15 Simplicité de $\mathfrak{A}_n$

Leçons 101, 103, 104, 105, 108

Ref : [Perrin] Prop I.4.10, Th I.8.1

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

Démonstration. Étape 1. Conjugaison des 3*-cycles dans* $\mathfrak{A}_n$*.*

La première étape de cette démonstration repose sur le lemme suivant, qui décrit l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$.

Lemme 2 Pour $n \geq 3$, l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est $n-2$-transitive.

Démonstration. On se donne deux familles d'éléments deux à deux distincts de $[\![1, n]\!]$, notées $(a_1, .., a_{n-2})$ et $(b_1, .., b_{n-2})$. On doit montrer qu'il existe un élément σ de $\mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq n-2$. On commence par noter a_{n-1} et a_n (resp. b_{n-1} et b_n) les deux éléments de $[\![1, n]\!]$ qui ne sont pas dans la famille $(a_i)_{1 \leq i \leq n-2}$ (resp. $(b_i)_{1 \leq i \leq n-2}$), puis on se donne une permutation $\sigma \in \mathfrak{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq n$ (σ existe car l'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est n-transitive). Si σ est paire, alors $\sigma \in \mathfrak{A}_n$ convient. Sinon, la permutation $\sigma(a_{n-1}\ a_n) \in \mathfrak{A}_n$ convient. □

On déduit de ce lemme que pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$: en effet, si l'on se donne deux cycles $(a_1\ a_2\ a_3)$ et $(b_1\ b_2\ b_3)$, puisque $n - 2 \geq 3$, l'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est 3-transitive, et donc il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $1 \leq i \leq 3$. Ainsi, on a

$$(b_1\ b_2\ b_3) = \sigma(a_1\ a_2\ a_3)\sigma^{-1}.$$

Étape 2. Simplicité de $\mathfrak{A}_5$*.*

Le même raisonnement permet de montrer que les bitranspositions $(a_1\ a_4)(a_2\ a_5)(a_3)$ et $(b_1\ b_4)(b_2\ b_5)(b_3)$ sont conjuguées dans $\mathfrak{A}_5$.

On se donne maintenant un sous-groupe distingué $H \lhd \mathfrak{A}_5$ différent de $\{\mathrm{id}\}$. Commençons par lister les 60 éléments de $\mathfrak{A}_5$:

- l'identité
- les éléments d'ordre 2 sont les bitranspositions, il y en a 15
- les éléments d'ordre 3 sont les 3-cycles, il y en a 20
- les éléments d'ordre 5 sont les 5-cycles, il y en a 24

Si H contient les éléments d'ordre 2 (resp. 3), il les contient tous d'après ce qui précède (resp. d'après l'étape 1). De plus, si H contient un 5-cycle, il contient le sous-groupe qu'il engendre, qui est un 5-Sylow de $\mathfrak{A}_5$. Comme les 5-Sylows sont conjugués, il les contient tous, et donc il contient tous les 5-cycles. Comme H n'est pas réduit au neutre, il contient au moins un de ces trois types d'éléments. Comme $1 + 15, 1 + 20$ et $1 + 24$ ne divisent pas 60, H ne peut pas contenir un seul de ces trois types d'éléments. Ainsi, son cardinal est au moins $1 + 15 + 20 = 36$, mais comme il divise 60, il est égal à 60. Donc $H = \mathfrak{A}_5$. On en déduit bien que $\mathfrak{A}_5$ est simple.

Étape 3. Simplicité de $\mathfrak{A}_n$*.*

On se donne cette fois un sous-groupe distingué $H \lhd \mathfrak{A}_n$ différent de $\{\mathrm{id}\}$, et on prend $\sigma \in H$ non trivial. On va se ramener au cas de l'étape 2 en fabriquant à partir de σ un élément de H agissant sur $[\![1, 5]\!]$ (i.e. ayant $n - 5$ points fixes).

Comme σ n'est pas l'identité, il existe un élément $a \in [\![1, n]\!]$ tel que $\sigma(a) = b \neq a$. On se donne $c \in [\![1, n]\!] \backslash \{a, b, \sigma(b)\}$ (possible car $n > 3$). On note alors τ le 3-cycle $(a\ c\ b)$ (c'en est un puisque a, b et c sont distincts), et $\rho = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c))$. Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ possède au plus 5 éléments, et on suppose quitte à en rajouter qu'il y en a exactement 5. Alors les $n-5$ éléments qui ne sont pas dans F sont des points fixes de ρ. De plus,

$$\rho(b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(b) \neq b$$

car $\tau^{-1}(b) = c \neq \sigma(b)$. Donc ρ n'est pas l'identité. Comme F possède 5 éléments, l'ensemble $\mathfrak{A}(F)$ de ses permutations paires est isomorphe à $\mathfrak{A}_5$, et il s'injecte bien sûr dans $\mathfrak{A}_n$ par extension en l'identité sur $[\![1, n]\!]\backslash F$ d'un élément de $\mathfrak{A}(F)$ (l'identité est de signature 1). On pose alors $H_F = H \cap \mathfrak{A}(F)$ [1]. Bien sûr, H_F est distingué dans $\mathfrak{A}(F)$, et ρ est un élément non trivial de H_F. On en déduit, comme $\mathfrak{A}(F)$ est simple (car isomorphe à $\mathfrak{A}_5$), que $H_F = \mathfrak{A}_F$. Ainsi, H_F contient les 3-cycles de $\mathfrak{A}(F)$, et donc H contient leur prolongements, qui sont des 3-cycles de $\mathfrak{A}_n$. Mais comme les 3-cycles sont conjugués, H les contient tous. Or les 3-cycles engendrent $\mathfrak{A}_n$, donc $H = \mathfrak{A}_n$. □

Remarque. Le cas des groupes alternés pour $n \leq 4$ est simple à résoudre :

- $\mathfrak{A}_2$ est le groupe trivial
- $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est cyclique d'ordre premier, donc simple
- Le groupe dérivé de $\mathfrak{A}_4$ est le groupe de Klein V_4, qui est non trivial, donc $\mathfrak{A}_4$ n'est pas simple

1. Ici, on identifie les éléments de $\mathfrak{A}(F)$ avec leur prolongement comme éléments de $\mathfrak{A}_n$.