Simplicité du groupe alterné

Leçons concernées

* **103 :** Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.
* **104 :** Groupes abéliens et non abéliens finis. Exemples et applications.
* **105 :** Groupe des permutations d'un ensemble fini. Applications.
* **108 :** Exemples de parties génératrices d'un groupe. Applications.

Réference

* *Rombaldi - Algèbre et géométrie*

Nous allons démontrer que si $n \neq 5$, alors le groupe alterné A_n est simple.
Commeçons par un lemme fondamental :

Lemme. *Le groupe A_n est engendré par les 3-cycles. De plus, les 3-cycles sont conjugués dans A_n.*

Démonstration. Soit $\sigma \in A_n$. En utilisant la décomposition en produit de cycles à support disjoint, on écrit $\sigma = \tau_1\tau_2...\tau_{2k-1}\tau_{2k}$ 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 transposition $\tau_1\tau_2$ (qui est bien un élément de A_n) est produit de 3-cycles.

On distingue alors plusieurs cas :
Si $\tau_1\tau_2 = (ab)(ab) = id$, alors l'identité est bien sûr produit de 3-cycles.
Si $\tau_1\tau_2 = (ab)(bc)$, alors $\tau_1\tau_2 = (abc)$ d'où le résultat.
Si $\tau_1\tau_2 = (ab)(cd)$ avec a, b, c, d 2 à 2 distincts. On remarque alors qu'on a l'égalité $\tau_1\tau_2 = (cad)(abc)$ (écrivez d'abord (abc) et cherchez en fonction le premier 3-cycle à trouver pour que ça marche).

Dans tous les cas, la première partie du lemme est démontrée.
Pour la deuxième partie, prenons (abc) et $(a'b'c')$ deux 3-cycles. On sait qu'ils sont conjugués dans S_n (car de même type) : il existe $\sigma \in S_n$ tel que $(abc) = \sigma(a'b'c')\sigma^{-1} = (\sigma(a')\sigma(b')\sigma(c'))$. Si $\sigma \in A_n$, il n'y a rien à faire. Sinon, puisque $n \geq 5$, on peut prendre i, j distincts de a', b', c'. Soit alors $\tau = (ij)$. Alors $(abc) = (\sigma\tau(a')\sigma\tau(b')\sigma\tau(c')) = \sigma\tau(a'b'c')(\sigma\tau)^{-1}$ et $\sigma\tau \in A_n$.
Dans tous les cas, (abc) et $(a'b'c')$ sont conjugués dans A_n.

□

Ceci nous permet alors de démontrer le théorème phare de ce développement :

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

Démonstration. Prenons H un sous-groupe distingué de A_n non trivial. Nous allons alors montrer que $H = A_n$. Pour ce faire, nous allons utiliser notre lemme : on a vu que les 3-cycles engendraient A_n. Donc il suffit de montrer que tous les 3-cycles sont dans H. Or, les 3-cycles sont conjugués dans A_n, et H est stable par conjugaison, puisqu'il est distingué dans A_n.
Nous allons alors montrer qu'il existe un 3-cycle dans H, et cela suffira pour montrer le théorème.

Il existe alors $\sigma \in H$ qui admet un point a tel que la quantité $b = \sigma(a)$ vérifie $b \neq a$. Prenons c tel que $c \neq a, b, \sigma(b)$, qui existe puisque $n \geq 5$. Considérons $\gamma = \sigma(abc)\sigma^{-1}(abc)^{-1}$. Que dire sur cette permutation ?
Premièrement, $\gamma \in H$. En effet, $(abc)\sigma^{-1}(abc)^{-1}$ est le conjugué dans A_n d'un élément de H, donc est dans H. Ainsi, $\gamma \in H$.
Mais on peut aussi calculer explicitement γ : $\gamma = (\sigma(a)\sigma(b)\sigma(c))(acb) = (b\sigma(b)\sigma(c))(acb)$.

Nous avons alors trouvé un élément γ de H qui admet, dans son support, au plus 5 éléments. Nous allons alors discuter en fonction du type de γ (avec 5 éléments, dans A_n, cela donne peu de possibilités), et déduire un 3-cycle dans H dans chacun des cas.

— $1, 1, 1, 1, 1$: Dans ce cas, $\gamma = id$ ce qui signifie que σ et (abc) commutent, ce qui est absurde car $\sigma(abc)(a) = \sigma(b)$ et $(abc)\sigma(a) = c \neq \sigma(b)$ par hypothèse. Ce cas-ci est donc impossible.
— $3, 1, 1$: Dans ce cas, γ est un 3-cycle dans H.
— $2, 2, 1$: On écrit $\gamma = (ij)(kl)$. Prenons un élément $u \neq i, j, k, l$ et faisons la même combinaison que tout à l'heure : on regarde $\gamma' = \gamma(iju)\gamma^{-1}(iju)^{-1}$ qui est un élément de H. Décrivons-le : $\gamma' = (\gamma(i)\gamma(j)\gamma(u))(iuj) = (jiu)(iuj) = (iju) \in H$.
— 5 : On écrit $\gamma = (ijklu)$. Regardons $\gamma' = \gamma(ijk)\gamma^{-1}(ijk)^{-1} \in H$. Alors $\gamma' = (jkl)(ikj) = (ilj)$.

Dans tous les cas, on a donc bien trouvé un 3-cycle dans H, et donc par la remarque du début de la preuve $H = A_n$ ce qui prouve la simplicité de A_n.

□

Remarques :
— Qu'en est-il du cas $n < 5$? Les groupes A_1 et A_2 sont triviaux, donc simples. A_3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ qui est simple aussi. Concernant A_4, un exercice classique est de prouver que $D = \{id; (12)(34); (13)(24); (14)(23)\}$ est un sous-groupe qui est distingué dans A_n (car en particulier distingué dans S_n). Donc en fait, tous les groupes A_n sont simples, sauf pour le cas $n = 4$.
— Ce résultat de simplicité est un théorème très, très fondamental en théorie de Galois. En effet, il permet de dire que le groupe S_n est résoluble si et seulement si $n \leq 4$. En effet, dans le cas $n \geq 5$, la suite $\{1\} \lhd A_n \lhd S_n$ est une suite de Jordan-Hölder (les quotients successifs sont des groupes simples). Or, un groupe fini est résoluble si et seulement si pour toute suite de Jordan-Hölder, les quotients sont d'ordre premiers. Mais A_n n'est pas d'ordre premier pour $n \geq 5$ ce qui prouve que S_n n'est pas résoluble pour $n \geq 5$. Pour $n = 1, 2, 3$ c'est une vérification directe. Pour $n = 4$, la suite $\{1\} \lhd D \lhd A_n \lhd S_n$ est une suite de Jordan-Hölder qui réponds bien aux attentes pour que S_4 soit résoluble.
En conséquence, les équations polynomiales de degré supérieur à 5 ne sont pas résolubles par radicaux, car l'extension de corps associé a un groupe de Galois isomorphe à S_n qui n'est pas résoluble.