$\mathfrak{A}_n$ est simple

Réf:
- Cours d'algèbre, D. Perrin

Leçons: 103, 105, 108.

Théorème

Soit $n \in \mathbb{N}$ tel que $n \geq 5$. Alors $\mathfrak{A}_n$ est simple.

Preuve:

Etape 1: $n = 5$.

Le groupe $\mathfrak{A}_5$ possède 60 éléments :

$$1 + 15 + 20 + 24 = 60$$

(1 : neutre ; 15 : ordre 2 ; 20 : ordre 3 ; 24 : ordre 5)

Les 3-cycles sont conjugués dans $\mathfrak{A}_5$. Les éléments d'ordre 2 le sont aussi. En effet, soient a, b, c, d distincts dans $[\![1,5]\!]$, et a', b', c', d' distincts dans $[\![1,5]\!]$. Notons σ une permutation de $[\![1,5]\!]$ qui vérifie $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(\{c,d\}) = \{c',d'\}$ et $\sigma \in \mathfrak{A}_5$.

Alors on a $\sigma(ab)(cd)\sigma^{-1} = (a'b')(c'd')$ (un tel σ existe!)

Soit alors H sous-groupe distingué de $\mathfrak{A}_5$ non réduit à $\{1\}$. Si H contient un élément d'ordre 3 (resp. 2) alors il les contient tous car ils sont conjugués dans $\mathfrak{A}_5$ et $H \triangleleft \mathfrak{A}_5$.

Puis les 5-Sylows de $\mathfrak{A}_5$ sont engendrés par les éléments d'ordre 5, donc si H contient un élément d'ordre 5 alors il les contient tous aussi.

NB: $n_5 \equiv 1 \bmod 5$ et $n_5 \mid 12$ et il y a 24 éléments d'ordre 5.

Alors le groupe H ne peut contenir qu'un seul de ces trois types d'éléments car ni 25 ni 16 ni 21 ne divisent 60.

Nécessairement, H contient au moins deux des trois types. D'où

$$\#H \geqslant 16 + 20 = 36$$

Toujours car $\#H$ divise 60, on obtient $\#H = 60$ et ainsi $H = \mathfrak{A}_5$.

Etape 2 : $n > 5$

Notons E l'ensemble $\{1, \dots, n\}$. Soit H un sous-groupe distingué de $\mathfrak{A}_n$ tel que $H \neq \{1\}$.

Nous allons nous ramener à $\mathfrak{A}_5$.

Soit $\sigma \in H \setminus \{1\}$. Comme $\sigma \neq 1$, il existe $a \in E$ tel que

$$b = \sigma(a) \neq a$$

Soit $c \in E \setminus \{b, a, \sigma(b)\}$. Notons τ le 3-cycle $(a\ c\ b)$ et p le commutateur $[\tau, \sigma]$. On a alors

$$p = (acb)\,(\sigma(a)\,\sigma(b)\,\sigma(c))$$

Notons F l'ensemble $\{a, b, c, \sigma(b), \sigma(c), \sigma(a)\}$. On a

$$p(F) = F \quad \text{et} \quad p_{|E \setminus F} = id_{E \setminus F}$$

Comme $b = \sigma(a)$, on a $\#F \leqslant 5$.

Quitte à rajouter des éléments à F, on peut supposer $\#F = 5$.

De plus, p est différent de 1. En effet, on a

$$p(b) = \tau\sigma(b) \neq b$$

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

Notons $\mathfrak{A}(F)$ l'ensemble des permutations paires de F. Alors on a naturellement $\mathfrak{A}(F) \simeq \mathfrak{A}_5$. Puis considérons le morphisme injectif

$$\varphi : \begin{array}{ccc} \mathfrak{A}(F) & \longrightarrow & \mathfrak{A}_n \\ u & \longmapsto & \varphi(u) \end{array}$$

de prolongement par l'identité sur $E \setminus F$.

Notons H_0 l'ensemble $\{u \in \mathfrak{S}(F) / \varphi(u) \in H\} = \varphi^{-1}(H)$.

Comme H est distingué, on en déduit que H_0 est distingué dans $\mathfrak{S}(F) \simeq \mathfrak{S}_5$ simple. Or on a vu que $p_{|F} \in H_0$ et $p_{|F} \neq id_F$

D'où $H_0 = \mathfrak{S}(F)$.

Soit u un cycle d'ordre 3 dans $\mathfrak{S}(F)$. Alors $u \in H_0$ et donc $\varphi(u) \in H$.

Or $\varphi(u)$ est toujours un cycle d'ordre 3. Comme les 3-cycles sont conjugués et engendrent $\mathfrak{A}_n$ $(n \geq 3)$, on en déduit

$$H = \mathfrak{A}_n$$

Cela conclut ■

Rmq: comme $\mathfrak{A}_4$ admet V_4 comme sous-groupe distingué, on obtient que $\mathfrak{A}_n$ est simple si et seulement si $n \neq 4$.

Corollaire

Pour tout $n \in \mathbb{N}$ tel que $n \geq 5$ on a

$$D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n$$

Preuve: comme $\mathfrak{A}_n$ est simple et non commutatif, on obtient que le groupe dérivé $D(\mathfrak{A}_n)$, qui est distingué dans $\mathfrak{A}_n$, est égal à $\mathfrak{A}_n$.

Or on a $D(\mathfrak{A}_n) \subset D(\mathfrak{S}_n)$ et $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ car $\frac{\mathfrak{S}_n}{\mathfrak{A}_n}$ est abélien.

Rmq: tout 3-cycle est un commutateur: soit $\sigma = (a,b,c)$ un 3 cycle. Alors $\sigma^2 = (a,c,b)$ en est un autre. Comme les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$, il existe $\tau \in \mathfrak{A}_n$ tel que

$$\sigma^2 = \tau \sigma \tau^{-1}$$

et donc $\sigma = \tau \sigma \tau^{-1} \sigma^{-1} = [\tau, \sigma]$.