Simplicité de $\mathcal{A}_n$ pour $n \geq 5$

Perrin, *Cours d'algèbre*, page 28

Théorème : Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$

Nous allons en donner une démonstration en deux temps : pour $n = 5$ d'abord, par une méthode très élémentaire qui mettra en évidence l'intérêt de la connaissance des classes de conjugaison dans les questions de simplicité ; pour $n > 5$ ensuite, par réduction au cas $n = 5$.

Le principe des démonstrations de simplicité est le suivant. Soit H un sous-groupe distingué de G,

1. Si $h \in H$, la classe de conjugaison de h est contenue dans H, *i.e.* on a $\forall g \in G, ghg^{-1} \in H$.
2. Si $h \in H$ et $g \in G$ le commutateur $c = ghg^{-1}h^{-1} = (ghg^{-1})h^{-1}$ est dans H et n'est pas, en général, conjugué de h, de sorte qu'on obtient ainsi une nouvelle classe de conjugaison le but ultime étant de montrer qu'un système générateur de G est tout entier dans H.

• **Le théorème pour** $n = 5$.

Le groupe $\mathcal{A}_5$ a 60 éléments : le neutre, 15 éléments d'ordre 2 (produit de deux transpositions disjointes), 20 d'ordre 3 (3-cycles), 24 d'ordre 5 (5-cycles).

On a vu que les cycles d'ordre 3 sont conjugués dans $\mathcal{A}_5$. Les éléments d'ordre 2 le sont aussi : si $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$, il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(e) = e'$ et on a alors $\tau' = \sigma\tau\sigma^{-1}$.

Soit alors $H \lhd \mathcal{A}_5$, $H \neq \{1\}$. Si H contient un élément d'ordre 3 (resp. 2) il les contient tous d'après ce qui précède. S'il 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, donc tous les éléments d'ordre 5.

Mais H ne peut 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 (n'oublions pas que le cardinal de H divise $|\mathcal{A}_5| = 60$). Donc H contient au moins deux des trois types, d'où $|H| \geq 15+20+1 = 36$ et donc $|H| = 60$, $H = \mathcal{A}_5$.

• **Le cas** $n > 5$

Posons $E = \{1, \ldots, n\}$. Soit $H \lhd \mathcal{A}_n, H \neq \{1\}$ et soit $\sigma \in H$, $\sigma \neq 1$. On va se ramener au cas $n = 5$ et, pour ceci, fabriquer à partir de σ un élément non trivial de H qui n'agisse, en fait, que sur un ensemble à 5 éléments, donc qui ait $n - 5$ points fixes.

Vu les remarques ci-dessus, la méthode naturelle à notre disposition est de prendre un commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$, avec $\tau \in \mathcal{A}_n$. Ecrivant $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$, on a vu que ρ est dans H. Mais si on regarde ρ par l'autre bout : $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$ on constate que ρ est produit de deux éléments du type de τ de sorte que si τ a beaucoup de points fixes, il en sera de même de ρ.

Il ne reste plus qu'à mettre ces remarques en forme :

Comme $\sigma \neq 1$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$, soit τ le 3-cycle $\tau = (acb)$, de sorte que $\tau^{-1} = (abc)$ et soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (acb)(\sigma a, \sigma b, \sigma c)$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma a, \sigma b, \sigma c\}$ a au plus 5 éléments et on a $\rho(F) = F$, $\rho_{|_{E\setminus F}} = Id_{|_{E\setminus F}}$.

Quitte à rajouter, au besoin, des éléments à F, on peut supposer $|F| = 5$. On note enfin que ρ est distinct de 1, car $\rho(b) = \tau\sigma(b) \neq b$ puisque $\sigma(b) \neq \tau^{-1}(b) = c$.

Soit alors $\mathcal{A}(F)$ l'ensemble des permutations paires de F, $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$ et $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ par $u \mapsto \overline{u}$ avec :

$$\overline{u}_{|_F} = u \quad ; \quad \overline{u}_{|_{E\setminus F}} = Id_{|_{E\setminus F}}$$

Posons $H_0 = \{u \in \mathcal{A}_(F) \ / \ \overline{u} \in H\} = H \cap \mathcal{A}(F)$. Il est clair que H_0 est distingué dans $\mathcal{A}(F)$ et qu'on a $\rho_{|_F} \in H_0$ et $\rho_{|_F} \neq Id_F$. Comme $\mathcal{A}(F) \simeq \mathcal{A}_5$ est simple, on a $H_0 = \mathcal{A}(F)$. Soit alors u un cycle d'ordre 3 de $\mathcal{A}(F)$, il est dans H_0, donc $\overline{u}$ qui est encore un cycle d'ordre 3 est dans H.

Mais comme, les 3-cycles sont conjugués dans $\mathcal{A}_n$, ils sont tous dans H, et comme ils engendrent $\mathcal{A}_n$, on a montré $H = \mathcal{A}_n$, ce qui achève la démonstration.