$\mathcal{A}_n$ Simple.

Perrin + tête.

Théorème : Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$

Preuve : Montrons dans un premier temps que $\mathcal{A}_5$ est simple.

Dans $\mathcal{A}_5$, il y a :
- Le neutre
- 15 éléments d'ordre 2 : Les doubles transpositions disjointes
- 20 éléments d'ordre 3 : Les 3-cycles
- 24 éléments d'ordre 5 : Les 5-cycles.

On sait que les éléments d'ordre 3 sont conjugués dans $\mathcal{A}_5$. C'est aussi le cas pour les éléments d'ordre 2 : Si $\tau = (a\,b)(c\,d)(e)$ et $\tau' = (a'\,b')(c'\,d')(e')$ sont deux éléments d'ordre 2 de $\mathcal{A}_5$.

Il existe $\sigma \in \mathcal{A}_5$, $\begin{cases} \sigma(a) = a' \\ \sigma(b) = b' \\ \sigma(e) = e' \end{cases}$ D'où $\tau' = \sigma \tau \sigma^{-1}$

Soit $H \triangleleft \mathcal{A}_5$, un sous groupe distingué non trivial. Montrons que $H = \mathcal{A}_5$.
Si H contient un élément d'ordre 3, ou d'ordre 2, alors il les contient tous.
Si H contient un élément d'ordre 5, alors il les contient tous :

Soient $\tau, \tau' \in S_5$, d'ordre 5. Il existe $\sigma \in S_5$, $\tau' = \tau \sigma \tau^{-1}$.

Supposons $\tau \in H$,
- Si $\sigma \in \mathcal{A}_5$, c'est bon $\tau' \in H$
- Sinon, on note $\tau = (a\,b\,c\,d\,e)$, on a $\tau^2 = (a\,c\,e\,b\,d)$ et en posant $\rho = (b\,c\,e\,d)$, on a $\rho \tau \rho^{-1} = \tau^2$

  d'où $\tau' = \sigma' \tau^2 \sigma'^{-1}$ où $\sigma' = \sigma \rho^{-1} \in \mathcal{A}_5$

D'où $\tau' \in H$.

Or les entiers $15+1$, $20+1$, $24+1$ ne divisent pas $60 = \#\mathcal{A}_5$. Donc par le théorème de Lagrange

H contient au moins 2 types d'éléments, d'où $\#H \geq 1 + 15 + 20 = 36$.

D'où $\#H = 60$ car $\#H \mid \#\mathcal{A}_5$ Donc $H = \mathcal{A}_5$.

Montrons maintenant le théorème pour $n \geq 5$

Soit $H \lhd \mathcal{A}_n$, un sous-groupe distingué non trivial. Soit $\sigma \in H$, $\sigma \neq Id$.

Comme $\sigma \neq Id$, $\exists a \in [\![1, n]\!]$, $b = \sigma(a) \neq a$. Soit $c \in [\![1, n]\!] \setminus \{a, b, \sigma(b)\}$.

On pose $\tau = (a\ c\ b)$ d'inverse $\tau^{-1} = (a\ b\ c)$ et $\rho = \tau \sigma \tau^{-1} \sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c))$

Ainsi, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ possède au plus 5 éléments car $b = \sigma(a)$

Quitte à rajouter des éléments fixés par ρ, on peut supposer $\# F = 5$. Ainsi, on a

$\rho(F) = F$ et $\rho \neq Id$ car $\rho(b) = \tau \sigma \tau^{-1} \sigma^{-1}(b) = \tau \sigma(b) \neq \tau(c) = b$.

$\rho_{|[\![1,n]\!] \setminus F} = Id_{[\![1,n]\!] \setminus F}$

Donc $\mathcal{A}(F) \simeq \mathcal{A}_5$ et se plonge dans $\mathcal{A}_n$ par $u \mapsto \bar{u}$ défini par :

$$\bar{u}_{|F} = u \quad \text{et} \quad \bar{u}_{|[\![1,n]\!] \setminus F} = Id_{[\![1,n]\!] \setminus F}.$$

Ainsi, le groupe $H_0 = \{u \in \mathcal{A}(F) \mid \bar{u} \in H\} = H \cap \mathcal{A}(F)$ est distingué dans $\mathcal{A}(F)$ et

$\rho_{|F} \in H_0$ et $\rho_{|F} \neq Id$ donc $\rho_{|F} \in H_0 \setminus \{Id_F\}$

Comme $\mathcal{A}(F) \simeq \mathcal{A}_5$ est simple, on a $H_0 = \mathcal{A}(F)$.

Soit $u_0 \in \mathcal{A}(F)$ un 3-cycle. Alors $\bar{u}_0 \in H$ est encore un 3-cycle.

Comme les 3-cycles sont conjugués dans $\mathcal{A}_n$ et H est distingué, on a H contient tous les 3-cycles.

Or les 3-cycles engendrent $\mathcal{A}_n$ donc $H = \mathcal{A}_n$.