LE GROUPE $\mathcal{A}_n$, $n \geq 5$, EST SIMPLE

Référence : Perrin, Cours d'algèbre, pages 28-30.

Théorème 1. *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$.*

Rappelons que si G est un groupe $D(G)$ désigne le groupe dérivé de G à savoir le sous-groupe de G engendré par les commutateurs de G.

Corollaire 2. *Dès que $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$.*
Dès que $n \geq 2$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$.

Remarque 3. Le Corollaire est une conséquence évidente du Théorème 1 mais il peut se montrer directement. Donnons quelques détails. On a les inclusions suivantes :

$$D(\mathcal{A}_n) \subset D(\mathcal{S}_n) \subset \mathcal{A}_n$$

Lemme 4. *Dès que $n \geq 3$ les 3-cycles engendrent $\mathcal{A}_n$.*

Démonstration. Puisque le groupe $\mathcal{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

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

□

Il suffit donc de montrer que tout 3-cycle est dans $\mathcal{A}_n$ un commutateur. Soit $\sigma = (a\ b\ c)$ un 3-cycle, $\sigma^2 = (a\ c\ b)$ en est un autre donc σ et σ^2 sont conjugués dans $\mathcal{A}_n$ ([Perrin, Cours d'Algèbre, Proposition 4.10, page 15]) : il existe τ dans $\mathcal{A}_n$ tel que $\sigma^2 = \tau^{-1}\sigma\tau$ d'où $\sigma = \sigma^{-1}\tau^{-1}\sigma\tau = [\sigma^{-1}, \tau^{-1}]$.

On montre de manière "analogue" que $D(\mathcal{S}_n) = \mathcal{A}_n$ dès que $n \geq 2$.

Remarques 5. Soit H un sous-groupe distingué de G.

— La classe de conjugaison d'un élément $h \in H$ est contenue dans H, c'est-à-dire

$$\forall\, g \in G \qquad ghg^{-1} \in H$$

— Si $h \in H$ et $g \in G$ le commutateur $ghg^{-1}h^{-1} = (ghg^{-1})h^{-1}$ appartient à H et n'est pas, en général, un conjugué de h ; on obtient donc une nouvelle classe de conjugaison, le but étant de montrer qu'un système générateur de G est tout entier dans H.

Démonstration du théorème 1 pour $n = 5$. Le groupe $\mathcal{A}_5$ a 60 éléments :
— le neutre ;
— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;
— 20 éléments d'ordre 3 (3-cycles) ;
— 24 éléments d'ordre 5 (5-cycles).

Les 3-cycles sont conjugués dans $\mathcal{A}_5$ ([Perrin, Cours d'Algèbre, Proposition 4.10, Page 15]). Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.

Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (resp. 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.

Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|H|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|H| \geq 15 + 20 + 1 + 36.$$

Comme $|H|$ divise $|\mathcal{A}_5| = 60$ on obtient $|H| = 60$ et $H = \mathcal{A}_5$. □

Remarque 6. Les 25 éléments d'ordre 5 de $\mathcal{A}_5$ ne sont pas conjugués dans $\mathcal{A}_5$ sinon ils formeraient une orbite et 24 diviserait 60. Nous pouvons cependant éviter le recours à Sylow dans la démonstration précédente en remarquant que si a et b sont d'ordre 5, alors b est conjugué à a ou a^2 dans ∞_5.

Démonstration du théorème 1 pour $n > 5$. Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq H \triangleleft \mathcal{A}_n$. Soit $\sigma \in H \setminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geq 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E\setminus F} = \mathrm{id}_{|E\setminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes
— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;
— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E\setminus F} = \mathrm{id}_{|E\setminus F} \end{cases}$$

Soit $H_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in H\} = H \cap \mathcal{A}(F)$. Alors
— $H_0 \lhd \mathcal{A}(F)$;
— $\rho_{|F} \in H_0$;
— $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $H_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ ([Perrin, Cours d'Algèbre, Proposition 4.10, Page 15]) ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (Lemme 4) on a $H = \mathcal{A}_n$. □

Remarque 7. Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

Corollaire 8. *Dès que $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Lemme 9. *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

Lemme 10. *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 9)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Démonstration du Corollaire 8. Soit $H \lhd \mathcal{S}_n$. Alors $H \cap \mathcal{A}_n \lhd \mathcal{A}_n$ donc $H \cap \mathcal{A}_n \in \big\{\mathrm{id},\ \mathcal{A}_n\big\}$.

Si $H \cap \mathcal{A}_n = \mathcal{A}_n$, alors $H = \mathcal{A}_n$ ou $H = \mathcal{S}_n$.

Si $H \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(H) \subset \{1, -1\}$. Par suite $|H| \leq 2$. Si $|H| = 2$, alors $H = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathcal{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (Lemme 10) : contradiction. Il en résulte que $H = \{\mathrm{id}\}$. □