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

Recasage : 103, 104, 105, 108

Réf : Perrin p 28

(1) Simplicité de $\mathcal{A}_5$ (par dénombrement) :

$\mathcal{A}_5$ possède $\frac{5!}{2} = 60$ éléments (car est d'indice 2 dans S_5) :

- l'identité, seul élément d'ordre 1
- les produits de transpositions à supports disjoints (les éléments d'ordre 2) on se donne pour ça un point fixe $\longrightarrow$ 5 choix possibles puis 2 éléments parmi les 4 restants pour l'une des deux transpositions (l'autre étant déterminée automatiquement après ça) ce qui fait $\binom{4}{2} = 6$ possibilités, mais comme les deux transpositions commutent (car à supports disjoints), cela en fait $\frac{6}{2} = 3$ distinctes d'où $5 \times 3 = 15$ choix.
- les 3-cycles (i.e les éléments d'ordre 3) : le choix de 3 éléments i, j, k distincts de $[\![1,5]\!]$ fournit deux 3-cycles distincts : $(i\ j\ k)$ et $(i\ k\ j)$ donc cela fait $\binom{5}{3} \times 2 = 10 \times 2 = 20$ éléments.
- les 5-cycles (éléments d'ordre 5) : il n'y a pas de points fixes donc on a 4 choix pour l'image de 1, 3 pour celle de 2, 2 pour celle de 3 d'où un total de $4 \times 3 \times 2 = 24$ éléments.

$60 = 1 + 15 + 20 + 24$ donc on a bien décrit tous les éléments de $\mathcal{A}_5$.

- On sait que les 3-cycles sont conjugués dans $\mathcal{A}_n$, $n \geq 5$
- Montrons que éléments d'ordre 2 sont conjugués dans $\mathcal{A}_5$:

  $\tau = (a\ b)(c\ d)(e)$, $\tau' = (a'\ b')(c'\ d')(e')$

  Comme $\mathcal{A}_5$ est $5-2=3$ transitif, il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$

On a donc $\sigma\tau\sigma^{-1} = \sigma(ab)(cd)(e)\sigma^{-1} = \sigma(ab)\sigma^{-1}\sigma(cd)\sigma^{-1}\sigma(e)\sigma^{-1}$

$= (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))(\sigma(e))$

$= (a'b')(c'd')(e')$

$= \tau'$

- Soit $H \lhd \mathcal{A}_5$ non trivial :
  - Si H contient un élément d'ordre 3 (resp. 2) il les contient tous d'après ce qui précède
  - Si H contient un élément d'ordre 5 σ, il contient le 5-Sylow $\langle\sigma\rangle$ et comme les 5-Sylow sont conjugués dans $\mathcal{A}_5$, H les contient tous et donc contient tous les éléments d'ordre 5.

$60 = 5\times 3\times 2^2$

  - D'après Lagrange, $|H| \mid 60$ mais si H ne contient qu'un seul type d'éléments ($\neq$ le neutre), on a $|H| \in \{15+1, 20+1, 24+1\} = \{16, 21, 25\}$ ce qui est impossible. Donc il en contient au moins deux types donc $|H| \geq 1+15+20 = 36$ donc $|H| = 60$ et $H = \mathcal{A}_5$ ce qui conclut.

⚠ Les 24 éléments d'ordre 5 ne sont pas conjugués sinon ils formeraient une orbite et l'on devrait avoir $24 \mid 60$.

② Cas $n > 5$: $E = [\![1, n]\!]$, $H \lhd \mathcal{A}_n$ non trivial, $\sigma \neq id \in H$

Idée : on se ramène au cas $n = 5$ à partir de σ en construisant $\rho \in H$ non trivial qui admet (au moins) $n-5$ points fixes. Avec F l'ensemble des (au plus) 5 éléments sur lesquels agit ρ, on a $\mathcal{A}(F) \simeq \mathcal{A}_5$ et on montre qu'on peut prolonger un 3-cycle de F en un 3-cycle de $\mathcal{A}_n$ qui est dans H.

Constats : • si $\rho = \underbrace{\tau\sigma\tau^{-1}}_{\in H}\underbrace{\sigma^{-1}}_{\in H}$ avec $\tau \in \mathcal{A}_n$, on a $\rho \in H$

• $\rho = \tau(\sigma\tau^{-1}\sigma^{-1})$ est de même type que τ donc a autant de pts fixes si τ aussi.

③ Comme $\sigma \neq id$, il existe $a \in E$ tel que $\beta := \sigma(a) \neq a$.

Soit $c \in E \setminus \{a, \beta, \sigma(\beta)\}$ et posons $\tau = (a\ c\ \beta)$ d'où $\tau^{-1} = (a\ \beta\ c)$.

Soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ \beta)\,\sigma\,(a\ \beta\ c)\,\sigma^{-1} = \underbrace{(a\ c\ \beta)}_{\text{distincts}}\,\underbrace{(\sigma(a)\ \sigma(\beta)\ \sigma(c))}_{\text{distincts}}$

$$\begin{cases} \beta = \sigma(a) = \sigma(\beta) \iff \beta = a & \text{impossible} \\ \beta = \sigma(a) = \sigma(c) \iff a = c & \text{impossible} \\ \sigma(\beta) = \sigma(c) \iff \beta = c & \text{impossible} \end{cases}$$

Comme $\beta = \sigma(a)$, l'ensemble $F := \{a, \beta, c, \sigma(a), \sigma(\beta), \sigma(c)\}$ possède au plus 5 éléments. ρ agit donc sur au plus 5 éléments, ceux de F donc $\rho(F) = F$ et $\rho_{|E\setminus F} = id_{E\setminus F}$ (tous les éléments de $E \setminus F$ sont des points fixes pour ρ)

Quitte à rajouter des éléments inutiles (i.e stables par ρ), on peut supposer que $|F| = 5$.

④ Comme $\tau^{-1}(\beta) = c \neq \sigma(\beta)$, on a $\rho(\beta) = \tau\sigma\tau^{-1}\sigma^{-1}(\beta) = \tau\sigma\tau^{-1}(a) = \tau\sigma(\beta) \neq \beta$

donc $\rho_{|F} \neq id_F$.

Soit $\mathcal{A}(F)$ l'ensemble des permutations paires de F, on a $\mathcal{A}(F) \simeq \mathcal{A}_5$ qui est simple d'après ①.

On peut plonger $\mathcal{A}(F)$ dans $\mathcal{A}_n$ via $u \longmapsto \tilde{u}$ avec $\begin{cases} \tilde{u}_{|F} = u \\ \tilde{u}_{|E\setminus F} = id_{E\setminus F} \end{cases}$

Soit $H_0 = \{u \in \mathcal{A}(F) : \tilde{u} \in H\} = H \cap \mathcal{A}(F)$ et montrons que $H_0 = \mathcal{A}(F)$.

- $H_0 \neq \{id\}$ car $\begin{cases} \rho_{|F} \in \mathcal{A}(F) \text{ donc } \rho_{|F} \in H_0 \text{ et } \rho_{|F} \neq id_F. \\ \widetilde{\rho_{|F}} = \rho \in H \end{cases}$
- si $u \in H_0$ et $v \in \mathcal{A}(F)$ alors $vuv^{-1} \in \mathcal{A}(F)$

et $\widetilde{vuv^{-1}} = \underbrace{\tilde{v}}_{\in \mathcal{A}_n}\underbrace{\tilde{u}}_{\in H}\underbrace{\tilde{v}^{-1}}_{\in \mathcal{A}_n} \in H$ car $H \trianglelefteq \mathcal{A}_n$, donc $H_0 \trianglelefteq \mathcal{A}(F)$

6

- par simplicité de $\mathcal{A}(F) \simeq \mathcal{A}_5$, on a bien $H_0 = \mathcal{A}(F)$.

Il existe donc $u \in \mathcal{A}(F)$ un 3-cycle qui se prolonge en $\tilde{u} \in \mathcal{A}_n$ qui est encore un 3-cycle et comme $\mathcal{A}(F) = H_0$, on a $\tilde{u} \in H$. Ainsi H contient un 3-cycle de $\mathcal{A}_n$.

Comme les 3-cycles sont conjugués dans $\mathcal{A}_n$, H les contient donc tous, et comme les 3-cycles engendrent $\mathcal{A}_n$, $H = \mathcal{A}_n$ ce qui conclut. □

Détails

- Si $\tau = (a_1 \cdots a_p) \in S_n$ est un cycle d'ordre p et si $\sigma \in S_n$, on a [Per] p 16

$$\sigma\tau\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_p)).$$

  - Si $x \notin \{\sigma(a_1), \dots, \sigma(a_p)\}$, $\sigma^{-1}(x) \notin \{a_1, \dots, a_p\}$ donc $\sigma^{-1}(x)$ est un point fixe de τ donc $\sigma\tau\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x$
  - Si $x = \sigma(a_i)$, on a $\sigma\tau\sigma^{-1}(x) = \sigma\tau(a_i) = \sigma(a_{i+1})$ où les indices sont pris mod. p.

Conséquence : si $g \in G$, $g' = \sigma g \sigma^{-1}$ est un élément « du même type » que g
e.g. si g est d'ordre k, g' l'est aussi
si g a k points fixes, g' en a autant ...

- Dans S_n tous les cycles d'ordre p sont conjugués. [Per] p 16

Soient $\sigma = (a_1 \cdots a_p)$ et $\tau = (b_1 \cdots b_p)$ et soit $g \in S_n$ qui envoie a_i sur b_i.
Alors d'après ce qui précède, $g\sigma g^{-1} = (g(a_1) \cdots g(a_p)) = (b_1 \cdots b_p) = \tau$.

- A_n est $n-2$ fois transitifs sur $[\![1, n]\!]$ i.e si $a_1, \dots, a_{n-2}$ sont distincts et $b_1, \dots, b_{n-2}$ sont distincts, il existe $\sigma \in A_n$ tel que $\sigma(a_i) = b_i$. [Per] p 16

On écrit $[\![1, n]\!] = \{a_1, \dots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \dots, b_{n-2}, b_{n-1}, b_n\}$
et on considère $\sigma \in S_n$ qui envoie a_i sur b_i pour tout i.
Si σ est paire on a fini, sinon on compose σ avec la transposition $(a_{n-1}\ a_n)$.

- Si $n \geq 5$, les 3-cycles sont conjugués dans A_n. [Per] p 16

Si $\sigma = (a_1\ a_2\ a_3)$ et $\tau = (b_1\ b_2\ b_3)$, comme A_n est $n-2$ transitif, il existe $g \in A_n$ qui envoie a_i sur b_i. On a alors

$$g\sigma g^{-1} = (g(a_1) \cdots g(a_3)) = (b_1 \cdots b_3) = \tau.$$

⚠ C'est faux pour $n \in \{3, 4\}$: • A_3 est abélien donc la conjugaison est triviale
• A_4 contient 8 cycles d'ordre 3 donc s'ils étaient conjugués ils formeraient une orbite dont le cardinal devrait diviser $|A_4| = \frac{4!}{2} = 12$.

Détails (suite)

- **Pour $n \geq 3$, A_n est engendré par les 3-cycles.** [Per] p 11

S_n est engendré par les transpositions donc A_n est engendré par les produits pairs de transpositions. On a $(a\,b)(c\,d) = (a\,b)(a\,c)(a\,c)(c\,d)$
$= (b\,a)(a\,c)(a\,c\,d)$
$= (a\,c\,b)(a\,c\,d)$.

- **A_3 est simple.**

On a $A_3 = \{id, (1\,2\,3), (1\,3\,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ qui abélien (donc la conjugaison est triviale) et comme 3 est premier il n'y a pas de sous-groupe (simple) non trivial.

- **A_4 n'est pas simple.**

A_4 est d'ordre 12, il contient les cycles d'ordre 3 et les produits de deux transpositions à supports disjoints :

$A_4 = \{id, (2\,3\,4), (2\,4\,3), (1\,3\,4), (1\,4\,3), (1\,2\,4), (1\,4\,2), (1\,2\,3), (1\,3\,2),$
$(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

- $V = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ est distingué dans A_4 :

$\sigma(1\,2)(3\,4)\sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4)) \in V$ et idem pour les autres donc V est clairement distingué dans A_4.

- les double transpositions sont conjuguées dans A_4

⚠ les 3-cycles ne sont pas conjugués dans A_4 ; sinon ils formeraient une orbite mais comme il y en a 8 on aurait $8 \mid 12$: impossible.

$Z(S_n) = \{id\}$: en effet si $\sigma \in Z(S_n)$, $\sigma(1\,2)\sigma^{-1} = (1\,2) = (\sigma(1)\,\sigma(2))$ donc $\sigma(1) \in \{1, 2\}$ et si on recommence avec $(1\,3)$ on a que $\sigma(1) = 1$ et de même $\sigma(k) = k$ d'où $\sigma = id$.

Si $H = \{e, x\} \trianglelefteq G$, $\forall g \in G$, $gxg^{-1} \in H$ car H est distingué dans G. Si $gxg^{-1} = e$ on a $gx = g$ d'où $x = e$, absurde. Donc $gx = xg$ i.e $x \in Z(G)$ donc $H \subset Z(G)$.
(i.e tout sous-groupe distingué d'ordre 2 est contenu dans le centre)