Simplicité du groupe alterné

Arnaud Girand

5 juillet 2012

Référence :
- [Per96], p. 28–29

Prérequis :
- théorèmes de Sylow.

Proposition 1
Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Démonstration : Traitons premièrement le cas $n = 5$, en commençant par passer en revue les éléments de $\mathfrak{A}_5$. Ce groupe, de cardinal 60, contient :
- un élément d'ordre 1. Vous l'aurez deviné, il s'agit du neutre $()$ ...
- des produits de deux transpositions à supports disjoints, qui sont d'ordre 2. On dispose de $C_5^2 = 10$ possibilités pour la première et de $C_3^2 = 3$ possibilités pour sa collègue, pour un total de 30 choix possible, en tenant compte de l'ordre dans lequel on compose. Nos permutations étant à support disjoints, elles commutent donc il n'en reste que 15 qui soient distinctes.
- des 3–cycles (rappelons qu'un cycle d'ordre k est de signature $(-1)^k$). Le choix de 3 éléments distincts i, j, k de $[5]$ nous livre deux 3–cycles distincts $(i \quad j \quad k)$ et $(i \quad k \quad j)$, ergo $\mathfrak{A}_5$ accueille $2 \times C_5^3 = 20$ 3–cycles en son sein.
- des 5–cycles. Notons que si on se donne $i, j, k, l, m \in [5]$ deux à deux distincts alors les cycles suivants sont égaux : $(i \quad j \quad k \quad l \quad m)$, $(m \quad i \quad j \quad k \quad l)$, $(l \quad m \quad i \quad j \quad k)$, $(k \quad l \quad m \quad i \quad j)$ et $(j \quad k \quad l \quad m \quad i)$, ainsi $\mathfrak{A}_5$ contient $\frac{5!}{5} = 24$ 5–cycles distincts.

Comme $60 = 1 + 15 + 20 + 24$, on a bien décrit le groupe $\mathfrak{A}_5$.

Soit $H \lhd \mathfrak{A}_5$ non trivial. Remarquons que comme les 3–cycles (resp. les produits de deux transpositions à supports disjoints) sont tous conjugués dans $\mathfrak{A}_5$, si H contient un élément d'ordre 3 (resp. 2), il les contient tous. De plus, si H contient un 5–cycle σ, il contient $\langle\sigma\rangle$, qui est un 5–Sylow de $\mathfrak{A}_5$. Ces derniers étant tous conjugués [1], H contient alors tous les éléments d'ordre 5 de $\mathfrak{A}_5$. Cependant, aucun des entiers $15 + 1$, $20 + 1$ et $24 + 1$ ne divise 60 donc H doit être dans au moins deux des cas précédents et donc $|H| \geq 15 + 20 + 1 = 36|$, ce qui implique –toujours car $|H||60$ – que $|H| = 60$ et donc $H = \mathfrak{A}_5$. On a bien démontré la simplicité de $\mathfrak{A}_5$.

Supposons à présent $n > 5$ et donnons nous $H \lhd \mathfrak{A}_n$ non trivial et $\sigma \in H \setminus \{()\}$. Il existe alors $a \in [n]$ tel que $b := \sigma(a) \neq a$. Donnons nous également $c \notin \{a, b, \sigma(b)\}$ et posons $\tau := (a \quad c \quad b)$ et $\rho := [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$. On a alors [2] :

$$\rho = (a \quad c \quad \underbrace{b}_{=\sigma(a)})(\sigma(a) \quad \sigma(b) \quad \sigma(c))$$

ρ agit donc sur au plus 5 éléments, ceux de l'ensemble $E := \{a, b, c, \sigma(b), \sigma(c)\}$, i.e on a $\rho(E) = E$ et $\rho_{|_{[n]\setminus E}} = \mathrm{id}_{[n]\setminus E}$. Quitte à rajouter des éléments inutiles, on peut supposer que $|E| = 5$ et comme $\rho(b) = \tau\sigma(b) \neq b$ (car $\tau^{-1}(b) = c \neq \sigma(b)$, $\rho_{|_E} \neq \mathrm{id_E}$.

L'ensemble $\mathfrak{A}$ des permutations paires de E est alors isomorphe à $\mathfrak{A}_5$ et on dispose de l'injection suivante :

$$\begin{aligned} &\mathfrak{A} \hookrightarrow \mathfrak{A}_n \\ &u \mapsto \overline{u} : x \mapsto \begin{cases} u(x) & \text{si } \ x \in E \\ x & \text{sinon} \end{cases} \end{aligned}$$

1. Attention cependant, tous les éléments d'ordre 5 de $\mathfrak{A}_5$ ne sont pas conjugués, car sinon l'orbite d'un 5–cycle pour l'action de $\mathfrak{A}_5$ sur lui–même par conjugaison serait d'ordre $24 \nmid 60$.
2. Pour les calculs explicites, remarquer que $\rho = \tau\nu$ où ν est le conjugué de τ par σ.

Posons alors (quitte à identifier) :

$$H_0 := \{u \in \mathfrak{A} \,|\, \overline{u} \in H\} = "H \cap \mathfrak{A}"$$

Remarquons alors que $H_0 \lhd \mathfrak{A} \cong \mathfrak{A}_5$ et que $\rho_{|E}$ est un élément non trivial de H_0. Ergo, par simplicité de $\mathfrak{A}_5$, $H_0 = \mathfrak{A}$.

Soit $u \in \mathfrak{A}$ un 3–cycle. Alors $\overline{u}$ est un 3–cycle de $\mathfrak{A}_n$ (l'injection $\mathfrak{A} \hookrightarrow \mathfrak{A}_n$ conservant le cardinal du support). Comme tous les 3–cycles sont conjugués dans $\mathfrak{A}_n$, H contient tous les 3–cycles. On conclut que $H = \mathfrak{A}_n$ en remarquant que le groupe alterné est engendré par les 3–cycles.

Détails supplémentaires :

- *$\mathfrak{A}_n$ est engendré par les 3–cycles.* Comme $\mathfrak{S}_n$ est engendré par les transpositions, $\mathfrak{A}_n$ est engendré par les produits de deux transpositions. On a de plus les relations suivantes :

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

  In fine :

  $$(a \quad b)(c \quad d) = (a \quad c \quad b)(a \quad c \quad d)$$

  D'où le résultat ([Per96], p.11).
- *Les 3–cycles sont conjugués dans $\mathfrak{A}_n$ ($n \geq 5$).* Ceci découle du résultat suivant ([Per96], p.16) :

  Lemme 1
  Soit $n \geq 3$.
  Soient $a_1, \ldots, a_n \in [n]$ deux à deux distincts.
  Soient $b_1, \ldots, b_n \in [n]$ deux à deux distincts.
  Alors il existe $\sigma \in \mathfrak{A}_n$ telle que $\forall i \in [n-2]$, $\sigma(a_i) = b_i$.
  Démonstration : On sait qu'il existe une telle permutation σ dans $\mathfrak{S}_n$. Si $\varepsilon(\sigma) = 1$, c'est terminé, sinon on compose par $(a_{n-1} \quad a_n)$ et on obtient une permutation paire adéquate.

  Ainsi, si $\rho = (a_1 \quad a_2 \quad a_3)$ et $\tau = (b_1 \quad b_2 \quad b_3)$ sont dans $\mathfrak{A}_n$, comme $n - 2 \geq 3$ il existe une permutation $\sigma \in \mathfrak{A}_n$ telle que $\forall i \in [3]$, $\sigma(a_i) = b_i$ et donc $\tau = \sigma\rho\sigma^{-1}$.
- *Les produits de deux permutations de supports disjoints sont conjugués dans $\mathfrak{A}_n$ ($n \geq 5$).* Si $n > 5$ cela découle immédiatement du lemme 1. Si $n = 5$, soient $\rho := (a \quad b)(c \quad d)(e)$ et $\tau := (a' \quad b')(c' \quad d')(e')$. D'après le lemme 1, il existe $\sigma \in \mathfrak{A}_5$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$. On a alors $\tau = \sigma\rho\sigma^{-1}$.
- *Simplicité pour $n \geq 4$.* $\mathfrak{A}_2 = \{()\}$ et $\mathfrak{A}_3 = \{(), (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)$ sont simples. $\mathfrak{A}_4$ n'est pas simple car il admet le sous–groupe distingué suivant :

  $$H := \{(), (1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2 \quad 3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Références

[Per96] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.