

A_n est simple pour $n \geq 5$.

Soit G un sous groupe distingué non trivial de A_n . Il suffit de montrer que G contient un 3-cycle car ils sont tous conjugués dans A_n qui est lui même engendré par les 3-cycle.

Soit $\sigma \in G$ non triviale, qui possède le maximum de points fixes. On décompose σ en produit "croissant" de permutations circulaires à supports dis-joints :

$$\sigma = c_1 \dots c_r \text{ où } p \leq q \implies \#supp(c_p) \leq \#supp(c_q).$$

Étape 1 : On montre que c_r n'est pas une transposition :

Si c_r est une transposition on a $r \geq 2$ (car $\sigma \in A_n$), $c_1 = (i \ j)$ et $c_2 = (k \ l)$.

On pose $\gamma = (k \ l \ m)$ avec $m \notin \{i, j, k, l\}$ et $\sigma' = \gamma \sigma \gamma^{-1} \sigma^{-1} \in G$.

On constate alors que $\{x \in G, x \neq m | \sigma(x) = x\} \subset \{x \in G | \sigma'(x) = x\}$.

De plus, on a $\sigma'(i) = i$ et $\sigma'(j) = j$ donc σ' présente plus de points fixes que σ alors que $\sigma' \neq id$ car $\sigma'(k) = m$; contradiction.

Étape 2 : On montre que σ est un 3-cycle :

On a $c_r = (i \ j \ k \ \dots)$; supposons que σ ne soit pas un 3-cycle. Si $r = 1$, alors c_r est au moins un 5-cycle (car $\sigma \in A_n$) donc dans tous les cas σ déplace au moins 5 points i, j, k, l, m .

On pose alors $\gamma = (k \ l \ m)$ et $\sigma' = \gamma \sigma \gamma^{-1} \sigma^{-1} \in G$.

Cette fois ci, on a $\{x \in G | \sigma(x) = x\} \subset \{x \in G | \sigma'(x) = x\}$ avec de plus $\sigma'(j) = j$.

De nouveau, $\sigma' \neq id$ puisque $\sigma'(k) = l$; contradiction.

Conclusion : G contient un 3-cycle donc $G = A_n$.