Simplicité de A_n.

Ref : Rombaldi - Algèbre p. 50.

$n=1$ et $n=2$: A_n est trivial donc simple.

Lemme 1 : Pour $n \geq 3$, A_n est engendré par les 3-cycles.

Lemme 2 : Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n.

Théorème : Pour $n = 3$ ou $n \geq 5$, le groupe A_n est simple.

Lemme 1 : Pour $n \geq 3$, A_n est engendré par les 3-cycles.

Preuve : A_n est l'ensemble des permutations paires, c'est à dire de produits d'un nombre pair de transpositions. (1)

il suffit alors de montrer que 2 transpositions est un produit de 3-cycles.

Soient τ_1 et τ_2 deux transpositions.

* si $\tau_1 = \tau_2$, alors $\tau_1 \tau_2 = id_E = \gamma^3$ pour tout γ un 3-cycle
* si $\tau_1 \neq \tau_2$, alors on a 2 possibilités :
  - $\rightarrow$ $Supp(\tau_1) \cap Supp(\tau_2) = \{x\}$ $\Rightarrow$ $\tau_1 = (x\, y)$ $\tau_2 = (x\, z)$ avec x, y, z distincts
    et $\tau_1 \tau_2 = (x\, z\, y)$
  - $\rightarrow$ $Supp(\tau_1) \cap supp(\tau_2) = \phi$ $\Rightarrow$ $\tau_1 = (x\, y)$ $\tau_2 = (z\, t)$ x, y, z, t distincts
    et $\tau_1 \tau_2 = (x y)(z t) = (x y)\underbrace{(y z)(y z)}_{= id}(z t) = (x y z)(y z t)$

Lemme 2 : Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n.

Preuve : On sait déjà que les 3-cycles sont conjugués dans S_n (2)

Soient $\gamma = (x_1 x_2 x_3)$ et $\gamma' = (x_1' x_2' x_3')$ deux 3-cycles.

Soit $\sigma \in S_n$ telle que $\sigma(x_i) = x_i'$ pour $i = 1, 2, 3$.

on a alors $\sigma \gamma \sigma^{-1} = \gamma'$.

$\rightarrow$ Si $\sigma \in A_n$ alors c'est ok, γ et γ' sont conjugués dans A_n.

$\rightarrow$ Si $\sigma \notin A_n$, alors on prend $x_4, x_5 \in \{1, .., n\} \setminus \{x_1, x_2, x_3\}$ (possible car $n \geq 5$)

et $\sigma' = (x_4, x_5)\sigma \in A_n$ avec $\sigma'(x_i) = x_i'$ pour $i = 1, 2, 3$

et alors $\sigma' \gamma \sigma'^{-1} = \gamma'$

Théorème : Pour $n=3$ ou $n \geq 5$, le groupe $\mathcal{A}_n$ est simple.

Preuve :

- $n=3$: $|A_3| = \frac{3!}{2} = 3$ premier donc A_3 est cyclique et donc simple

  Les groupes d'ordre p premier sont simples.

- On suppose $n \geq 5$. Soit H un sous groupe distingué de $\mathcal{A}_n$ distincts de $\{id\}$.

Mq : $H = \mathcal{A}_n$.

il suffit de montrer que H contient un 3-cycle car les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ et l'engendrent.

Soit $\sigma \in H \setminus \{id\}$ et $\gamma = (x\ z\ y) \in \mathcal{A}_n$ un 3-cycle avec $y = \sigma(x)$ et tel que γ ne commute avec σ (*)

Comme H est un sous groupe distingué de $\mathcal{A}_n$, on a :

$$\sigma' := \underbrace{\sigma}_{\in H} \underbrace{\gamma \sigma^{-1} \gamma^{-1}}_{\substack{\in H \text{ car } \sigma \in H \\ \text{et } \gamma \in \mathcal{A}_n \text{ et } H \trianglelefteq \mathcal{A}_n}} \in H$$

On réécrit σ' : $\sigma' = \sigma \underbrace{(x z y)}_{\gamma} \sigma^{-1} \underbrace{(x y z)}_{\gamma^{-1}}$

$$= (\sigma(x)\ \sigma(z)\ \sigma(y))\ (y\ z\ x)$$

$$= (y\ \sigma(z)\ \sigma(y))\ (y\ z\ x)$$

σ' est alors produit de deux 3-cycles qui agissent sur $F = \{x, y, z, \sigma(y), \sigma(z)\}$ formé d'au plus 5 éléments.

On a : $\sigma' \neq id$ car sinon on aurait $\sigma\gamma\sigma^{-1}\gamma^{-1} = id$

c'est à dire $\sigma\gamma = \gamma\sigma$ Absurde

Dans $S(F)$, σ' s'écrit comme produit de cycles à supports disjoints, cette décomposition étant celle dans S_n.

Comme $\sigma' \in A_n$, il n'y a que 3 possibilités :

→ <u>σ' est un 3-cycle :</u> alors H contient bien un 3-cycle

→ <u>σ' est un produit de 2 transpositions :</u> $\sigma' = (x_1, x_2)(x_3\, x_4)$

on choisit $x_5 \in E \setminus \{x_1, x_2, x_3, x_4\}$ et $\tau = (x_1 x_2 x_5) \in A_n$

alors $\sigma' \tau \sigma'^{-1} \tau^{-1} = (\sigma'(x_1)\ \sigma'(x_2)\ \sigma'(x_5))\,(x_5\ x_2\ x_1)$

$= (x_2\ x_1\ x_5)(x_5\, x_2\, x_1) = (x_1\, x_2\ x_5)$

→ <u>σ' est un 5-cycle :</u> $\sigma' = (x_1 x_2 x_3\, x_4\, x_5)$

$\tau = (x_1\, x_2\ x_3) \in A_n$

$\sigma' \tau \sigma'^{-1} \tau^{-1} = (\sigma'(x_1)\ \sigma'(x_2)\, \sigma'(x_3))\,(x_1\ x_3\ x_2)$

$= (x_2\ x_3\ x_4)(x_1\ x_3\ x_2) = (x_1 x_4\ x_2)$

(*) on prend $z \notin \{x, y, \sigma^{-1}(x)\}$ possible car $n \geq 5$.

$\sigma\gamma\sigma^{-1}(y) = \sigma\circ\gamma(x) = \sigma(z)$ et $\gamma(y) = x \neq \sigma(z)$

donc $\sigma\gamma\sigma^{-1}(y) \neq \gamma(y) \Rightarrow \sigma\gamma \neq \gamma\sigma$

produits d'un nombre pair de transpositions (1)

mq: toute permutation s'écrit comme produit de transpositions:

on peut utiliser la décomposition en cycles à support disjoint.

ou

on part de $(a_1 a_2 \dots a_n)$

$(a_1 a_n)(a_1 a_2 \dots a_n)$ fixe a_n

$(a_1 a_{n-1})(a_1 a_n)(a_1 a_2 \dots a_n)$ fixe a_n, a_{n-1}

$(a_1 a_{n-2})(a_1 a_{n-1})(a_1 a_n)(a_1 a_2 \dots a_n)$ fixe a_n, a_{n-1}, a_{n-2}

$\vdots$

$(a_1 a_2)(a_1 a_3) \dots (a_1 a_n)(a_1 a_2 \dots a_n)$ fixe $a_n, \dots, a_1$.

donc $(a_1 a_2 \dots a_n) = ((a_1 a_2) \dots (a_1 a_n))^{-1}$

$= (a_1 a_n) \dots (a_1 a_2)$.

3-cycles sont conjugués dans S_n (2)

rq: 2 permutations de même type sont conjuguées.

soient $\sigma_1, \sigma_2 \in S_n$ deux p-cycles

$\sigma_1 = (x_1 \dots x_p)$ $\sigma_2 = (y_1 \dots y_p)$. x_i 2 à 2 distincts et y_i 2à2 distincts

Soit $\gamma \in S_n$ tel que $\gamma(x_i) = y_i$ $\forall i \in [\![1, p]\!]$

Alors $\gamma\sigma_1\gamma^{-1} = (\gamma(x_1) \dots \gamma(x_p)) = (y_1 \dots y_p)$.