
Simplicité de $\mathfrak{A}_n$ (pour $n \geq 5$)

Recasage : 103 / 104 / 105 / 108

Référence : Rombaldi p.50

On commence par démontrer deux lemmes avant la preuve du théorème. On se fixe alors $n \geq 5$

Lemme 1

$\mathfrak{A}_n$ est engendré par les trois cycles.

Preuve.

On pose G le groupe engendré par les 3 cycles, on veut démontrer que $G = \mathfrak{A}_n$ procédons par double inclusions :

► Soit $\sigma \in G$, par définition la signature d'un trois cycle est 1 donc $\sigma \in \mathfrak{A}_n$ de fait $G \subset \mathfrak{A}_n$.

► On considère $\sigma \in \mathfrak{A}_n$ on peut alors décomposer σ en produit de transposition donc $\sigma = \prod_{i=1}^p \tau_i$ où chaque τ_i est une transposition. Or $\epsilon(\sigma) = 1$ puisque $\sigma \in \mathfrak{A}_n$ donc p est pair. Montrons à présent que le produit de deux transpositions est nécessairement un trois cycles : Soit $a, b, c, d \in \llbracket 1; n \rrbracket$

$$(a \ b)(c \ d) = (a \ b \ c)(b \ c \ d) \quad \text{et} \quad (a \ b)(c \ a) = (b \ a \ c)$$

Ainsi le produit de deux transpositions est nécessairement un 3-cycles donc σ est un 3-cycles. De fait $\mathfrak{A}_n \subset G$ et finalement $G = \mathfrak{A}_n$ ■

Lemme 2

Les 3-cycles sont conjugués dans $\mathfrak{A}_n$

Preuve.

On se donne deux trois cycles $(a \ b \ c), (d \ e \ f)$ avec a, b, c distinct et d, e, f distincts. On sait que les trois cycles sont conjugués dans $\mathfrak{S}_n$ donc il existe $\sigma \in \mathfrak{S}_n$ tel que $(a \ b \ c) = \sigma(d \ e \ f)\sigma^{-1}$ on peut alors distinguer deux cas :

► Si $\sigma \in \mathfrak{A}_n$ c'est bon.

► Sinon on peut trouver i, j distinct de a, b, c (car $n \geq 5$) tel que $\sigma' = \sigma(i \ j) \in \mathfrak{A}_n$ de ce fait $\sigma'(a \ b \ c)\sigma'^{-1} = (d \ e \ f)$

Finalement les trois cycles sont conjugués dans $\mathfrak{A}_n$ ■

Théorème 1

$\mathfrak{A}_n$ est simple pour $n \geq 5$

Preuve.

Soit $H \triangleleft \mathfrak{A}_n$ (un sous groupe **distingué**) tel que H ne soit pas le groupe identité. On veut montrer que $H = \mathfrak{A}_n$. Il suffit alors d'après les lemmes que H contient un trois cycles, si c'est le cas H contiendra tous les trois cycles puisque ces derniers sont tous conjugués (lemme 2) et enfin on obtiendra $H = \mathfrak{A}_n$ par le lemme 1.

Soit $\sigma \in H \setminus \{I_d\}$ et soit $a \in \llbracket 1; n \rrbracket$ tel que $\sigma(a) \neq a$ et $b = \sigma(a)$ (ce qui est possible car σ n'est pas l'identité). On fixe alors également c tel que $c \neq a, b, \sigma(b)$ ce qui est toujours possible puisque $n \geq 5$. On considère alors le trois cycles $\gamma = (a \ b \ c)$ et la permutation $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1}$. Comme H est distingué dans $\mathfrak{A}_n$ alors $\sigma' \in H$ en effet on écrit par associativité $\sigma' = \sigma(\gamma\sigma^{-1}\gamma^{-1})$ De plus :

$$\begin{aligned}\sigma' &= (\sigma\gamma\sigma^{-1})\gamma^{-1} \\ &= (\sigma(a) \ \sigma(b) \ \sigma(c))(c \ b \ a) \\ &= (b \ \sigma(b) \ \sigma(c))(c \ b \ a)\end{aligned}$$

On peut alors décomposer σ' en produit de cycles à support disjoint et que le support à au plus 5 éléments on peut donc affirmer que σ ne peut pas être un 4 cycles ou alors un produit d'un trois cycles et d'une transposition sinon on aurait des signatures -1). On distingue alors tous les cas possibles :

- Si $\sigma' = I_d$ alors $\sigma\gamma = \gamma\sigma$ on aurait donc $\sigma(\gamma(a)) = \gamma(\sigma(a))$ et donc on aurait $c = \sigma(b)$ ce qui est impossible par construction de c .
- Si σ' est un produit de transposition alors $\sigma' = (i \ j)(k \ l)$ on peut alors trouver $m \notin \{i, j, k, l\}$. On pose alors $\tau = (i \ j \ m) \in \mathfrak{A}_n$ on pose alors $\sigma'' = \sigma'\tau\sigma'^{-1}\tau^{-1}$ et comme H est distingué $\sigma'' \in H$ c'est un 3-cycles :

$$\begin{aligned}\sigma'' &= (\sigma'\tau\sigma'^{-1})\tau^{-1} \\ &= (\sigma'(i) \ \sigma'(j) \ \sigma'(m))(m \ j \ i) \\ &= (j \ i \ m)(m \ j \ i) \\ &= (j \ m \ i)\end{aligned}$$

- Si σ' est un trois cycle c'est bon.
- Si σ' est un cinq cycle alors $\sigma' = (i \ j \ k \ l \ m)$ donc en posant $\sigma'' = (i \ j \ k)\sigma'(i \ j \ k)^{-1}\sigma'^{-1}$ toujours du fait que H est distingué on obtient alors en calculant que $\sigma'' = (i \ j \ k)(\sigma'(i) \ \sigma'(j) \ \sigma'(k)) = (i \ j \ k)(j \ k \ l) = (i \ l \ k)$

Dans tous les cas on retrouve bien un trois cycle de fait H contient un trois cycles, il les contient donc tous et donc d'après les lemmes $H = \mathfrak{A}_n$.

■