Simplicité du groupe alterné

Mon développement

Lemme.
(i) Les produits de deux transpositions disjointes sont conjugués dans $\mathfrak{A}_5$.
(ii) Les 3-cycles sont conjugués dans $\mathfrak{A}_n$ lorsque $n \geq 5$.

Soient $n \geq 3$, $a_1, \ldots, a_{n-2}$ des éléments distincts de $\{1, \ldots, n\}$ et $b_1, \ldots, b_{n-2}$ des éléments distincts de $\{1, \ldots, n\}$ également. Il existe alors $\sigma \in \mathfrak{A}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i \in [\![1, n-2]\!]$.
En effet, en écrivant

$$\{1, \ldots, n\} = \{a_1, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et en notant σ l'application envoyant tout a_i sur b_i, l'une des deux permutations σ ou $\sigma(a_{n-1}a_n)$ est paire, donc l'une des deux convient.

Ainsi, soient σ, σ' deux produits de deux transpositions disjointes. On note $\sigma = (ab)(cd)(e)$ et $\sigma' = (a'b')(c'd')(e')$. D'après ce qui précède, il existe $\tau \in \mathfrak{A}_5$ telle que $\tau(a) = a'$, $\tau(b) = b'$ et $\tau(e) = e'$. On a alors $\tau\sigma\tau^{-1} = \sigma'$.
Les produits de deux transpositions disjointes sont donc conjugués dans $\mathfrak{A}_5$.

De même, soient $\sigma = (abc)$ et $\sigma' = (a'b'c')$ deux 3-cycles dans $\mathfrak{A}_n$, $n \geq 5$. Il existe $\tau \in \mathfrak{A}_n$ telle que $\tau(a) = a'$, $\tau(b) = b'$ et $\tau(c) = c'$, et on a alors $\tau\sigma\tau^{-1} = \sigma'$.
Les 3-cycles sont donc conjugués dans $\mathfrak{A}_n$ lorsque $n \geq 5$. □

Proposition. Soit $n \in \mathbb{N}^*$. Le groupe alterné $\mathfrak{A}_n$ est simple si et seulement si $n \neq 4$.

- Lorsque $n \leq 3$, il est évident que $\mathfrak{A}_n$ est simple.

- Le groupe $\mathfrak{A}_4$ est constitué de 12 éléments : l'identité, 3 produits de deux transpositions disjointes et 8 cycles d'ordre 3. Le sous-groupe

$$H = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$$

engendré par les doubles transpositions est distingué dans $\mathfrak{A}_4$ puisque, si τ est une double transposition et $\sigma \in \mathfrak{A}_4$, alors $\sigma\tau\sigma^{-1}$ est encore une double transposition.
Le groupe $\mathfrak{A}_4$ n'est donc pas simple.

- Le groupe $\mathfrak{A}_5$ possède 60 éléments : l'identité, 15 produits de deux transpositions disjointes (éléments d'ordre 2), 20 cycles d'ordre 3 et 24 cycles d'ordre 5. D'après le lemme, les éléments d'ordre 2 sont conjugués dans $\mathfrak{A}_5$, de même pour les éléments d'ordre 3.

Soit H un sous-groupe distingué de $\mathfrak{A}_5$, distinct de $\{\mathrm{Id}\}$.
D'après la remarque précédente, si H contient un élément d'ordre 2, alors il les contient tous.
De même pour les éléments d'ordre 3.
De plus, si H contient un élément d'ordre 5, noté σ, alors il contient le 5-Sylow $< \sigma >$, donc,

les 5-Sylow étant conjugués entre eux, H contient tous les 5-Sylow de $\mathfrak{A}_5$, donc H contient tous les éléments d'ordre 5.
En conclusion, si H contient un élément différent de l'identité, alors il contient tous les éléments ayant le même ordre.

Comme $\text{Card}(H)$ divise $\text{Card}(\mathfrak{A}_5) = 60$, et 16, 21, 25 ne divisent pas 60, H ne peut contenir exactement un des trois types d'éléments précédents (en plus de l'identité). H contient donc au moins deux des trois types d'éléments, donc $\text{Card}(H) \geq 1 + 15 + 20 = 36$. Puisque $\text{Card}(H)$ divise 60, on en déduit que $\text{Card}(H) = 60$ et que $H = \mathfrak{A}_5$.

Finalement, le groupe $\mathfrak{A}_5$ est simple.

• On considère désormais le cas où $n > 5$. On note $E = \{1, \ldots, n\}$.
Soit H un sous-groupe distingué de $\mathfrak{A}_n$ distinct de $\{\text{Id}\}$.
Il existe un élément $\sigma \in H \setminus \{\text{Id}\}$. Cet élément n'étant pas l'identité, il existe $a \in E$ tel que $b = \sigma(a)$ soit distinct de a. Soient $c \in E \setminus \{a, b, \sigma(b)\}$ et $\tau = (acb)$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ contient au plus 5 éléments.
Soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (acb)(\sigma(a)\sigma(b)\sigma(c))$.
On a
- $\rho(F) = F$,
- pour tout $d \in E \setminus F$, $\rho(d) = d$,
- $\rho \neq \text{Id}$, puisque $\rho(b) = \tau\sigma(b) \neq \tau(c) = b$,
- $\rho \in H$, puisque $\tau\sigma\tau^{-1} \in H$ et $\sigma^{-1} \in H$.

De plus, quitte à rajouter des éléments à F, on peut supposer que $|F| = 5$, ce qui ne change pas les quatre propriétés ci-dessus. Alors, l'ensemble $\mathfrak{A}(F)$ des permutations paires de F est isomorphe à $\mathfrak{A}_5$.

On note A l'ensemble des $u \in \mathfrak{A}_n$ tels que pour tout $d \in E \setminus F$, $u(d) = d$. A est clairement un sous-groupe de $\mathfrak{A}_n$. On note alors

$$\pi : \begin{array}{ccc} A & \rightarrow & \mathfrak{A}(F) \\ u & \rightarrow & u|_F^F \end{array} .$$

π est bien défini, c'est un morphisme de groupes, il est clairement injectif et surjectif, donc c'est un isomorphisme. On en déduit que A est isomorphe à $\mathfrak{A}_5$, donc A est simple d'après le point précédent.

Soit $H_0 = A \cap H$. H_0 est un sous-groupe de A et il est distingué dans A. En effet, pour tous $u \in A$ et $v \in H_0$, uvu^{-1} appartient à A et à H (car H est distingué dans $\mathfrak{A}_n$), donc à H_0.
De plus, ρ appartient à H_0 et $\rho \neq \text{Id}$, donc $H_0 \neq \{\text{Id}\}$. A étant simple, on en déduit que $H_0 = A$, et donc $A \subset H$.
Par conséquent, H contient le 3-cycle τ. H étant distingué dans $\mathfrak{A}_n$ et les 3-cycles étant conjugués dans $\mathfrak{A}_n$ (point (ii) du lemme), H contient tous les 3-cycles. Le groupe $\mathfrak{A}_n$ étant engendré par les 3-cycles, on en déduit que H contient $\mathfrak{A}_n$, donc $H = \mathfrak{A}_n$.

En conclusion, on a montré que $\mathfrak{A}_n$ est simple pour $n > 5$. □

Références

J'ai utilisé [Per96, pp. 15, 28]. On peut aussi consulter [Jac74, p. 240].

Leçons correspondantes

J'utilise ce développement pour les leçons 103, 104, 105. On peut également l'utiliser pour la leçon 108.

Remarques

– Implicitement, on a utilisé à plusieurs reprises la formule $\tau(a_1 \dots a_p)\tau^{-1} = (\tau(a_1) \dots \tau(a_p))$.
– On utilise le théorème de Sylow (voir [Per96, p. 19]) pour la simplicité de $\mathfrak{A}_5$. Comme il l'est mentionné dans [Per96, p. 29], il est possible de se passer de cet argument, ce qui est préférable afin d'éviter l'utilisation d'un « gros » théorème.
– Si ce développement est présenté dans la leçon 108, il faut insister sur le rôle des parties génératrices et éventuellement modifier la présentation.
– Un autre développement classique consiste à démontrer que $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60. Voir [Ort04, p. 91] par exemple.

Questions possibles

1. Peut-on généraliser le point (i) du lemme à $\mathfrak{A}_n$?
2. Les cycles d'ordre 5 sont-ils conjugués dans $\mathfrak{A}_5$?
3. Étudier la conjugaison des 3-cycles dans $\mathfrak{A}_3$ et $\mathfrak{A}_4$.
4. Le groupe $\mathfrak{A}_4$ est-il simple ?
5. Montrer que les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.
6. Montrer que pour tout $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble.
7. Expliquer comment on calcule le nombre de doubles transpositions dans $\mathfrak{A}_5$. Indication : étudier le commutant des doubles transpositions dans $\mathfrak{A}_5$.

Références

[Jac74] Nathan Jacobson : *Basic algebra I.* W. H. Freeman and Company, 1974.

[Ort04] Pascal Ortiz : *Exercices d'algèbre.* Ellipses, 2004.

[Per96] Daniel Perrin : *Cours d'algèbre.* Ellipses, 1996.