Simplicité de A_n, pour $n=3$ ou $n \geq 5$

↳ Refs : Grand Combat p 217-220, Rombaldi p 50-51 et Perrin p28-3[illegible]

Lemme : 1) Si $n \geq 3$, A_n est engendré par les 3-cycles.
2) Si $n \geq 5$, les 3-cycles sont conjugués dans A_n.

Théorème : (Simplicité de A_n) Pour $n=3$ ou $n \geq 5$, A_n est simple.

Corollaire 1 : Si $n \geq 2$ et $n \neq 4$, les sous groupes distingués de S_n sont $\{Id\}$, A_n, S_n.

Corollaire 2 : Tout sous groupe d'indice n de S_n est isomorphe à S_{n-1}.

Preuve du lemme : 1) le sous groupe engendré par les 3cycles est dans A_n car les 3-cycles sont de signature égale à 1.
Réciproquement, les éléments de A_n peuvent s'écrire comme des produits de transpositions (S_n est engendré par les transpositions) en nombre pair.
Ainsi, il suffit de montrer que les doubles transpositions sont engendrées par les 3 cycles. Soit $\tau_1, \tau_2 \in S_n$ deux transpositions. On écrit $\tau_1 = (i\ j)$, $\tau_2 = (k, l)$

* si $\{i,j\} = \{k,l\}$, alors $\tau_1 \tau_2 = Id$ ⊳ ok
* si $\{i,j\} \cap \{k,l\}$ a un elt, supposons $j=k$, alors $\tau_1\tau_2 = (i\ k)(k\ l) = (i\ k\ l)$
* si $\{i,j\} \cap \{k,l\} = \emptyset$, alors $\tau_1 \tau_2 = (i\ j)(k\ l) = (i\ k\ j)(i\ k\ l)$

Cela permet de conclure que A_n est engendré par les 3-cycles.

2) Soit $\sigma_1 = (a\ b\ c)$ et $\sigma_2 = (d\ e\ f)$ deux 3-cycles. Ils sont conjugués dans S_n donc il existe $\tau \in S_n$ telle que $\tau \sigma_2 \tau^{-1} = \sigma_1$.
Si $\tau \in A_n$ c'est terminé. Supposons donc que $\varepsilon(\tau) = -1$. Puisque $n \geq 5$, on peut trouver $i \neq j \notin \{a, b, c\}$, on pose alors $\tau' = (i\ j)\tau$. Alors $\tau' \in A_n$ et $\tau' \sigma_2 \tau'^{-1} = (i\ j) \sigma_1 (i\ j)^{-1} = \sigma_1 (i\ j)(i\ j)^{-1} = \sigma_1$. puisque σ_1 et $(i\ j)$ sont à supports disjoints par construction, donc commutent.
Et on a bien obtenu le résultat.

Preuve du théorème : Pour $n=3$, A_3 (de cardinal 3) est cyclique d'ordre 3 et donc il est simple (pas de sous groupe autre lui même ou $\{Id\}$)
Supposons maintenant $n \geq 5$. Soit H un sous groupe distingué de A_n distinct de $\{Id\}$. Notre objectif est donc de montrer $H = A_n$, et pour cela, il suffit d'après ce qui précède de montrer que H contient un 3cycle : alors puisqu'ils sont tous conjugués dans A_n et que H est distingué, alors tous les 3 cycles seront inclus dans H, et puisqu'ils engendrent A_n, on aura bien $A_n = H$.
Soit $\sigma \in H \setminus \{Id\}$. Ainsi, il existe $x, y \in [\![1, n]\!]$ distincts tels que $\sigma(x) = y$. Comme $n \geq 5$, il existe $z \notin \{x, y, \sigma(y)\}$, et on définit alors le 3 cycle suivant : $\tau = (x\ y\ z) \in A_n$. Ainsi, puisque H est distingué dans A_n,
$\sigma' = \sigma\tau\sigma^{-1}\tau^{-1} = \overset{\in H}{\sigma}(\overset{\in H}{\tau\sigma^{-1}\tau^{-1}}) \in H$ (idée : créer σ' avec beaucoup de points fixes)

Et on peut même exprimer cette permutation simplement :

$$\sigma' = (\sigma(x\ y\ z)\sigma^{-1})(y\ x\ z) = (\sigma(x)\ \sigma(y)\ \sigma(z))(y\ x\ z)$$
$$= (y\ \sigma(y)\ \sigma(z))(y\ x\ z).$$

Donc σ' est une permutation dont le support $F = \{x, y, z, \sigma(y), \sigma(z)\}$ compte au plus 5 éléments. Ainsi, il n'y a que peu de possibilités concernant le type de σ' (puisque $\sigma' \in A_n$)

* Soit 1, 1, 1, 1, 1 ie $\sigma' = Id$, or cela signifie $\tau\sigma = \sigma\tau$. Mais cela signifie en particulier $\sigma\tau(x) = \sigma(y)$ et $\tau\sigma(x) = \tau(y) = z \neq \sigma(y)$ ↯

* Soit 3, 1, 1 alors σ' est un 3 cycle et c'est gagné !

* Soit 2, 2, 1, on écrit alors $\sigma' = (i\ j)(k\ l)$ (décomposit° en transpo. à supports disjoints) Prenons $m \notin \{i, j, k, l\}$ possible car $n \geq 5$, et refaisons la même chose que précédemment : on pose $\gamma = (i\ j\ m) \in A_n$, et alors $\sigma'' = \sigma'\gamma\sigma'^{-1}\gamma^{-1} \in H$ et $\sigma'' = (\sigma'(i)\ \sigma'(j)\ \sigma'(m))(i\ m\ j)$
$= (j\ i\ m)(i\ m\ j) = (i\ j\ m)$

et donc σ'' est un 3 cycle et c'est gagné !

* Soit 5, on écrit alors $\sigma' = (i\ j\ k\ l\ m)$, et on recommence en posant $\gamma = (i\ j\ k) \in A_n$, alors $\sigma'' = \sigma'\gamma\sigma'^{-1}\gamma^{-1} \in H$ et
$\sigma'' = (\sigma(i)\ \sigma(j)\ \sigma(k))(i\ k\ j) = (j\ k\ l)(i\ k\ j) = (i\ l\ j)$
donc σ'' est un 3 cycle et c'est gagné !

Dans tous les cas c'est gagné, donc $H = A_n$.

<u>Preuve du corollaire 1 :</u> Si $n = 2$, le résultat est clair puisque $A_2 = \{Id\}$. Supposons donc $n \geq 3$ et $n \neq 4$. Soit H un sous groupe distingué de S_n. Alors $H \cap A_n$ est distingué dans A_n, donc $H \cap A_n = \{Id\}$ ou A_n.

* Si $H \cap A_n = A_n$, alors $A_n \subset H$. Si $H \subset A_n$, $H = A_n$, sinon H contient une signature de signature -1 que l'on appelle σ_0, alors H contient A_n et $\sigma_0 A_n$ donc H contient S_n et donc $H = S_n$

* Si $H \cap A_n = \{Id\}$, alors la signature induit un morphisme injectif de H sur $\{\pm 1\}$, de sorte que $|H| \leq 2$.
Supposons $|H| = 2$ et soit $\sigma \in H$ l'unique élément non trivial de H. Soit $\tau \in S_n$, alors $\tau\sigma\tau^{-1} \in H$ (distingué) et $\tau\sigma\tau^{-1} \neq Id$ (puisque $\sigma \neq Id$), donc $\tau\sigma\tau^{-1} = \sigma$, ie $\sigma \in Z(S_n)$. Donc puisque $Z(S_n) = \{Id\}$ (*) on obtient $\sigma = Id$ ↯ donc $|H| = 1$ ie $H = \{Id\}$.

(*) En effet, si $\sigma \in S_n \setminus \{Id\}$, alors il existe $a, b \in [\![1, n]\!]$ tels que $\sigma(a) = b$ et $a \neq b$. Comme $n \geq 3$, il existe $c \notin \{a, b\}$, et alors en posant $\tau = (b\ c)$, on a $\sigma\tau(a) = \sigma(a) = b$ et $\tau\sigma(a) = \tau(b) = c \neq b$ donc $\sigma\tau \neq \tau\sigma$ donc $\sigma \notin Z(S_n)$. (faux pour S_2 abélien)

(Bonus)
Preuve du corollaire 2 : Pour $n=2$ c'est clair.

Pour $n=3$, un sous groupe d'indice 3 est d'ordre 2 donc iso à $\mathbb{Z}/2\mathbb{Z}$, iso à S

Pour $n=4$, un sous groupe d'indice 4 est d'ordre 6, donc soit cyclique d'ordre 6 (iso à $\mathbb{Z}/6\mathbb{Z}$) soit iso à $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ (D_6) (c'est le cas de S_3 qui est d'ordre 6 non abélien). Or S_4 ne contient pas d'éléments d'ordre 6, donc cela exclut la première possibilité.

Supposons $n \geq 5$, et soit H sous groupe d'indice n de S_n. Alors S_n agit par translation à gauche sur S_n/H qui est donc de cardinal n, et on a donc un morphisme de groupes $\varphi : S_n \longrightarrow Bij(S_n/H) \simeq S_n$, et

$\operatorname{Ker} \varphi = \bigcap_{\sigma \in S_n} \sigma H \sigma^{-1} \subset H$ et $\operatorname{Ker}\varphi$ distingué dans S_n, donc $\operatorname{Ker}\varphi = \{Id\}$

(intersect° de tous les $Stab(\sigma H) = \sigma H \sigma^{-1}$) (car $|\operatorname{Ker}\varphi| \leq (n-1)! < \frac{n!}{2}$).

Donc φ est injective donc c'est un isomorphisme (grâce aux cardinaux), et ainsi comme $\varphi(H)$ (iso à H) est le stabilisateur de $H \in S_n/H$, c'est finalement le stabilisateur d'un point dans S_n, et c'est donc un sous groupe isomorphe à S_{n-1}.

Remarques : * les groupes A_1 et A_2 sont égaux à $\{Id\}$ donc pas simple, et A_4 n'est pas simple car $D(A_4) = \{id, (12)(34), (13)(24), (14)(23)\}$ est distingué non trivial. (et les 3 cycles ne peuvent pas être conjugués dans A_4, car 8×12

* On peut montrer (mais c'est dur*) qu'en fait A_5 est l'unique groupe simple d'ordre 60, à isomorphisme près (même chose pour A_6 et A_7, mais pas A_8). (*utilise les thm de Sylow)

* le corollaire 1 est d'après la remarque 1 directement faux pour $n=4$, les sous groupes distingués de S_4 sont en fait $\{Id_4\}$, V_4, A_4 et S_4.

* Ce théorème dû à Galois est historiquement très important, car il a permis de montrer l'impossibilité de résoudre par radicaux une équation polynomiale générale de degré ≥ 5.

* Ce théorème peut permettre de montrer que si $n \geq 5$, $D(A_n) = A_n$ et $D(S_n) = A_n$. En effet $D(A_n) \triangleleft A_n$ donc soit A_n soit $\{Id\}$ mais A_n n'est pas abélien donc $D(A_n) \neq \{Id\}$ et donc $D(A_n) = A_n$. (Mais on peut le faire à la main : $D(A_n) \subset D(S_n) \subset A_n$, et tout 3 cycle est un commutateur : si σ est un 3cycle, σ^2 aussi donc (lemme 2), $\exists \tau \in A_n$, $\sigma^2 = \tau\sigma\tau^{-1}$ ie $\sigma = \tau\sigma\tau^{-1}\sigma^{-1}$, donc $D(A_n) = A_n$)
Et ensuite pour S_n, $\underset{\underset{A_n}{\|}}{D(A_n)} \subset D(S_n) \subset A_n$ nous donne direct $D(S_n) = A_n$.

En fait c'est surtout ce corollaire et le fait que cela implique A_n et S_n non résolubles (pour $n \geq 5$, résolubles sinon) qui est utile à la théorie de Galois (askip)

* Il existe une autre preuve du théorème, qui consiste à montrer que A_5 est simple grâce à du dénombrement puis à se ramener au

cas $n=5$ en trouvant une permutation avec beaucoup de points fixes.
Voilà les clés de la preuve :

Pour $n=5$: • 1 neutre

$\tau_1\tau_2=\tau_2\tau_1$

• 15 élts d'ordre 2 (bi-transpo) : $\frac{1}{2}\binom{5}{2}\binom{3}{2}$

• 20 élts d'ordre 3 : $2\times\binom{5}{3}$

• 24 élts d'ordre 5 : $4!$

Et ensuite, on déduit le reste avec de la bricole sur les cardinaux.
Et pour généraliser, on fait la même bricole que dans ma preuve pour se ramener au cas $n=5$.