Développement : Simplicité de $\mathcal{A}_n$.

RM

2022-2023

Référence :

1. Algèbre Perrin
2. algèbre Rombaldi

Énoncé :

Théorème 1 : Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$.

On pose dans la suite $n \geq 5$.

Résolution :

Lemme 2 : Les cycles d'ordre 3 engendrent $\mathcal{A}_n$.

Démonstration : On sait que $\mathcal{S}_n$ est engendré par les transpositions et que la signature d'une transposition est -1. Donc si $\sigma \in \mathcal{A}_n$, alors σ est un produit paire de transpositions. De plus on a les formules : $(a,b)(b,c) = (a,b,c)$ et $(a,b)(a,c) = (a,c,b)$. On en déduit

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

Donc chaque produit de transposition est un produit de 3-cycles. On en déduit que les 3-cyles engendrent $\mathcal{A}_n$. □

Lemme 3 : Les 3-cycles sont conjuguées dans $\mathcal{A}_n$.

Démonstration : On sait que les p-cycles sont conjugués dans $\mathcal{S}_n$

> En effet, si $\sigma = (a_1, ..., a_p)$ et $\tau \in \mathcal{S}_n$, alors on la relation " de conjugaison " $\tau\sigma\tau^{-1} = (\tau(a_1), ..., \tau(a_p))$. Donc si on prend $\sigma = (a_1, ..., a_p)$ et $\tau = (b_1, ..., b_p)$ deux p-cycles, alors il existe $g \in \mathcal{S}_n$ tel que $g(a_i) = b_i$. On a donc $\tau = g\sigma g^{-1}$ ce qui prouve que les p-cycles sont conjugués.

Soient (a,b,c) et (d,e,f) deux 3-cycles. Donc il existe $\sigma \in \mathcal{S}_n$ tel que $\sigma(a,b,c)\sigma^{-1} = (d,e,f)$. Si $\sigma \in \mathcal{A}_n$, alors c'est bon. Sinon, on prend $\sigma' = \sigma(i,j)$ ou i,j différent de a,b,c,d,e,f qui est donc de signature pair et donc dans $\mathcal{A}_n$. On a bien $\sigma'(a,b,c)\sigma'^{-1}$ et donc les 3-cycles sont conjugués. □

Nous allons 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 $n = 5$, suivant une technique que nous retrouverons pour les groupes orthogonaux.
Le principe des démonstrations de simplicité que nous donnerons dans cet ouvrage 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 (car $ghg^{-1} \in H$ comme H est distingué et $h^{-1} \in H$) 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.

1. Le théorème pour $n = 5$.

   Le groupe $\mathcal{A}_5$ à 60 éléments : le neutre, 15 éléments d'ordre 2 (produit de 2 transpositions disjointes), 20 d'ordre 3, 24 d'ordre 5.
   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 $\tau' = (a'b')(c'd')(e')$, comme (a, b, e) et (a', b', e') sont conjugués dans $\mathcal{A}_5$, il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a, b, e)\sigma^{-1} = (a', b', e')$. On a alors σ qui envoie $\{c, d\}$ sur $\{c', d'\}$ (les deux fonctionnent) et donc $\sigma\tau\sigma^{-1} = \tau'$ qui sont donc conjugués.
   Soit H un sous-groupe distingué de $\mathcal{A}_5$ différent du groupe trivial. Si H contient un élément d'ordre 3 (respectivement 2), alors on peut atteindre tous les autres éléments d'ordre 3 (respectivement 2) par conjugaison, et comme H est distingué, ils sont tous dans H. S'il contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc tous les 5-Sylow puisqu'ils sont conjugués et encore une fois car H est distingué, donc tous les éléments d'ordre 5.
   Mais H ne peut contenir un seul des trois types éléments précédents (en plus du neutre) car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (par Lagrange). Donc H contient au moins deux des trois types, d'où $|H| \geq 15 + 20 + 1 = 36$ et donc $|H| = 60$. Finalement, $H = \mathcal{A}_5$ et donc $\mathcal{A}_5$ est simple.

2. Le cas $n > 5$.

   Posons $E = \{1, ..., n\}$. Soit H sous-groupe distingué de $\mathcal{A}_n$ non trivial et soit $\sigma \neq Id$ dans H. 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.
   Comme $\sigma \neq Id$, 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 $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (acb)(\sigma(a), \sigma(b), \sigma(c)) \in H$ (voir début remarque 2)). 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 $\rho(b) = \tau\sigma(b) \neq b$ car $\sigma(b) \neq c$ par hypothèse.
   Soit $\mathcal{A}(F)$ 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 $H_0 = \{u \in \mathcal{A}(F) | \overline{u} \in H\} = H \cap \mathcal{A}(F)$ (au sens ou si $u \in \mathcal{A}_n$, alors u est dans H_0 si $u_{|F} \in \mathcal{A}(F)$ et $u \in H$). Soit $u \in H_0$ et $v \in \mathcal{A}(F)$, alors $vuv^{-1} \in \mathcal{A}(F)$ et $\overline{vuv^{-1}} = \overline{v}\overline{u}\overline{v^{-1}} \in H$ car H est distingué. Donc H_0 est distingué dans $\mathcal{A}(F)$. De plus, on a que $\rho_{|F} \in \mathcal{A}(F)$ (car produit de 3-cycles) et $\overline{\rho_{|F}} = \rho \in H$ et donc $\rho_{|F} \in H_0$ avec $\rho_{|F} \neq Id_F$, donc H_0 n'est pas trivial. Comme $\mathcal{A}(F) \cong \mathcal{A}_5$, on a que $\mathcal{A}(F)$ est simple et donc H_0 est finalement égale à $\mathcal{A}(F)$. Soit alors u un 3-cycle de $\mathcal{A}(F)$ (existe car $\mathcal{A}(F) \cong \mathcal{A}_5$), il est dans H_0, donc $\overline{u}$ qui est encore un cycle d'ordre 3 est dans H.
   Comme les 3-cycles sont conjugués dans $\mathcal{A}_n$, ils sont tous dans H, et comme ils engendrent $\mathcal{A}_n$, on a finalement $H = \mathcal{A}_n$ et donc $\mathcal{A}_n$ est simple.