$\mathfrak{A}_n$ est simple

Leçons : *103, 104,* 105, *108*

Théorème 1

Le groupe $\mathfrak{A}_n$ est simple.

Démonstration. Étape 1 : cas $n=5$.

Dans $\mathfrak{A}_5$, les types d'éléments suivants forment des classes de conjugaison distinctes :

- l'identité ;
- les 3-cycles : il y en a $\dfrac{5\times 4\times 3}{3}=20$. En effet, $\mathfrak{A}_5$ est 3-transitif : si (abc) et $(a'b'c')$ sont deux 3-cycles, il existe $\sigma\in\mathfrak{A}_5$ tel que $\sigma(a)=a', \sigma(b)=b'$ et $\sigma(c)=c'$ donc $\sigma(abc)\sigma^{-1}=(a'b'c')$;
- les doubles transpositions : une double transposition de $\mathfrak{A}_5$ est déterminée par le choix de l'élément x laissé fixe (5 possibilités) et par celui de la double transposition restreinte à $[\![1,5]\!]\setminus\{x\}$ (3 possibilités), donc il y en a 15. Elles sont deux à deux conjuguées car si $\tau=(ab)(cd)(e)$ et $\tau'=(a'b')(c'd')(e')$, il existe par 3-transitivité $\sigma\in\mathfrak{A}_5$ envoyant (c,d,e) sur (c',d',e'). Par conséquent, elle envoyant également l'ensemble $\{a,b\}$ sur $\{a',b'\}$ et $\sigma\tau\sigma^{-1}=\tau'$.

Pour des raisons d'ordre, les classes sont bien distinctes. Par ailleurs, il y a $\dfrac{5\times 4\times 3\times 2}{5}=$ 24 5-cycles dans $\mathfrak{A}_5$, et cela achève le catalogue de ses éléments.

Soit H un sous-groupe distingué non trivial de $\mathfrak{A}_5$. Par le théorème de Lagrange, $|H|$ divise 60. De plus, si H contient un 3-cycle (resp. une double transposition), il les contient tous. Il en va de même pour les 5-cycles car si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc comme les 5-Sylow sont deux à deux conjugués (théorème de Sylow), il contient tous les 5-Sylow donc tous les éléments d'ordre 5.

Étant donné que ni $24+15+1=40$, ni $24+20+1=45$, ni $15+20+1=36$ ne divisent 60, il est impossible que H ne contienne que deux catégories d'éléments (et pour les mêmes raisons, il est exclu qu'il en contienne une seule). Donc il les contient tous : $H=\mathfrak{A}_5$.

Étape 2 : cas général, en se ramenant à l'étape 1.

Soit $n>5$, $E=[\![1,n]\!]$, H un sous-groupe distingué non trivial de $\mathfrak{A}_n$. Soit $\sigma\in H$ distinct de l'identité. On peut donc fixer $a\in E$ tel que $b=\sigma(a)\neq a$. Soit $c\notin\{a,b,\sigma(b)\}$ et $\tau=(acb)$. On a $\tau^{-1}=(abc)$.

Introduisons le commutateur $\rho=\tau\sigma\tau^{-1}\sigma^{-1}=(\tau\sigma\tau^{-1})\sigma^{-1}\in H$. On a

$$\rho=(acb)(\sigma(a)\sigma(b)\sigma(c))=(acb)(b\sigma(b)\sigma(c))$$

donc ρ laisse fixes au moins $n-5$ éléments : quitte à ajouter des éléments à l'ensemble $F=\{a,b,c,\sigma(b),\sigma(c)\}$, on peut supposer que c'est exactement le cas.

Soit $\varphi: \begin{array}{ccc}\mathfrak{A}(F) & \longrightarrow & \mathfrak{A}(E)\\ u & \longmapsto & \overline{u}\end{array}$ où $\overline{u}_{|F}=u$ et $\overline{u}_{|E\setminus F}=\mathrm{id}_{E\setminus F}$. On note $H_0=\varphi^{-1}(F)$, c'est un sous-groupe distingué non trivial de $\mathfrak{A}_5$ car $\rho_{|F}\in H_0$, donc selon l'étape 1, $H_0=\mathfrak{A}_5$.

En particulier, si u est un cycle d'ordre 3 de $\mathfrak{A}(F)$, alors $u\in H_0$ donc $\overline{u}\in H$ donc comme les 3-cycles sont deux à deux conjugués dans $\mathfrak{A}_n$ (voir étape 1), H contient tous les 3-cycles donc $H=\mathfrak{A}_n$ car les 3-cycles engendrent $\mathfrak{A}_n$.

□

Remarque.

- S'il reste un peu de temps, on peut expliquer pourquoi les 3-cycles engendrent $\mathfrak{A}_n$ (décomposer en produit pair de transpositions de la forme $(1\,i)$ et regrouper deux à deux).
- $\mathfrak{A}_4$ n'est pas simple car $\langle(12),(34)\rangle$ est un sous-groupe distingué d'ordre 4.

Référence : Daniel PERRIN (1996). *Cours d'algèbre*. Ellipses, pp. 28-30.