Simplicité du groupe A_n lorsque $n \geq 5$

Préparation à l'agrégation de mathématiques
Université de Nice - Sophia Antipolis
Antoine Ducros

Novembre 2007

Nous nous proposons dans ce court texte de donner une traduction en français de la preuve de la simplicité de A_n (où $n \geq 5$) qui figure dans *Basic Algebra* I de N. Jacobson. Ce résultat repose sur deux lemmes, qui peuvent être admis lors du développement, mais dont il est évidemment recommandé de connaître les démonstrations.

Lemme. *Pour tout entier n, le groupe A_n est engendré par les 3-cycles.*

Démonstration. Tout élément de A_n est produit d'un nombre pair de transpositions. Il suffit donc de vérifier que tout produit de deux transpositions appartient au groupe engendré par les 3-cycles. Si ces deux transpositions sont égales, c'est évident (leur produit est alors l'identité) ; si leurs supports ont exactement un point commun, leur produit est de la forme $(ab)(bc) = (abc)$, et c'est donc un 3-cycle ; si leurs supports sont disjoints, leur produit est de la forme $(ab)(cd) = (abc)(bcd)$, qui est le produit de deux 3-cycles. $\square$

Lemme. *Pour tout entier $n \geq 5$, deux 3-cycles quelconques de A_n sont toujours conjugués dans A_n.*

Démonstration. Soient (abc) et $(\alpha\beta\gamma)$ deux 3-cycles de A_n. Soit σ une permutation quelconque de $\{1, \ldots, n\}$ envoyant a sur α, b sur β et c sur γ. On a $\sigma(abc)\sigma^{-1} = (\alpha\beta\gamma)$. Si σ est paire, le lemme est démontré. Si elle est impaire, soit τ une transposition portant sur deux éléments du complémentaire de $\{\alpha, \beta, \gamma\}$ (l'existence d'au moins deux éléments dans le complémentaire en question est assurée par l'hypothèse que $n \geq 5$). Comme τ fixe α, β et γ l'on a $(\tau\sigma)(abc)(\tau\sigma)^{-1} = (\alpha\beta\gamma)$, et $\tau\sigma$ est par ailleurs paire, ce qui achève la démonstration du lemme. $\square$

Corollaire. *Supposons $n \geq 5$, et soit G un sous-groupe distingué de A_n contenant un 3-cycle ; le groupe G est égal à A_n.*

Démonstration. Comme G contient un 3-cycle et est distingué, il contient tous les conjugués de ce 3-cycle, c'est-à-dire tous les 3-cycles d'après le lemme ci-dessus. Comme les 3-cycles engendrent A_n en vertu du premier lemme, G est égal à A_n. $\square$

Venons-en au théorème proprement dit.

Théorème. *Soit n un entier au moins égal à 5. Le groupe A_n est simple.*

Démonstration. Soit G un sous-groupe distingué de A_n. On suppose que G n'est pas réduit à $\{\mathsf{Id}\}$; on va montrer qu'il contient un 3-cycle ce qui assurera, au vu du corollaire précédent, que $G = A_n$.

Par hypothèse, l'ensemble des éléments de G différents de Id est non vide ; parmi ceux-ci, choisissons-en un, noté σ, ayant le plus grand nombre possible de points fixes ; on note N ce nombre. Le but est maintenant de montrer que σ est un 3-cycle.

On raisonne sur la décomposition de σ en produit de cycles à supports disjoints.

- Si les cycles de la décomposition de σ sont tous des transpositions, il y en a au moins 2 (car σ est paire et différente de l'identité) ; on peut donc, quitte à renuméroter les éléments de $\{1, \ldots, n\}$, supposer que σ s'écrit $(12)(34)...$, les points de suspension désignant des produits de cycles à support disjoint de $\{1, 2, 3, 4\}$. Posons $\tau = (345)$ (c'est possible car $n \geq 5$). On a alors $\tau\sigma\tau^{-1} = (12)(45)...$. Posons $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$; c'est un élément de G, puisque G est un sous-groupe distingué de A_n ; il est différent de Id, puisque $\tau\sigma\tau^{-1} \neq \sigma$; il fixe 1 et 2 (faire le calcul !) ainsi que tout élément de $\{1, \ldots, n\}$ strictement supérieur à 5 et fixé par σ. Comme σ ne fixe ni 1, ni 2, ni 3, ni 4, le nombre de points fixes de ρ vaut au moins $N + 2$ si 5 n'est pas fixé par σ, et au moins $N + 1$ dans la situation contraire ; dans tous les cas, ρ est un élément de G différent de Id qui possède au moins $N + 1$ points fixes, ce qui contredit la maximalité de N.

- S'il y a au moins un cycle de la décomposition de σ qui n'est pas une transposition, et si σ n'est pas un 3-cycle, on peut alors, quitte là encore à renuméroter, écrire $\sigma = (123...)....$ Il y a au moins deux éléments appartenant au complémentaire de $\{1, 2, 3\}$ (que l'on peut toujours, en modifiant à nouveau la numérotation, supposer être 4 et 5) qui ne sont pas fixés par σ : c'est en effet évident s'il y a un second cycle dans la décomposition ; et s'il n'y en a qu'un, qui est donc celui commençant par $(123...)$, c'est évident également, car ce cycle est de longueur strictement supérieure à 3 (puisque par hypothèse σ n'est pas un 3-cycle), et donc strictement supérieure à 4 (puisqu'un 4-cycle est impair).

  Posons $\tau = (345)$. On a alors $\tau\sigma\tau^{-1} = (124...)...$. Posons $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$; c'est un élément de G, puisque G est un sous-groupe distingué de A_n ; il est différent de Id, puisque $\tau\sigma\tau^{-1} \neq \sigma$; il fixe 2 (faire le calcul !) ainsi que tout élément de $\{1, \ldots, n\}$ strictement supérieur à 5 et fixé par σ. Comme σ ne fixe ni 1, ni 2, ni 3, ni 4, ni 5, le nombre de points fixes de ρ vaut au moins $N + 1$. Ainsi, ρ est un élément de G différent de Id qui possède au moins $N + 1$ points fixes, ce qui contredit la maximalité de N.

- Il reste donc une seule possibilité : σ est un 3-cycle. $\square$