Simplicité de $\mathcal{A}_n$ pour $n \geq 5$

Références : [Per96] p.28-29 ([Gou94] et [Mé06]).

Théorème 0.1 *Le groupe alterné $\mathcal{A}_n$ est simple pour $n \geq 5$.*

Rappels : $\mathcal{A}_n$ est défini comme étant le noyau du morphisme de groupe surjectif défini par la signature $\epsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$, dont le noyau est formé des permutations paires (ie de signature 1). De plus, on dit qu'un groupe est simple, si ses sous-groupes distingués sont triviaux.

Démonstration

Étape 1 $n = 5$.

Étudions les éléments de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ admet $\dfrac{5!}{2} = 60$ éléments. Déterminons ces éléments :

- un élément d'ordre 1 : l'identité, ie $(a)(b)(c)(d)(e)$, avec a, b, c, d, e distincts.
- 15 éléments d'ordre 2, qui sont les produits de transpositions, ie $(a\,b)(c\,d)$ avec a, b, c, d distincts deux à deux.
  Les produits de transpositions sont d'ordre 2 car $(a\,b)(c\,d)(a\,b)(c\,d) = (a\,b)(a\,b)(c\,d)(c\,d) = (a)(b)(c)(d)$.
  Les produits de transpositions sont dans $\mathcal{A}_5$ car $\epsilon((a\,b)) = -1$ d'où $\epsilon((a\,b)(c\,d)) = \epsilon((a\,b))\epsilon((c\,d)) = 1$.
  Il y en a 15 car on choisit tout d'abord a, ie on a C_5^1 possibilités, ensuite on choisit b, ie C_4^1 possibilités, puis c, ie on a C_3^1 possibilités et enfin on a C_2^1 possibilités pour choisir d, d'où $5 \times 4 \times 3 \times 2 = 120$ possibilités pour le produit de transpositions. Cependant, on sait que $(a\,b)(c\,d) = (c\,d)(a\,b)$, donc il reste 60 possibilités, ensuite $(a\,b)(c\,d) = (b\,a)(c\,d)$ donc il reste 30 possibilités et enfin $(a\,b)(c\,d) = (b\,a)(d\,c)$ donc au final on a 15 possibilités.
- 20 éléments d'ordre 3, qui sont les 3-cycles, ie $(a\,b\,c)$ avec a, b, c distincts deux à deux.
  Les 3-cycles sont bien d'ordre 3 car $(a\,b\,c)(a\,b\,c) = (a\,c\,b)$ et $(a\,b\,c)(a\,c\,b) = (a)(b)(c)$.
  Les 3-cycles sont dans $\mathcal{A}_5$ car $\epsilon((a\,b\,c)) = (-1)^{3+1} = 1$.
  Il y en a 20, car on a C_5^1 possibilités pour choisir a, on a C_4^1 possibilités pour choisir b et C_3^1 possibilités pour choisir c, d'où $5 \times 4 \times 3 = 60$ possibilités pour les 3-cycles. Or $(a\,b\,c) = (b\,c\,a) = (c\,a\,b)$ d'où 20 possibilités.
- 24 éléments d'ordre 5, qui sont les 5-cycles, ie $(a\,b\,c\,d\,e)$ avec a, b, c, d, e distincts deux à deux.
  Les 5-cycles sont d'ordre 5 car $(a\,b\,c\,d\,e)(a\,b\,c\,d\,e) = (a\,c\,e\,b\,d)$, $(a\,b\,c\,d\,e)(a\,c\,e\,b\,d) = (a\,d\,b\,e\,c)$, $(a\,b\,c\,d\,e)(a\,d\,b\,e\,c) = (a\,e\,d\,c\,b)$, $(a\,b\,c\,d\,e)(a\,e\,d\,c\,b) = (a)(b)(c)(d)(e)$.
  Les 5-cycles sont dans $\mathcal{A}_5$ car $\epsilon((a\,b\,c\,d\,e)) = (-1)^{5+1} = 1$.
  Il y en a 24 car on a C_5^1 possibilités pour choisir a, C_4^1 possibilités pour choisir b, C_3^1 possibilités pour choisir c, C_2^1 possibilités pour choisir d et C_1^1 possibilités pour choisir e, d'où $5 \times 4 \times 3 \times 2 \times 1 = 120$ possibilités. Or $(a\,b\,c\,d\,e) = (b\,c\,d\,e\,a) = (c\,d\,e\,a\,b) = (d\,e\,a\,b\,c) = (e\,a\,b\,c\,d)$ d'où 24 possibilités.

On a bien trouvé de la sorte tous les éléments car $1 + 15 + 20 + 24 = 60 = |\mathcal{A}_5|$. On sait que les 3-cycles sont conjugués dans $\mathcal{A}_5$ et les produits de transpositions aussi.
Soit alors H un sous-groupe distingué de $\mathcal{A}_5$ tel que $H \neq \{1\}$. Alors si H contient un élément d'ordre 2, on sait qu'il les contient tous (car H distingué, ie les éléments de H sont conjugués dans $\mathcal{A}_5$), de même si H contient un élément d'ordre 3 alors il les contient tous.
De plus si H contient un élément d'ordre 5, il contient alors le 5-Sylow engendré par cet élément, donc tous les 5-Sylow puisqu'ils sont conjugués d'après le théorème de Sylow, donc tous les éléments d'ordre 5.
Or $15 + 1 = 16 \nmid 60$, $20 + 1 = 21 \nmid 60$ et $24 + 1 = 25 \nmid 60$, donc H contient au moins deux types d'éléments, ie il admet au moins $1 + 15 + 21 = 36$ éléments, or $36 \nmid 60$ et d'après le théorème de Lagrange le cardinal de H doit diviser celui de $\mathcal{A}_5$ d'où $H = \mathcal{A}_5$.

Étape 2 $n \geq 5$.

On pose $E = \{1, \ldots, n\}$.
Soit H un sous-groupe distingué de $\mathcal{A}_n$ et $H \neq \{1\}$.
Soit $\sigma \in H$ et $\sigma \neq 1$.
Le but est ici de se ramener au cas où $n = 5$ et pour ceci fabriquer à partir de σ un élément non trivial de H qui n'agisse en fait que sur un ensemble à 5 éléments, donc qui ait $n - 5$ points fixes.
Soit $\tau \in \mathcal{A}_n$.
On considère le commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$.
Comme $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$ et que H est distingué dans $\mathcal{A}_n$, alors $\forall \tau \in \mathcal{A}_n$, $\forall \sigma \in H$, $\tau\sigma\tau^{-1} \in H$, d'où comme $\sigma^{-1} \in H$ (car H groupe) alors $\rho \in H$.
Comme $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$, alors ρ est le produit de deux éléments du type de τ de sorte que si τ admet beaucoup de points fixes alors ρ aussi.
Plus précisément, comme $\sigma \neq 1$ alors $\exists a \in E$ tel que $\sigma(a) = b \neq a$.
Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$ (un tel élément existe car $n \geq 5$).
Soit τ le 3-cycle $\tau = (a\, c\, b)$, de tel sorte que $\tau^{-1} = (a\, b\, c)$ (en effet $\tau\tau^{-1} = (a\, c\, b)(a\, b\, c) = (a)(b)(c)$).
On considère $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\, c\, b)(\sigma(a)\, \sigma(b)\, \sigma(c))$.
Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et on a $\rho(F) = F$ et $\rho(E \setminus F) = id_{E \setminus F}$ (par définition de ρ puisque son support est F et ainsi cette permutation n'agit que sur son support et laisse fixe les autres éléments).
Quitte à rajouter au besoin des éléments à F, on peut supposer que $|F| = 5$.
On remarque que $\rho \neq 1$ car $\rho(b) = \tau\sigma(b) \neq b$ (en effet par l'absurde, si $\tau\sigma(b) = b$, alors en composant par τ^{-1}, $\sigma(b) = \tau^{-1}(b) = c$ et on a choisi $c \neq \sigma(b)$).
Soit alors $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Comme $|F| = 5$ alors $\mathcal{A}(F) \simeq \mathcal{A}_5$ et $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via l'application :

$$\begin{aligned} \mathcal{A}(F) &\hookrightarrow \mathcal{A}_n \\ u &\longmapsto \overline{u} \end{aligned}$$

où $\overline{u}_{|_F} = u$ et $\overline{u}_{|_{E \setminus F}} = id_{E \setminus F}$.
On pose $H_0 = \{u \in \mathcal{A}(F), \overline{u} \in H\} = H \cap \mathcal{A}(F)$. Alors H_0 est distingué dans $\mathcal{A}(F)$, $\rho_{|_F} \in H_0$ et $\rho_{|_F} \neq id_F$. En effet :

- $H_0 \subset \mathcal{A}(F)$ par définition. Soit $u \in H_0$, alors $u \in \mathcal{A}(F)$ et $\overline{u} \in H$. Soit $g \in \mathcal{A}(F)$. Alors $gug^{-1} \in \mathcal{A}(F)$ car $g, u \in \mathcal{A}(F)$ et $\overline{gug^{-1}} = \overline{g}\,\overline{u}\,\overline{g}^{-1}$ car le plongement est un morphisme de groupes, d'où $gug^{-1} \in H$ car H est distingué dans $\mathcal{A}_n$.
- $\rho \in \mathcal{A}(F)$ et $\rho \in H$ (on l'a montré précédemment), donc $\rho_{|_F} \in H$, d'où $\rho_{|_F} \in H_0$.
- $\rho(b) \neq b$ d'après ce qu'on a montré précédemment et $b \in F$ donc $\rho_{|_F} \neq id_F$.

Comme $\mathcal{A}(F) \simeq \mathcal{A}_5$ et que $\mathcal{A}_5$ est simple alors $H_0 = \mathcal{A}(F)$ (car on vient de montrer que $\rho_{|_F} \in H_0$ et $\rho_{|_F} \neq 1$).
Soit alors u un 3-cycle de $\mathcal{A}(F)$, alors $u \in H_0$ d'après ce qu'on vient de faire, donc $\overline{u} \in H$ (par définition de H_0) et est toujours un 3-cycle.
Or les 3-cycles sont conjugués dans $\mathcal{A}_n$ (pour $n \geq 5$) et $\overline{u}$ est un 3-cycle dans H donc tous les 3-cycles sont dans H (car H distingué dans $\mathcal{A}_n$, donc stable par conjugaison).
Or les 3-cycles engendrent $\mathcal{A}_n$ donc $H = \mathcal{A}_n$.

Lemmes utilisés

Lemme 0.1 *Soit $n \geq 3$. Alors $\mathcal{A}_n$ est engendré par les 3-cycles.*

Démonstration On procède par récurrence sur n.

- $n = 3$ Le groupe $\mathcal{A}_3$ est de cardinal $\frac{3!}{2} = 3$. Plus précisément $\mathcal{A}_3$ est composé de l'identité et des 3-cycles $(1\,2\,3)$ et $(1\,3\,2)$ et $(1\,2\,3)(1\,3\,2) = (1)(2)(3)$, d'où le fait que $\mathcal{A}_3$ soit engendré par les 3-cycles.
- $n \geq 3$ On suppose que $\mathcal{A}_n$ est engendré par les 3-cycles. Soit $\sigma \in \mathcal{A}_{n+1}$. Alors on distingue deux cas :
  - $\rightsquigarrow$ si $\sigma(n+1) = n+1$, alors $\sigma \in \mathcal{A}_n$ et donc σ s'écrit comme un produit de 3-cycles par hypothèse de récurrence.
  - $\rightsquigarrow$ si $\sigma(n+1) = i < n+1$, on considère alors le 3-cycle $\tau = (n+1\, j\, i)$ avec $j \in \{1, \ldots n+1\}$ et $j \neq i, n$. Alors $\tau\sigma(n+1) = \tau(i) = n+1$ et on se ramène ainsi au cas précédent, donc $\sigma = \tau^{-1}\times$ un produit de 3-cycles.

Lemme 0.2 (Théorème de Lagrange) *Soit G un groupe fini. Alors l'ordre de tout sous-groupe H de G divise l'ordre de G.*

Démonstration On considère la relation d'équivalence $x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$. C'est bien une relation d'équivalence car :
- $x\mathcal{R}x$ car $xx^{-1} = e \in H$ car H sous-groupe ;
- si $x\mathcal{R}y$, ie $xy^{-1} \in H$, alors $(xy^{-1})^{-1} = yx^{-1} \in H$ car H groupe, d'où $y\mathcal{R}x$;
- si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $xy^{-1} \in H$ et $yz^{-1} \in H$ d'où $xy^{-1}yz^{-1} = xz^{-1} \in H$ car H groupe, ie $x\mathcal{R}z$.

On note $\overline{x}$ la classe de $x \in G$.
On a $\overline{x} = Hx = \{zx, z \in H\}$ car $y \in \overline{x} \Leftrightarrow y\mathcal{R}x \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \in Hx$.
Pour tout $x \in G$, l'application :

$$\begin{aligned} H &\longrightarrow Hx \\ y &\longmapsto yx \end{aligned}$$

est une bijection (en effet, on peut exhiber sa réciproque : $Hx \ni y \longmapsto yx^{-1} \in H$). Donc $|H| = |Hx|$.
Ainsi les classes ont toutes $|H|$ éléments. Or les classes d'équivalence forment une partition de G donc $|G| = n|H|$ où $n = |G/H|$ est le nombre de classes d'équivalence.

Lemme 0.3 *Soit $n \geq 2$. Le cardinal de $\mathcal{A}_n$ est $\dfrac{n!}{2}$.*

Démonstration On utilise la définition du groupe alterné $\mathcal{A}_n$, c'est le noyau de l'application : $\epsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$. D'après la propriété universelle du quotient, on sait que le morphisme de groupes ϵ induit un isomorphisme de $\mathfrak{S}_n/\ker(\epsilon) \longrightarrow Im(\epsilon)$. Or $Im(\epsilon) = \{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$, donc $|\mathfrak{S}_n| = |\mathcal{A}_n| \times 2$; d'où le résultat.

Lemme 0.4 *Soit $\sigma \in \mathfrak{S}_n$ un cycle d'ordre p, ie $\sigma = (a_1 \ \ldots \ a_p)$. Soit $\tau \in \mathfrak{S}_n$. Alors $\tau\sigma\tau^{-1} = (\tau(a_1) \ \ldots \ \tau(a_p))$.*

Démonstration Montrons que le support de $\tau\sigma\tau^{-1}$ est $\{\tau(a_1), \ldots, \tau(a_p)\}$. Si $x \notin (\tau(a_1) \ \ldots \ \tau(a_p))$, alors $\tau^{-1}(x) \notin (a_1 \ \ldots \ a_p)$ et donc $\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$.
Regardons maintenant comment agit $\tau\sigma\tau^{-1}$ sur son support. Si $x = \tau(a_i)$, alors $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$.
D'où le résultat.

Lemme 0.5 *Soit $n \geq 3$. Soient $a_1, \ldots, a_n \in \{1, \ldots n\}$ distincts deux à deux, soient $b_1, \ldots, b_n \in \{1, \ldots, n\}$ distincts deux à deux. Alors $\exists \sigma \in \mathcal{A}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, \ldots, n-2$.*

Démonstration On remarque qu'il existe $\widehat{\sigma} \in \mathfrak{S}_n$ tel que $\forall i \in \{1, \ldots, n\}$, $\widehat{\sigma}(a_i) = b_i$ (par définition de $\mathfrak{S}_n$, quitte à prendre $\widehat{\sigma} = \prod_{i=1}^{n}(a_i \, b_i)$). On distingue alors deux cas :
- soit $\epsilon(\widehat{\sigma}) = 1$, alors $\widehat{\sigma} \in \mathcal{A}_n$ et on a le résultat.
- soit $\epsilon(\widehat{\sigma}) = -1$ alors on pose $\sigma = \widehat{\sigma}(a_{n-1} \, a_n)$ ($a_{n-1} \neq a_n$ d'après l'énoncé du lemme) et ainsi $\epsilon(\sigma) = \epsilon(\widehat{\sigma})\epsilon((a_{n-1} \, a_n)) = 1$, donc $\sigma \in \mathcal{A}_n$ et $\forall i = \{1, \ldots, n-2\}$, $\sigma(a_i) = b_i$.

Corollaire 0.1.1 *Soit $n \geq 5$. Alors les 3-cycles sont conjugués dans $\mathcal{A}_n$.*

Démonstration Soient $(a \, b \, c) \in \mathcal{A}_n$ et $(a' \, b' \, c') \in \mathcal{A}_n$ avec $a \neq b \neq c$ et $a' \neq b' \neq c'$.
Comme $n - 2 \geq 5 - 2 \geq 3$ alors d'après le lemme précédent il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(c) = c'$, ie $(a' \, b' \, c') = (\sigma(a) \, \sigma(b) \, \sigma(c)) = \sigma(a \, b \, c)\sigma^{-1}$.

Corollaire 0.1.2 *Soit $n \geq 5$. Alors les produits de transpositions sont conjugués dans $\mathcal{A}_n$.*

Démonstration On distingue deux cas :
- si $n \geq 6$, soient $(a \, b)(c \, d) \in \mathcal{A}_n$ et $(a' \, b')(c' \, d') \in \mathcal{A}_n$ avec $a \neq b \neq c \neq d$ et $a' \neq b' \neq c' \neq d'$. Alors d'après le lemme précédent, $\exists \sigma \in \mathcal{A}_n$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$, $\sigma(c) = c'$ et $\sigma(d) = d'$, ie $(a' \, b')(c' \, d') = \sigma(a \, b)(c \, d)\sigma^{-1} = \sigma(a \, b)\sigma^{-1}\sigma(c \, d)\sigma^{-1}$.
- si $n = 5$, soient $(a \, b)(c \, d)(e) \in \mathcal{A}_5$ et $(a' \, b')(c' \, d')(e') \in \mathcal{A}_5$, alors d'après le lemme précédent $\exists \sigma \in \mathcal{A}_5$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$, on a alors deux possibilités :
  - $\rightsquigarrow$ soit $\sigma(c) = c'$ et $\sigma(d) = d'$ et alors $(a' \, b')(c' \, d')(e') = \sigma(a \, b)(c \, d)(e)\sigma^{-1} = \sigma(a \, b)\sigma^{-1}\sigma(c \, d)\sigma^{-1}\sigma(e)\sigma^{-1}$.
  - $\rightsquigarrow$ soit $\sigma(c) = d'$ et $\sigma(d) = c'$ et alors $\sigma(c \, d)\sigma^{-1} = (d' \, c') = (c' \, d')$ (car $c' \neq d'$ par hypothèse) d'où le résultat.

Et $\mathcal{A}_n$ pour $n \leq 4$?

$\mathcal{A}_0$ **et** $\mathcal{A}_1$ $\quad \mathcal{A}_0 = \mathcal{A}_1 = \emptyset$

$\mathcal{A}_2$ $\quad |\mathcal{A}_2| = \dfrac{2!}{2} = 1$, donc $\mathcal{A}_2 = \{()\}$ et est simple.

$\mathcal{A}_3$ $\quad |\mathcal{A}_3| = \dfrac{3!}{2} = 3$, plus précisément $\mathcal{A}_3$ est composé de (), $(1\,2\,3)$ et de $(1\,3\,2)$.
Déterminons les sous-groupes possibles de $\mathcal{A}_3$, on a : $\{()\}$ et $\mathcal{A}_3$ et si on considère seulement deux éléments de $\mathcal{A}_3$, on a forcément l'élément $\{()\}$ sinon le sous-groupe n'admet pas d'élément neutre et si on ajoute par exemple $(1\,2\,3)$ alors ce dernier n'admet pas d'inverse dans le sous-groupe puisque son inverse est $(1\,3\,2)$ (et vice versa). Donc $\mathcal{A}_3$ est simple.

$\mathcal{A}_4$ $\quad |\mathcal{A}_4| = \dfrac{4!}{2} = 12$. Déterminons les éléments de $\mathcal{A}_4$:
- un élément d'ordre 1 : $()$;
- 3 éléments d'ordre 2 : $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$;
- 8 éléments d'ordre 3 de la forme $(a\,b\,c)$ avec a, b, c distincts car on a 4 possibilités pour choisir a, 3 possibilités pour choisir b et 2 possibilités pour choisir c, soit 24 possibilités, or $(a\,b\,c) = (b\,c\,a) = (c\,a\,b)$ donc il reste 8 possibilités, on a donc trouvé tous les éléments !

Déterminons un sous-groupe de $\mathcal{A}_4$ distingué. Considérons le sous-groupe $H = \{(); (1\,2)(3\,4); (1\,3)(2\,4); (1\,4)(2\,3)\}$. Il est bien distingué car : $\forall \sigma \in \mathcal{A}_4$,

$$\sigma(1\,2)(3\,4)\sigma^{-1} = \sigma(1\,2)\sigma^{-1}\sigma(3\,4)\sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4))$$

ce qui sera nécessairement un produit de transposition donc dans H. Donc $\mathcal{A}_4$ n'est pas simple.

Références

[Gou94] Xavier Gourdon. *Algèbre*. Ellipses, 1994.

[Mé06] Jean-Yves Mérindol. *Nombres et algèbre*. EDP Sciences, 2006.

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