Simplicité de A_n, $n \geq 5$

Leçons : 104, 105.

Énoncés :
- Lemme : ⇝ Pour tout $n \geq 2$, A_n est engendré par les 3-cycles.
  ⇝ Si $n \geq 5$, les 3-cycles sont conjugués dans A_n.
- Th : Si $n \geq 5$, A_n est simple.
- Corollaire : Si $n \geq 5$, les sg distingués de S_n sont $\{id\}$, A_n, S_n.

⊛ Lemme.

- Un élément de A_n est produit d'un nombre pair de transpositions. Il suffit alors de vérifier que les doubles transpositions sont engendrées par les 3-cycles. On considère $(a\,b)$ et $(c\,d)$: si elles ont un ou deux éléments communs, $(a\,b)(c\,d)$ est l'identité ou un 3-cycle. Sinon $(a\,b)(c\,d) = (a\,b)(b\,c)^2(c\,d) = (a\,b\,c)(b\,c\,d)$ est produit de deux 3-cycles.
- Soient $(a\,b\,c)$ et $(a'\,b'\,c')$ deux 3-cycles. On prend $\sigma \in S_n$ tq $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(c) = c'$: $\sigma(a\,b\,c)\sigma^{-1} = (a'\,b'\,c')$. Si $\sigma \in A_n$ c'est bon. Sinon soient $d, e \notin \{a, b, c\}$ (ce qui est possible puisque $n \geq 5$). $(\sigma(d\,e))(a\,b\,c)(\sigma(d\,e))^{-1} = \sigma(d\,e)(a\,b\,c)(d\,e)\sigma^{-1} = \sigma(a\,b\,c)\sigma^{-1}$ $= (a'\,b'\,c')$ car $(d\,e)$ et $(a\,b\,c)$ commutent. Cette fois on a $\sigma(d\,e) \in A_n$. □

⊛ Th.

- Soit $H \triangleleft A_n$ non trivial. Pour mq $H = A_n$, d'après le lemme il suffit de trouver un 3-cycle dans H. Soit $\sigma \in H \setminus \{id\}$ de nombre de points fixes maximal : on mq il s'agit d'un 3-cycle.
- On décompose σ en cycles à supports disjoints. Par l'absurde sq tous ces cycles sont des transpositions. $\sigma \in A_n$ donc elles sont en nombre pair. Soient $(a\,b)$ et $(c\,d)$ deux d'entre elles. On prend alors $e \notin \{a, b, c, d\}$ (possible car $n \geq 5$), et $\gamma = (c\,d\,e)$ et $\sigma' = [\gamma, \sigma] = \gamma\sigma\gamma^{-1}\sigma^{-1}$. Puisque $H \triangleleft A_n$, $\gamma\sigma\gamma^{-1} \in H$ et $\sigma' \in H$. Tout point fixe de σ différent de e est aussi fixé par γ, donc par σ'. De plus $\sigma'(b) = \gamma\sigma\gamma^{-1}\sigma^{-1}(b) = \gamma\sigma\gamma^{-1}(a) = \gamma\sigma(a) = \gamma(b) = b$, et de même $\sigma'(a) = a$. Au total σ' a donc au moins un point fixe de plus que σ, sans être l'identité (en effet $\sigma'(c) = \gamma\sigma\gamma^{-1}\sigma^{-1}(c) = \gamma\sigma\gamma^{-1}(d) = \gamma\sigma(c) = \gamma(d) = e$) : cela contredit la minimalité de σ : c'est absurde.

- Ce qui précède montre qu'au moins un cycle de la décomposition est de longueur ≥ 3, et on note trois de ses points consécutifs a, b, c. De nouveau, on suppose par l'absurde $\sigma \neq (a\ b\ c)$. Si le support de σ ne compte qu'un seul autre point d, nécessairement $\sigma = (a\ b\ c\ d)$; mais c'est impossible car $\sigma \in A_n$.
Soient donc $d \neq e$ dans le support de σ mais pas dans $\{a,b,c\}$. On pose $\gamma = (c\ d\ e)$ et $\sigma' = [\gamma, \sigma] = \gamma\sigma\gamma^{-1}\sigma^{-1}$. Là encore $\sigma' \in H$ et $\sigma' \neq id$ ($car\ \sigma'(c) = \gamma\sigma\gamma^{-1}\sigma^{-1}(c)$ $= \gamma\sigma\gamma^{-1}(b) = \gamma\sigma(b) = \gamma(c) = d$). Tout point fixe de σ est aussi fixé par γ (car le support de γ est inclus dans le support de σ), donc par σ'. De plus $\sigma'(b) = \gamma\sigma\gamma^{-1}\sigma^{-1}(b)$ $= \gamma\sigma\gamma^{-1}(a) = \gamma\sigma(a) = \gamma(b) = b$. σ' a au moins un point fixe de plus que σ ; là encore la minimalité de σ est mise en défaut et c'est absurde.
Finalement on conclut que $\sigma = (a\ b\ c)$ est un 3-cycle. □

⊛ <u>Corollaire :</u>

Soit $H \triangleleft \mathfrak{S}_n$. $H \cap A_n \triangleleft A_n$ donc d'après le th $H \cap A_n$ est A_n ou $\{id\}$. Dans le premier cas, $A_n \subset H$ donc H est A_n ou $\mathfrak{S}_n$.
Dans le second on mq $H = \{id\}$. $\ker(\varepsilon|_H) = H \cap A_n = \{id\}$ donc $\varepsilon|_H$ est injective et $H \simeq \varepsilon(H)$ est d'ordre 1 ou 2. On suppose par l'absurde que c'est 2, en notant $H = \{id, \sigma\}$ avec $\sigma \neq id$.
Pour $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} \neq id$ et $\tau\sigma\tau^{-1} \in H$ car $H \triangleleft \mathfrak{S}_n$: $\tau\sigma\tau^{-1} = \sigma$, cad que σ et τ commutent. σ est donc dans le centre de $\mathfrak{S}_n$, qui est trivial dès que $n \geq 3$: $\sigma = id$.
C'est absurde, d'où $H = \{id\}$. □

<u>Complément 1 :</u> Pour $n \geq 3$, $Z(\mathfrak{S}_n)$ est trivial.

Preuve.
Soit $\sigma \neq id$: il existe a tq $\sigma(a) \neq a$; on note $b = \sigma(a)$. Vu que $n \geq 3$ on peut prendre $c \notin \{a, b\}$.
Alors $(\sigma\ (b\ c))(a) = \sigma(a) = b$ mais $((b\ c)\sigma)(a) = (b\ c)(b) = c$. σ et $(b\ c)$ ne commutent pas. □

<u>Complément 2 :</u> A_4 n'est pas simple.

Preuve.
A_4 est constitué de l'identité, de 3-cycles et de doubles transpositions. Si on note H l'ensemble regroupant id et les doubles transpositions, c'est un sg de A_4. Par ailleurs c'est l'ens des éléments d'ordre 1 ou 2 de A_4 ; or les conjugaisons préservent l'ordre : elles laissent H stable.
Ainsi $H \triangleleft A_4$. □

Complément 3 : Si $n \geq 5$, $D(A_n) = D(S_n) = A_n$; en particulier A_n et S_n ne sont pas résolubles.

Preuve.
Il est clair que $D(A_n) \subset D(S_n) \subset A_n$. De plus $D(A_n)$ est un sg distingué de A_n, et n'est pas trivial car A_n n'est pas abélien (pour $n \geq 5$) : $D(A_n) = A_n$. □

Complément 4 : Pour $n \geq 2$, tout sg d'indice n de S_n est isomorphe à S_{n-1}.

Preuve.
C'est trivial si $n \leq 3$. Si $n = 4$, $|H| = 6$. S_4 n'admettant pas d'élément d'ordre 6 (le ppcm des longueurs devrait pour cela être 6), H n'est pas cyclique, ce qui impose $H \simeq S_3$.

Sq $n \geq 5$. S_n agit sur l'ens des classes à gauches S_n/H (qui n'est pas un groupe sauf si $n = 2$), ce que l'on reformule en un morphisme $\varphi : S_n \to \mathfrak{S}(S_n/H)$. $\ker\varphi \lhd S_n$, or $\ker\varphi \subset \mathrm{Stab}(H) = H$ donc $|\ker\varphi| \leq (n-1)! < \frac{n!}{2} = |A_n|$ et $A_n \not\subset H$: le corollaire du th donne $\ker\varphi = \{\mathrm{id}\}$.
Puisque $|S_n/H| = n$, $|S_n| = |\mathfrak{S}(S_n/H)|$ et φ est donc un isomorphisme.
Voyant maintenant l'action naturelle de $\mathfrak{S}(S_n/H)$ sur S_n/H, $\mathrm{Stab}(H) = \varphi(H)$. En effet si $\varphi(\sigma) \in \varphi(S_n) = \mathfrak{S}(S_n/H)$, $\varphi(\sigma)(H) = H \Leftrightarrow \sigma H = H \Leftrightarrow \sigma \in H$. $\varphi(H)$ est ainsi le stabilisateur d'un point de S_n/H sous l'action du groupe symétrique $\mathfrak{S}(S_n/H)$, donc isomorphe au stabilisateur d'un point de $[\![1;n]\!]$ sous l'action de S_n, ce qui est bien isomorphe à S_{n-1}. Finalement, $H \simeq \varphi(H) \simeq S_{n-1}$. □

Réf : • Lang - Algebra : ↑ 32 (lemme, th).
• Perrin : ↑ 13 (ql 1), ↑ 28 (ql 3), ↑ 30 (corollaire, ql 4).

↳ Deux remarques sur Lang. D'abord il note $J_n = [\![1;n]\!]$. Ensuite à la fin de la preuve du th il y a une erreur : il affirme que $\sigma'(a) = a$ (il note $i = a$), alors que c'est faux (c'est plutôt $\sigma'(k) = k$).

↳ Dans les deux parties principales de la preuve du th le raisonnement est le même, avec $\gamma = (c\ d\ e)$ et $\sigma' = [\gamma, \sigma]$ def pareil ; attention cependant les hypothèses sur a, b, c, d, e ne sont pas les mêmes ! Mais la structure et les arguments communs permettent d'aller plus vite à la fin.

↳ Perrin donne une autre preuve du th (elle aussi basée sur le lemme).

↳ Le corollaire et les ql 3 et 4 sont des corollaires du th. Ils sont faits dans Perrin mais pas dans Lang.

↳ Le cas de A_4 et de son sg propre non trivial $H \lhd A_4$ est évoqué dans Lang et Perrin sans démonstration. On peut montrer d'une part que $H = D(A_4)$ (en particulier H est caractéristique et $H \lhd S_4$ également, et A_4 et S_4 sont résolubles), d'autre part que H est l'unique sg propre non trivial distingué de A_4.

↳ On peut aussi mq $D(A_n) = D(S_n) = A_n$ pour $n \geq 5$ en utilisant le lemme mais pas le th. Cette preuve est donnée dans Perrin.

↳ Le corollaire indiquant la non-résolubilité de S_n pour $n \geq 5$ est important par son application en théorie de Galois. Via le théorème d'Abel-Galois (K de car nulle, $P \in K[X]$ irréd : P résoluble par radicaux ssi son groupe de Galois est résoluble) il indique que le polynôme générique sur $K(T_1, \cdots, T_n)$, $P = X^n + \sum_{k=1}^{n} (-1)^k T_k X^{n-k}$, qui est de groupe de Galois S_n, n'est pas résoluble par radicaux si $n \geq 5$. Autrement dit il n'existe pas de formule "par radicaux" générique pour exprimer les racines d'un polynôme de degré ≥ 5 sur K. Cette impossibilité générique n'empêche pas qu'une expression par radicaux soit possible dans certains cas ($Rac(X^5) = \{0\}$ sur $\mathbb{Q}$), mais s'y ajoute une impossibilité dans tous les cas où le groupe de Galois est S_n ($X^5 - 6X + 3$ sur $\mathbb{Q}$ (non trivial)).