Rombaldi Mathématiques pour l'agrégation p 52
Perrin Cours d'Algèbre. p 15

103
104
105
108

Développement : Simplicité du groupe alterné.

Théorème : Si $n \geq 5$, alors A_n est simple.

Démo :

(1) **Lemme :** Le groupe A_n est engendré par les 3 cycles. De plus, les 3 cycles sont conjugués dans A_n.

- Soit $\sigma \in A_n$. En utilisant la décomposition en produit de cycles à support disjoint, on écrit $\sigma = \tau_1 \cdots \tau_{2k}$ comme produit de transpositions. Remarquons que les transpositions sont en nombre pair, puisque la signature est paire.
Ainsi, pour prouver que les 3 cycles engendrent A_n, il suffit de prouver qu'un produit de transpo $\tau_1\tau_2 \in A_n$ est produit de 3 cycles.
On distingue trois cas :
i) Si $\tau_1\tau_2 = (ab)(ab) = id$ alors $\tau_1\tau_2 = \gamma^3$ pour n'importe quel 3 cycle.
ii) Si $\tau_1\tau_2 = (ab)(bc)$ alors $\tau_1\tau_2 = (abc)$.
iii) Si $\tau_1\tau_2 = (ab)(cd)$ alors $\tau_1\tau_2 = (ab)(bc)(bc)(cd) = (abc)(bcd)$
- Soient (abc) et $(a'b'c')$ deux 3 cycles. On sait qu'ils sont conjugués dans S_n (p15 Per)
donc il existe $\sigma \in S_n$ tq $(abc) = \sigma(a'b'c')\sigma^{-1} = (\sigma(a')\sigma(b')\sigma(c'))$
i) Si $\sigma \in A_n$, il n'y a rien à faire $\qquad |A_n| \geq |A_5| = 60$
q voir exo 2.23
ii) Sinon, puisque $n \geq 5$, on peut prendre $i \neq j \neq (a', b', c')$. Soit alors $\tau = (ij)$. Alors
car $\tau(a') = a'$ car $i, j \neq a'$!
$(abc) = (\sigma\tau(a')\,\sigma\tau(b')\,\sigma\tau(c')) = \sigma\tau\,(a'b'c')\,(\sigma\tau)^{-1}$ et $\sigma\tau \in A_n$
$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = -1 \cdot -1 = 1$ et $\sigma\tau \in A_n$
Dans tous les cas (abc) et $(a'b'c')$ sont conjugués dans A_n.

(2) On démontre maintenant le théorème.
Soit $H \triangleleft A_n$ non trivial. Mq $H = A_n$. On a vu que les 3 cycles engendraient A_n.
Donc il suffit de mq tous les 3 cycles sont dans H. Or, les 3 cycles sont conjugués dans A_n et H est stable par conjugaison puisque $H \triangleleft A_n$.
? existence ? on le def comme ça
On se donne $\sigma \in H \setminus \{id\}$ et $\gamma = (xzy) \in A_n$ un 3 cycle tq $y = \sigma(x)$ qui ne commute pas à σ (exo 2.23). Puisque $H \triangleleft A_n$ on a $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1}$ on le def comme ça.
H est 1 gr $\quad = \underbrace{\sigma}_{\in H}\,(\underbrace{\gamma\sigma^{-1}\gamma^{-1}}_{\in H}) \in H$ et en écrivant que
$$\sigma' = (\sigma(xzy)\sigma^{-1})(yzx) = (\sigma(x)\sigma(z)\sigma(y))(yzx)$$
$$= (y\,\sigma(z)\,\sigma(y))(yzx).$$

$A(E) = \{\sigma \in S(E) \mid \varepsilon(\sigma) = 1\}$
$S(E) = \{$ bij de $E \to E\}$
où $m = \dim E$.
$(2,1,1,1)$
$(3,2), (4,1)$
cas à exclure car de signature impaire !

Si on prouve les mus dire.

Attention à la preuve du Rombaldi

on voit que σ' est produit de deux 3cycles qui agissent sur l'ensemble $F = \{x, y, z, \sigma(y), \sigma(z)\}$ et $\mathrm{card}(F) \leq 5$ (tous les pts de $E \setminus F$ sont fixes)

- si $\sigma' = id$ alors $\sigma \gamma \sigma^{-1} \gamma^{-1} = id$, $\sigma\gamma = \gamma\sigma$ ie σ et γ commutent. C'est absurde par hypothèse donc $\sigma' \neq id$.
- si σ' est un 3cycle, c'est terminé.
- si σ' est un produit de deux transpositions à support disjoint on a $\sigma' = (x_1\, x_2)(x_3\, x_4)$ et en choisissant $x_5 \in E \setminus \{x_1, \dots, x_4\}$, on a :

$$\sigma'' = (x_1 x_2 x_5)\underbrace{\sigma' (x_1 x_2 x_5)^{-1} (\sigma')^{-1}} = \overbrace{\left((x_1 x_2 x_5)\, \sigma' (x_1 x_2 x_5)^{-1}\right)}^{\in H \triangleleft A_m} \overbrace{(\sigma')^{-1}}^{\in H} \overset{\text{ok}}{\in H}$$

avec $\sigma'' = (x_1 x_2 x_5)\left(\sigma'(x_1) \sigma'(x_5) \sigma'(x_2)\right) = (x_1 x_2 x_5)(x_2 x_5 x_1) = (x_1\, x_5\, x_2)$

et c'est terminé.

- si $\sigma' = (x_1\, x_2\, x_3\, x_4\, x_5)$ alors :

$$\sigma'' = (x_1 x_2 x_3)\underbrace{\sigma'(x_1 x_2 x_3)^{-1} (\sigma')^{-1}} = \overbrace{\left((x_1 x_2 x_3)\, \sigma'(x_1 x_2 x_3)^{-1}\right)}^{\in H \triangleleft A_m} \overbrace{(\sigma')^{-1}}^{\in H} \overset{\text{ok}}{\in H}$$

$$= (x_1 x_2 x_3)\left(\sigma'(x_1) \sigma'(x_2) \sigma'(x_3)\right) = (x_1 x_2 x_3)(x_2 x_4 x_3) = (x_1\, x_2\, x_4)$$ et c'est terminé.

Dans tous les cas, on a bien trouvé un 3cycle dans H et donc par la remarque du début de la preuve $H = A_m$ ie A_m est simple.

<u>Remarques</u> :

- A_1 et A_2 sont triviaux donc simples.
- $A_3 \simeq \mathbb{Z}_3$ qui est simple aussi.
- Un exercice classique consiste à mq $D = \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4$

- Résultat fondamental dans la théorie de Galois. Permet de mq les équations polynomiales de d° ≥ 5 ne sont pas résolubles par radicaux (ie il n'y a pas de formules n'utilisant que les coefficients, la valeur x, les 4 opérations $+ - \times \div$ et l'extraction des racines $n$ièmes)

- Il faut savoir faire l'exo 2.23 du Rombaldi :

Si γ est un 3cycle, il en est de m̂ de $\gamma^{-1} = \gamma^2$ donc γ^2 est conjugué à γ ds A_m, $\exists \sigma \in A_m$, $\gamma^2 = \sigma^{-1}\gamma\sigma$ et $\gamma = \gamma^{-1}\sigma^{-1}\gamma\sigma \neq id$

donc $\gamma\sigma \neq \sigma\gamma$ et σ et γ ne commutent pas.

Prendre le 3cycle $(x\, z\, \sigma(x))$

Pourquoi $\sigma \in H \setminus \{id\}$?