Simplicité de $\mathfrak{A}_n$ ($n \geq 5$) Perrin, Rombaldi

Soit $n \geq 5$.

Lem 1 : $\mathfrak{A}_n$ est engendré par les trois cycles.

Dém : On pose G le groupe engendré par les 3 cycles. Mq $G = \mathfrak{A}_n$.

$\boxed{\subset}$ Soit $\sigma \in G$: $\varepsilon(\sigma) = 1$ donc $\sigma \in \mathfrak{A}_n$.

$\boxed{\supset}$ Soit $\sigma \in \mathfrak{A}_n$. On décompose σ en produit de transpositions donc $\sigma = \prod_{i=1}^{p} \tau_i$.

On $\varepsilon(\sigma) = 1$ et $\varepsilon(\tau_i) = -1$ donc p est pair.

Mq le produit de 2 transps est un 3-cycle : ($a \neq b \neq c \neq d$)

$(a b)(c d) = (a b c)(b c d)$ et $(a b)(c a) = (b c a)$

et $(a b)(b a) = id$.

Alors, c'est bien un 3 cycle. Donc $\sigma \in G$ par déf. ☐

Lem 2 : Les 3 cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$

Dém : Soient $a \neq b \neq c$ et $d \neq e \neq f$. On sait que les 3 cycles sont conjugués dans $\mathfrak{S}_n$

donc $\exists \sigma \in \mathfrak{S}_n$ tq $(a b c) = \sigma^{-1}(d e f)\sigma$.

$\rightarrow$ si $\sigma \in \mathfrak{A}_n$ ok. $\rightarrow$ sinon, comme $n \geq 5$, on peut choisir i et j distincts de a, b, c et alors :

$\sigma' = \sigma(i j) \in \mathfrak{A}_n$

D'où $\sigma'(a b c)\sigma'^{-1} = (\sigma'(a)\ \sigma'(b)\ \sigma'(c)) = (\sigma(a)\ \sigma(b)\ \sigma(c))$

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

Donc les 3 cycles sont conjugués dans $\mathfrak{A}_n$. ☐

Thm 3 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Dém : Soit $H \neq \{id\} \triangleleft \mathfrak{A}_n$. Par Lem 1 et Lem 2, il suffit de mq H contient un 3 cycle.

Soit $\sigma \in H \setminus \{id\}$. Prenons a tq $b = \sigma(a) \neq a$.

Fixons $c \notin \{a, b, \sigma(b)\}$ (possible car $n \geq 5$) et posons $\gamma = (a b c)$

et $\sigma_2 = \sigma\gamma\sigma^{-1}\gamma^{-1}$. On a $\sigma_2 \in H$ car $\sigma \in H$ et $\underbrace{\gamma\sigma^{-1}\gamma^{-1}}_{\in H \text{ car } H \triangleleft \mathfrak{A}_n} \in H$.

De plus, $\sigma_2 = (\sigma(a)\ \sigma(b)\ \sigma(c))\gamma^{-1} = (b\ \sigma(b)\ \sigma(c))(c\ b\ a)$.

On va décomposer σ_2 en produit de cycles à support disjoints.
Remarquons que $\operatorname{supp}\sigma_2 \subset \{a, b, c, \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\varepsilon(\sigma_2) = 1$

- $(1\,1\,1\,1\,1)$ si $\sigma_2 = id$ alors $\sigma\gamma = \gamma\sigma$ ce qui faux car $\sigma\gamma(a) = \sigma(b) \neq c = \gamma\sigma(a)$ ×
- $(2\,1\,1\,1)$ impossible $\varepsilon((i\,j)) = -1$ ×
- $(2\,2\,1)$ si $\sigma_2 = (i\,j)(k\,l)$ alors $\sigma_3 = \underbrace{(i\,j\,k\,l\,m)\sigma_2(i\,j\,k\,l\,m)^{-1}}_{\in H}\underbrace{\sigma_2^{-1}}_{\in H} \in H$

  et $\sigma_3 = (i\,j\,k\,l\,m)(\sigma_2(i)\,\sigma_2(j)\,\sigma_2(k)\,\sigma_2(l)\,\sigma_2(m))^{-1}$ car $H \triangleleft A_n$

  $= (i\,j\,k\,l\,m)(j\,i\,l\,k\,m)^{-1} = (i\,k\,m\,l\,j)$

  → et on se ramène au type (5)
- $(3\,1\,1)$ σ_2 est un 3 cycle : gagné.
- $(3\,2)$ $\varepsilon((i\,j\,k)(l\,m)) = -1$ ×.
- $(4\,1)$ $\varepsilon((i\,j\,k\,l)) = -1$ ×.
- (5) $\sigma_2 = (i\,j\,k\,l\,m)$ alors $\sigma_3 = \underbrace{(i\,j\,k)\sigma_2(i\,j\,k)^{-1}}\underbrace{\sigma_2^{-1}}_{\in H} \in H$

  et $\sigma_3 = (i\,j\,k)(\sigma_2(i)\sigma_2(j)\sigma_2(k))^{-1} \in H$

  $= (i\,j\,k)(j\,k\,l)^{-1} = (i\,j\,k)(l\,k\,j) = (i\,j\,l)$

Dans tous les cas, on a trouvé un 3 cycle dans H. Par Lem 2, ils sont tous dans H ($\triangleleft A_n$) et par Lem 1, $A_n \subset H$. Donc $H = A_n$. ☐

<u>Rq</u> : • $A_1 = A_2 = \{id\}$ simples. • $A_3 = \{id, (1\,2\,3), (1\,3\,2)\}$ simple

• A_4 n'est pas simple car $D = \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4$ $\neq A_4$ $\neq \{id\}$

$A_4 = D \sqcup \{3 \text{ cycles}\}$. De plus, les 3 cycles ne sont pas conjugués sinon par la formule des classes (action de conjugaison) $|\mathrm{Orb}(3\text{ cycle})| = |\text{tous les 3 cycles}| = 8$ qui doit diviser $|A_4| = 12$.
Impossible. Donc A_n est simple $\forall n \geq 1$ sauf $n = 4$.

Corollaire : Si $n \geq 5$, les ss grp distingués de S_n sont $\{id\}$, A_n et S_n.

Dém : Soit $H \triangleleft S_n$. On a $H \cap A_n \triangleleft A_n$ donc par simplicité de A_n,
$H \cap A_n = \{id\}$ ou $H \cap A_n = A_n$.

. Si $H \cap A_n = A_n$ alors $A_n \subset H$ donc $\{H = A_n$ ou $H = S_n\}$ (cardinaux)

. Si $H \cap A_n = \{id\}$ mq $H = \{id\}$. $\mathrm{Ker}(\varepsilon_{|H}) = H \cap A_n = \{id\}$ donc $\varepsilon_{|H}$ est inj.
Donc $\varepsilon_{|H}$ induit un iso sur son image : $H \simeq \varepsilon(H)$ est d'ordre 1 ou 2.
Si $H = \{id, \sigma\}$ (=ordre 2). $(\sigma \neq id)$ $\quad \subset \varepsilon(S_n) = \{\pm 1\}$
Pour $\tau \in S_n$ on a $\tau\sigma\tau^{-1} \neq id$ et $\tau\sigma\tau^{-1} \in H$ car $H \triangleleft S_n$ donc $\tau\sigma\tau^{-1} = \sigma$
càd τ et σ commutent $\forall \tau$ donc $\sigma \in Z(S_n) = \{id\}$ $(n \geq 3)$. Absurde car $\sigma \neq id$
Donc $H = \{id\}$. CCL : $H = S_n$ ou A_n ou $\{id\}$. (cf Lem) $\square$

Lem : $Z(S_n) = \{id\}$ pour $n \geq 3$

Dém : Pour $\sigma \neq id$, $\exists a$ tq $\sigma(a) \neq a$. On note $b = \sigma(a)$. Puisque $n \geq 3$,
on prend $c \notin \{a, b\}$. Alors $[\sigma(b\,c)](a) = b$ mais $[(b\,c)\sigma](a) = (bc)(b) = c$
et $b \neq c$ donc σ et $(b\,c)$ ne commutent pas.

Prop : S_n est engendré par les transpositions. De plus, une permutation est un produit de cycles.

Dém : Mq une permutation est un produit de cycles. Soit $\sigma \in S_n$.
. Existence : $[\![1, n]\!] = \bigsqcup_{k=1}^{R} \mathcal{O}_k$ (partition d'orbites) $(\mathcal{O}_k = (id, \sigma, \dots, \sigma^p))$. Posons $c_k(i) = \begin{cases} i \text{ si } i \notin \mathcal{O}_k \\ \sigma(i) \text{ si } i \in \mathcal{O}_k \end{cases}$
c_k est un cycle de longueur $l_k = \mathrm{card}(\mathcal{O}_k)$. Comme les supports des cycles c_k sont disjoints
alors $\forall i \in [\![1, n]\!]\ \exists! k$ tq $i \in \mathcal{O}_k$ et $c_1 \circ \dots \circ c_R(i) = c_k(i) = \sigma(i)$.
Donc $\sigma = c_1 \circ \dots \circ c_R$.

. Unicité : Si $\sigma = \tau_1 \circ \dots \circ \tau_p$ alors $\mathrm{supp}\,\sigma = \bigsqcup_{j=1}^{p} \mathrm{supp}(\tau_j) = \bigsqcup_{i=1}^{R} \mathrm{supp}(c_i)$
$= c_1 \circ \dots \circ c_R$
Donc $\forall k\ \exists! i$
$\exists! j$ tq $k \in \mathrm{supp}(c_i) \cap \mathrm{supp}(\tau_j)$.
Quitte à renuméroter qps, $k \in \mathrm{supp}(c_1) \cap \mathrm{supp}(\tau_1)$. Donc $\sigma(k) = c_1(k) = \tau_1(k) = \sigma(k)$.
Donc $\forall N$ $\sigma^N(k) = c_1^N(k) = \tau_1^N(k)$ donc $c_1 = \tau_1$. En continuant ce raisonnement,
$R = p$ et $c_i = \tau_i$. Donc une permutation est un produit de cycles.
. Mq un cycle est un produit de transps :
$(x_1, \dots, x_n) = (x_1\, x_2)(x_2\, x_3) \dots (x_{n-1}\, x_n)$. Donc S_n est engendré par les transps. $\square$

Prop : Tous les 3 cycles sont conjugués dans S_n.

Dem : Soit $\sigma = (x_1\ x_2\ x_3)$ - $\tau \in S_n$ - $\sigma'' = (\tau(x_1)\ \tau(x_2)\ \tau(x_3))$

. Si $x \notin \{x_1, x_2, x_3\}$ alors $\sigma(x) = x$ et $\tau(x) \notin \{\tau(x_1), \tau(x_2), \tau(x_3)\}$

donc $\sigma''(\tau(x)) = \tau(x)$. Ainsi, $\tau \circ \sigma(x) = \sigma'' \circ \tau(x)$

. Si $x = x_k$ alors $\tau(\sigma(x)) = \tau(\sigma(x_k)) = \tau(x_{k+1})$ et $\sigma''(\tau(x)) = \tau(x_{k+1})$

$= \tau \circ \sigma(x)$. ☐

Prop : Dénombrement des éléments de A_5 : $|A_5| = 60$

$(1\ 1\ 1\ 1\ 1)$ id $\boxed{1}$

$(2\ 1\ 1\ 1)$ $\varepsilon = -1$ ×

$(2\ 2\ 1)$ $\left(\frac{5\times 4}{2} \times \frac{3\times 2}{2}\right) \times \frac{1}{2} = \boxed{15}$ doubles transpos ← les 2 transpos commutent

$(3\ 1\ 1)$ $\frac{5\times 4\times 3}{3} = \boxed{20}$ 3-cycles

$(3\ 2)$ $\varepsilon = -1$ ×

$(4\ 1)$ $\varepsilon = -1$ ×

(5) $\frac{5\times 4\times 3\times 2\times 1}{5} = 4\times 3\times 2 = \boxed{24}$ 5-cycles

total $= 60$ ☐