Simplicité de A_n pour $n \geq 5$

Leçons 103,104,105,108

Théorème (Simplicité du groupe alterné A_n pour $n \geq 5$)

Soit $n \geq 5$. Le groupe alterné $A_n = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$ est un groupe simple (où ε désigne le morphisme de signature).

Voici le plan de la démonstration:

1. Montrer la simplicité de A_5 en étudiant ses classees de conjugaison.

2. Montrer le cas général en considérant $\sigma \in A_n$ ayant $n-5$ points fixes puis en utilisant la simplicité de A_5

Avant de montrer le théorème, on étudie quelques résultats préliminaires:

Définition (Type d'une permutation)

Soit $\sigma \in S_n$. On dit que σ est de type $[k_1, \cdots, k_n]$ si, et seulement si σ s'écrit comme un produit de cycles à support disjoint comportant:

- k_1 cycles de longueur 1 (points fixes)
- k_2 2-cycles
- $\vdots$
- k_n n-cycles (k_n vaut 0 ou 1)

Lemme (Cardinal d'une classe de conjugaison de S_n)

Dans S_n, le nombre de permutations du type $[k_1, \cdots, k_n]$ est de:

$$\frac{n!}{\prod_{i=1}^{n} k_i! i^{k_i}}$$

Lemme (Deux propriétés de A_n)

Soit $n \geq 5$. On a alors:

1. A_n est engendré par les 3-cycles
2. Les 3-cycles sont conjugués dans A_n

Démonstration. *1. Soit $\sigma \in A_n$. On écrit σ comme un produit de transpositions τ_i: $\sigma = \tau_1 \cdots \tau_{2k}$ (le nombre est pair puisque $\sigma \in A_n$). Montrons alors que $\tau_i\tau_{i+1}$ est un produit de 3-cycles, où $i \in 2\mathbb{N}$:*

- *Si $\tau_i = \tau_{i+1}$, alors $\tau_i\tau_{i+1} = Id$*
- *Si $\tau_i = (ab)$ et $\tau_{i+1} = (ac)$, alors $\tau_i\tau_{i+1} = (ab)(ac) = (acb)$*
- *Si $\tau_i = (ab)$ et $\tau_{i+1} = (cd)$, alors $\tau_i\tau_{i+1} = (ab)(cd) = (abc)(bcd)$*

2. Soient (abc) et $(\alpha\beta\gamma)$ deux trois cycles quelconques de A_n. Soit $\sigma \in S_n$ donnée par $\sigma(a) = \alpha$, $\sigma(b) = \beta$ et $\sigma(c) = \gamma$. On a alors: $\sigma(abc)\sigma^{-1} = (\alpha\beta\gamma)$. Si σ est paire, alors c'est terminé. Si σ est impaire, comme $n \geq 5$, il existe $\varepsilon, \delta \notin \{\alpha\beta\gamma\}$ distincts et on pose alors: $\sigma' = (\delta\varepsilon)\sigma$. On a donc $\sigma'(abc)\sigma'^{-1} = (\alpha\beta\gamma)$, et σ' est paire.

■

On peut maintenant passer à la démonstration du théorème principal:

Démonstration. *1. On étudie les classes de conjugaison de A_5 via la relation orbite-stabilisateur (appelé centralisateur)*

- $\left|C_{(12345)}\right| = \frac{|A_5|}{Z_{(12345)}} = \frac{|A_5|}{|\langle(12345)\rangle|} = 12$. *$C_{(12345)}$ est une classe de conjugaison à 12 éléments.*
- $\left|C_{(21345)}\right| = \frac{|A_5|}{Z_{(21345)}} = \frac{|A_5|}{|\langle(21345)\rangle|}$. $C_{(21345)}$. *$C_{(21345)} = 12$ est une classe de conjugaison à 12 éléments.*
- *Il y a 15 bitranspositions et $C_{(12)(34)} = \frac{|A_5|}{Z_{(12)(34)}} = \frac{|A_5|}{|V_4|} = 15$. Les bitranspositions forment une classe de conjugaison à 15 éléments.*
- *Il y a 20 3-cycles et par le lemme précédent, ces derniers forment une classe de conjugaison de A_n, comportant ainsi 20 éléments.*
- *Le neutre $\{Id\}$ forme une classe de conjugaison à 1 élément*

Soit $H \lhd A_5$, tel que $H \neq \{Id\}$. Alors H contient une classe de conjugaison hors du neutre. En vertu du théorème de Lagrange, on a $|H|\,||A_n| = 60$

- *Si il en a strictement une, alors $|H| \in \{13, 16, 21\}$, mais aucun de ces nombres ne divise 60, donc il y a au moins deux classes de conjugaison hors de $\{Id\}$.*
- *Avec deux classes de conjugaison hors du neutre, on a $|H| \in \{25, 28, 36\}$, là encore, aucun de ces nombres ne divise 60, donc il y a au moins trois classes de conjugaison hors du neutre.*
- *Avec trois classes de conjugaison hors du neutre, on a toujours $|H| \geq 40$, donc forcément $|H| = 60$, d'où $H = A_5$.*

Donc A_5 est simple.

2. *Montrons le cas général: Soit $n > 5$ un entier naturel et soit $H \lhd A_n$ un sous-groupe normal. Supposons que $H \neq \{Id\}$. Donc il existe $\sigma \in H$ tel que $\sigma \neq Id$. Construisons un élément non trivial de H comportant $n-5$ points fixes: $\sigma \neq Id$ donc il existe $\sigma \in [\![1,n]\!]$ tel que $\sigma(a) \neq a$. Soit $c \in [\![1,n]\!]$ tel que $c \neq a, \sigma(a), \sigma^2(a)$ et soit $\tau = (a\, c\, \sigma(a))$. Posons $\rho = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$ (commutateur).*

   On a alors: $\rho = (a\, c\, \sigma(a))(\sigma(a)\, \sigma(c)\, \sigma^2(a))$. Soit $F = \{a, \sigma(a), \sigma^2(a), c, \sigma(c)\}$. On a $\rho(F) = F$. Quitte à rajouter des éléments, on peut supposer que $|F| = 5$. $\varepsilon(\rho) = 1$ donc on a:

$$\rho \in A_F \quad \simeq \quad A_5 \tag{1}$$

   Soit $H_0 = \{u \in A_F : \overline{u} \in H\} = H \cap A_F$. On a: $H_0 \lhd A_F \simeq A_5$. Par simplicité de A_5, on a: $H_0 = \{Id\}$ ou $H_0 = A_F$, de plus, on a $\rho|_F \in H_0$ et $\rho|_F \neq Id$, donc $H_0 = A_F$.

   Soit $u \in A_F = H \cap A_F$ un 3-cycle (qui est, par construction, un 3-cycle de A_n). H contient donc un 3-cycle de A_n, et les 3-cycles forment une classe de conjugaison de A_n, et $H \lhd A_n$, donc tous les 3-cycles sont contenus dans H. Or, par le lemme précédent, A_n est engendré par les 3-cycles, donc $H = A_n$, donc A_n est simple.

■

Remarque(s). *L'isomorphisme donné par (1) est évident. De plus, on a l'injection suivante:*

$$\begin{array}{ccc} A_F & \hookrightarrow & A_n \\ u & \longmapsto & \overline{u} \end{array}$$

où l'on a:
$\overline{u}|_{[\![1,n]\!]\setminus F} = Id|_{[\![1,n]\!]\setminus F}$ *et* $\overline{u}|_F = u$

Reférence(s). *D. Perrin, Cours d'algèbre*