Développement : Le groupe alterné est simple pour n>=5

On note ε la fonction signature. $\mathfrak{S}_n$ le groupe symétrique et $\mathfrak{A}_n$ le groupe alterné.

1. **Lemme 1.** — Si $n \geq 4$ les 3-cycles engendrent $\mathfrak{A}_n$
   - Notons H le sous-groupe engendré par les 3-cycles.
   - Les 3-cycles sont dans $\mathfrak{A}_n$ (signature $(-1)^2$). Donc $H \subset \mathfrak{A}_n$.
   - Les transpositions engendrent $\mathfrak{S}_n$ donc $\forall \sigma \in \mathfrak{A}_n$, $\exists(\sigma_i)\ Pi_i\sigma_i = \sigma$. On impose (sans perte de généralité) aux σ_i de ne pas être l'identité.
   - Les σ_i sont en nombre pair puisque $\varepsilon(Pi_i\sigma_i) = 1$: groupons les par deux.
   - On a donc que $\mathfrak{A}_n \subset K$ où K désigne le sous-groupe de $\mathfrak{S}_n$ engendré par les permutations produit de deux transpositions.
   - Montrons que si τ_{ij} et τ_{kl} sont deux transpositions permutant l'une i et j et l'autre k et l, elles s'expriment en termes de 3-cycles. On sait que $i \neq j$ et $k \neq l$.
     - Cas où i, j, k, l sont tous différents : $\tau_{ij}\tau_{kl} = \tau_{ij}\tau_{jk}\tau_{jk}\tau_{kl} = (ijk)(jkl)$ et donc c'est le produit de deux 3-cycles.
     - Cas où les paires $\{i, j\}$ et $\{k, l\}$ partagent une valeur et une seule, disons $j = k$. Alors $\tau_{ij}\tau_{kl} = \tau_{ij}\tau_{jl} = (ijl)$ qui est un 3-cycles.
     - CQFD

2. **Lemme 2.** — Si $n \geq 4$ les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
   - Mq (123) et (ijk) sont conjugués dans $\mathfrak{A}_n$. Alors, par transitivité, ils le seront tous.
   - On prend l, s différents de i, j, k et on considère σ : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ i & j & k & l & s & \cdots & \end{pmatrix}$
   - σ ou $\sigma' = \sigma(ls)$ est paire et appartiennent à $\mathfrak{A}_n$.
   - Or $\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (ijk)$ et de même pour σ'.
   - CQFD.

3. **Le Théorème lui-même.** — "Si $n \geq 5$ le groupe alterné est simple".
   - On raisonne par l'absurde et on considère H un *sous-groupe propre et distingué* de $\mathfrak{A}_n$.
   - On considère $\sigma \in H$ différent de Id et on considère son unique décomposition en cycles à supports disjoints $\sigma = \Pi_{k \in I}\ \sigma_k$.
   - Cas 1 : Il existe au moins un k-cycle parmi les (σ_i) avec $k \geq 4$.
     - Avec un choix adéquat de numérotation nous pouvons considérer que $\sigma_1 = (a_1, a_2, \cdots, a_k)$.
     - Considérons $\nu = (a_1a_2a_3)$ et son inverse $\nu^{-1} = (a_1a_3a_2)$. Ils sont dans $\mathfrak{A}_n$.
     - Considérons $C = \sigma^{-1}\nu^{-1}\sigma\nu$ qui est le commutateur de $[\sigma, \nu]$.
     - C est dans H car $C = \sigma^{-1}(\nu^{-1}\sigma\nu)$. Or, le terme entre parenthèses est dans H qui est normal ainsi que σ^{-1} et donc, comme H est un groupe, $C \in H$.
     - Or, en faisant le calcul on obtient $C = (a_2a_3a_k)$. (notons que ν commute avec tous les σ_i autres que σ_1).
     - Alors, d'après le lemme 2, H contient un générateur de $\mathfrak{A}_n$ et le contient, ce qui contredit notre hypothèse.
     - Conc : le Cas 1 est impossible.
   - Rem : on vient de prouver au passage que H ne peut contenir aucun k-cycle avec $k \geq 4$, car sinon il serait présent dans sa propre décomposition et le Cas 1 ne serait pas vide.
   - Cas 2 : Il existe uniquement des 3-cycles parmi les (σ_s).
     - Il ne peut n'y en avoir qu'un car là encore nous engendrerions alors $\mathfrak{A}_n$ en entier.
     - Si on en a deux correspondant à $\sigma_1 = (iju)$ et $\sigma_2 = (klv)$ on opère comme dans le cas 1 en construisant le commutateur avec le 3-cycle (ijk) qui est dans $\mathfrak{A}_n$.
     - Ici $C = \sigma^{-1}\nu^{-1}\sigma\nu = (\Pi_{s\neq 1,2}\sigma_s)^{-1}\sigma_2\sigma_1(ikj)\sigma_1\sigma_2(\Pi_{s\neq 1,2}\sigma_s)(ijk) = (ikjul)$.
     - D'après la remarque ci-dessus, ceci est encore impossible.
     - Concl : le Cas 2 est impossible.
   - Cas 3 : Il existe un unique 2-cycle et quelques 3-cycles parmi les (σ_s).
     - Un simple raisonnement de parité invalide un tel scénario car σ doit être paire.
     - Concl : le Cas 3 est impossible.
   - Cas 4 : Il existe au moins deux transpositions parmi les (σ_s).
     - On les note : $\sigma_1 = (ij)$ et $\sigma_2 = (kl)$.
     - Notons φ tel que $\sigma = (ij)(kl)\sigma$.
     - En considérant encore le commutateur on a $C = \sigma^{-1}\nu^{-1}\sigma\nu = (\Pi_{s\neq 1,2}\sigma_s)^{-1}\sigma_2\sigma_1(ikj)$ $(\Pi_{s\neq 1,2}\sigma_s)^{-1}(kl)(ij)(ikj)(ij)(kl)(ijk)(\Pi_{s\neq 1,2}\sigma_s) = (il)(jk)$.
     - On a donc $(il)(jk) \in H$.
     - Or, en considérant un élément $s \notin \{i, j; k; l\}$, ce qui est possible lorsque $n \geq 5$, on pose $\beta = (kls)$.
     - Alors, si on considère $C' = \beta{-}1\sigma\beta\sigma{-}1$, on remarque que $\mathbb{C}' = \beta$.
     - Or, $C' \in H$, donc $\beta \in H$ mais β est un 3-cycle et H posséderait un générateur de $\mathfrak{A}_n$ ce qui ne peut être.
     - Concl : le Cas 4 est impossible.
   - Tous les cas sont vides ce qui rend absurde l'hypothèse faite sur le caractère propre du sous-groupe H.
   - CQFD

4. **Corollaire 1.** — "Si $n \geq 5$ les seuls sous-groupes distingués/normaux du groupe symétrique $\mathfrak{S}_n$ sont lui-même, $\{1\}$ et le groupe alterné".
   - Supposons qu'il existe H sous-groupe *propre* et distingué dans $\mathfrak{S}_n$.
   - Si $B = H \cap \mathfrak{A}_n \neq \{1\}$:
     - comme B est un sous-groupe distingué de $\mathfrak{A}_n$ qui est simple, $B = \mathfrak{A}_n$.
     - Donc $\mathfrak{A}_n \in H$.
     - Mais comme l'indice de $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$ et que l'indice $[H : \mathfrak{A}_n]$ le divise,
     - $[H : \mathfrak{A}_n] \in \{1, 2\}$

    - Donc soit $H = \mathfrak{A}_n$, soit $H = \mathfrak{S}_n$.
  - Si $B = H \cap \mathfrak{A}_n = \{1\}$:
    - Cela veut dire que la seule permutation paire de H est 1.
    - Or, dès que H a plus de 4 éléments, on peut trouver a et b tels que a, b et ab ne sont ps 1 alors que un au moins des 3 a une signature paire.
    - on a nécessairement $H = \{1\}$ ou $H = \{1, a, b\}$.
    - Dans ce deuxième cas, comme $ab = 1$, $a^2 = b$ et b a une signature paire ce qui est impossible.

5. Corollaire 2. — "Si $n \geq 5$ $D(\mathfrak{A}_n) = \mathfrak{A}_n$"
- Si σ est un 3-cycle σ^2 l'est aussi.
- Or, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
- $\exists \nu \in \mathfrak{A}_n$ tel que $\sigma^2 = \nu\sigma\nu{-}1$.
- Le commutateur $\sigma{-}1\nu\sigma\nu{-}1 = \sigma^4 = \sigma$ est dans $D(\mathfrak{A}_n)$ par définition du groupe dérivé.
- Donc $D(\mathfrak{A}_n)$ contient tous les 3-cycles qui engendrent $\mathfrak{A}_n$ ce qui achève la démonstration.

6. Leçons. —
- 103. Sous-groupes distingués
- 105. Groupe symétrique
- 108. Exemples des génératrices d'un groupe

)

7. Sources : —
- D-J. Mercier 'Fondamentaux d'Algèbre et d'Arithmétique'
- D. Perrin "Cours d'Algèbre"

January 12, 2018

Bruno Nitrosso, EPP et candidat libre