est inutile puisqu'on ne se sert que de son cardinal, mais bon ça ne mange pas de pain de savoir qu'un groupe G engendré par une famille d'éléments d'ordre 2 qui commutent deux à deux est nécessairement une puissance de $\mathbb{Z}/2\mathbb{Z}$. Le plus économe est certainement de construire sur G (qui est nécessairement abélien) une loi de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel compatible avec la loi de groupe. Le choix d'une telle loi est limité puisqu'on doit naturellement poser $0 \cdot g = e_G$ et $1 \cdot g = g$ pour tout $g \in G$. Reste à vérifier que cela vérifie bien les axiomes d'une structure d'espace vectoriel, ce qui est garantit par le fait que les éléments soient d'ordre 2.

- La question naturelle (bien que non triviale) qui vient après ce développement est certainement "que se paso old el paso dans le cas $n = 6$?". Je vais tenter de détailler le raisonnement que propose Perrin, qui utilise à plusieurs reprises le fait que les seuls sous-groupes distingués de $\mathfrak{S}_n$ soient (pour $n \neq 4$) $\{\mathrm{id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$. Il faut donc être à l'aise sur ce corollaire relativement immédiat de la simplicité de $\mathfrak{A}_n$ pour $n \neq 4$. Posons d'abord quelques notations. Si X est un ensemble, et $x \in X$, alors on note $S(x)$ le stabilisateur de x sous l'action naturelle de $\mathfrak{S}_X$ sur X. On a donc
$$S(x) = \big\{\sigma \in \mathfrak{S}_X : \sigma(x) = x\big\}.$$
Si $x, y \in X$, puisque l'action $\mathfrak{S}_X \circlearrowright X$ est transitive, il existe $\sigma \in \mathfrak{S}_X$ telle que $\sigma(x) = y$ (prendre la transposition qui échange x et y par exemple) et alors on a $S(y) = \sigma S(x) \sigma^{-1}$. Ainsi, les sous-groupes $S(x)$ de $\mathfrak{S}_X$ sont conjugués. Réciproquement, si H est un sous-groupe de $\mathfrak{S}_X$ conjugué à un $S(x)$, alors en écrivant $H = \sigma S(x) \sigma^{-1}$ pour une permutation $\sigma \in \mathfrak{S}_X$, on voit que $H = S\big(\sigma(x)\big)$ (le principe de conjugaison si cher à tout géomètre ou groupiste est partout). On montre alors le lemme suivant :

3 Lemme : Supposons qu'il existe un sous-groupe d'indice 6 de $\mathfrak{S}_6$ différent des $S(i)$ pour $i \in [\![1,6]\!]$. Alors, $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Démonstration. Soit H un sous-groupe de $\mathfrak{S}_6$ d'indice 6 et différent des $S(i)$. En particulier, H n'est pas conjugué aux $S(i)$ d'après la discussion précédente. On considère alors l'action $\mathfrak{S}_6 \circlearrowright \mathfrak{S}_6/H$ par translation à gauche, qui se représente par un morphisme de groupes

$$\varphi : \mathfrak{S}_6 \longrightarrow \mathfrak{S}_{\mathfrak{S}_6/H}.$$

Notons que φ est injectif car $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué de $\mathfrak{S}_6$, donc c'est soit $\{\mathrm{id}\}$, soit $\mathfrak{A}_6$ soit $\mathfrak{S}_6$. Or, si $\sigma \in \mathrm{Ker}(\varphi)$, alors en particulier, σ fixe l'élément H de $\mathfrak{S}_n/H$ donc $\sigma H = H$, ce qui donne $\sigma \in H$. Ainsi, $\mathrm{Ker}(\varphi) \subseteq H$ d'où l'inégalité $\#\mathrm{Ker}(\varphi) \leqslant \#H = 5! < \frac{6!}{2}$. Par conséquent, on a bien $\mathrm{Ker}(\varphi) = \{\mathrm{id}\}$, ce qui signifie que φ est injectif. Or, H étant d'indice 6 dans $\mathfrak{S}_6$, $\mathfrak{S}_6/H$ est de cardinal 6 donc $\#\mathfrak{S}_{\mathfrak{S}_6/H} = 6!$. Ainsi, par égalité des cardinaux, φ est un isomorphisme de groupes. Par ailleurs, $\varphi(H) = S(H)$ (pour l'action naturelle $\mathfrak{S}_{\mathfrak{S}_6/H} \curvearrowright \mathfrak{S}_6/H$).

D'autre part, si $f : \mathfrak{S}_6/H \to [\![1,6]\!]$ est une énumération des éléments de $\mathfrak{S}_6/H$ (c'est-à-dire une bijection), avec $f(H) = 1$, alors f induit l'isomorphisme de groupes

$$\psi : \left| \begin{array}{ccc} \mathfrak{S}_{\mathfrak{S}_6/H} & \longrightarrow & \mathfrak{S}_6 \\ \sigma & \longmapsto & f\sigma f^{-1}. \end{array} \right.$$

De plus, on a $\psi\big(S(H)\big) = S\big(f(H)\big) = S(1)$ et donc $\psi\big(\varphi(H)\big) = S(1)$. Ainsi, on a construit un automorphisme $\psi \circ \varphi$ de $\mathfrak{S}_6$ tel que $(\psi \circ \varphi)(H) = S(1)$. Or, par hypothèse, H et $S(1)$ ne sont pas conjugués, donc $\psi \circ \varphi$ ne peut pas être intérieur, ce qui signifie bien que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$ et termine la preuve de **3**.

On peut alors montrer le théorème suivant :

4 Théorème : $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$

Démonstration. D'après **3**, il nous suffit d'exhiber un sous-groupe d'indice 6 de $\mathfrak{S}_6$, différent des $S(i)$ pour $i \in [\![1,6]\!]$. Pour cela, considérons l'ensemble X des 5-Sylow de $\mathfrak{S}_5$ (qui sont ses sous-groupes d'ordre 5). Par les théorèmes de Sylow, si $n_5 = \#X$, on a $n_5 \equiv 1\ [5]$ et $n_5 \mid 24$. Ainsi, $n_5 \in \{1,6\}$ mais si $n_5 = 1$, alors à nouveau par les théorèmes de Sylow, on sait que l'unique 5-Sylow de $\mathfrak{S}_5$ est distingué, ce qui est impossible puisque ni $\{\mathrm{id}\}$, ni $\mathfrak{A}_5$ ni $\mathfrak{S}_5$ n'est d'ordre 5. Ainsi, $n_5 = 6$. On fait alors agir transitivement $\mathfrak{S}_5$ sur X par conjugaison, ce qui fournit un morphisme de groupes

$$\varphi : \mathfrak{S}_5 \longrightarrow \mathfrak{S}_X \simeq \mathfrak{S}_6.$$

Le morphisme φ est injectif puisque $\mathrm{Ker}(\varphi) \lhd \mathfrak{S}_5$ et $\mathrm{Ker}(\varphi) \neq \mathfrak{A}_5$ ou $\mathfrak{S}_5$ puisque l'action étant transitive, $\varphi(\mathfrak{S}_5)$ contient strictement plus de 2 éléments. Ainsi, $\mathrm{Ker}(\varphi) = \{\mathrm{id}\}$, et on a donc un morphisme injectif $\varphi : \mathfrak{S}_5 \hookrightarrow \mathfrak{S}_6$. Considérons $H = \mathrm{Im}(\varphi)$. Par cardinalité, c'est un sous-groupe d'indice 6 de $\mathfrak{S}_6$. Par ailleurs, comme l'action est transitive, H est un sous-groupe transitif, c'est-à-dire qu'il ne peut pas fixer l'un des $i \in [\![1,6]\!]$. Ainsi H est différent des $S(i)$, ce qui prouve bien **4** d'après **3**.

- La dernière question potentielle sur ce sujet serait d'identifier le groupe quotient $\mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Int}(\mathfrak{S}_6)$ (rappelons que dans tout groupe G, $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$). Pour cela, remarquons que si $\varphi \in \mathrm{Aut}(\mathfrak{S}_6)\backslash\mathrm{Int}(\mathfrak{S}_6)$, alors d'après **1** et le raisonnement mené dans la preuve de **2**, φ échange la classe de conjugaison des transpositions avec celle des produit de trois transpositions à supports disjoints. Ainsi, si φ et ψ sont extérieurs, alors $\varphi \circ \psi$ envoie les transpositions sur les transpositions, donc par **1**, $\varphi \circ \psi \in \mathrm{Int}(\mathfrak{S}_6)$. Ainsi, il n'y a que deux classes dans $\mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Int}(\mathfrak{S}_6)$ que sont $\mathrm{Int}(\mathfrak{S}_6)$ et son complémentaire. Autrement dit, $\mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Int}(\mathfrak{S}_6) \simeq \mathbb{Z}/2\mathbb{Z}$. Comme $\mathcal{Z}(\mathfrak{S}_6)$ est trivial, on a $\mathrm{Int}(\mathfrak{S}_6) \simeq \mathfrak{S}_6$, donc en particulier, on en déduit que $\#\mathrm{Aut}(\mathfrak{S}_6) = 2 \times 6! = 1440$.