Développement. **Simplicité de A_n, $n \geq 5$** Leçons : 103, 104, 105, 108

Références : • D. Perrin, Cours d'algèbre pp 15-16.
• J-E Rombaldi, Mathématiques pour l'agrégation, Algèbre et géométrie, pp 49-51.

Lemme 1 Pour $n \geq 3$, A_n est engendré par les 3-cycles.

Preuve

Soit $n \geq 3$. S_n est engendré par les transpositions.
Soit $\sigma \in A_n$. Alors σ s'écrit comme un produit pair de transposit°.
Or chaque produit de transpositions peut s'écrire comme un produit de 3-cycles. En effet, si $x, y, z, t \in \{1, \dots, n\}$ sont 2 à 2 $\neq$ (sauf si $n = 3$, auquel le point i) suffit), alors :

i) $(x\ y)(x\ z) = (x\ z\ y)$
ii) $(x\ y)(z\ t) = (x\ y\ z)(y\ z\ t)$

Donc σ s'écrit comme un produit de 3-cycles. $\square$

Lemme 2 Pour $n \geq 5$, les 3 cycles sont conjugués dans A_n.

Preuve

Soit $n \geq 5$. Soit $(a\ b\ c)$ et $(\alpha\ \beta\ \gamma)$ deux 3-cycles. Soit $\sigma \in S_n$ telle que $\sigma(a) = \alpha$, $\sigma(b) = \beta$, $\sigma(c) = \gamma$. Alors $\sigma (a\ b\ c) \sigma^{-1} = (\sigma(a)\ \sigma(b)\ \sigma(c)) = (\alpha\ \beta\ \gamma)$.

• Si $\sigma \in A_n$: c'est bon.
• Si $\sigma \notin A_n$: soit τ $i, j \notin \{\alpha, \beta, \gamma\}$ (possible car $n \geq 5$). Alors, $\tilde{\sigma} := \tau \sigma \in A_n$ et $\tilde{\sigma}(a\ b\ c)\tilde{\sigma}^{-1} = (\alpha\ \beta\ \gamma)$, ce qui conclut $\square$

Théorème Pour $n \geq 5$, A_n est simple.

Preuve

Par les lemmes, si $H \triangleleft A_n$, il suffit de prouver que $H = \{Id\}$ ou bien que H contient un 3-cycle. Soit donc $H \triangleleft A_n$ un sous-groupe distingué de A_n non trivial. Soit $\sigma \in H \setminus \{Id\}$. Soit $x \in [\![1, n]\!]$, et on pose $y = \sigma(x) \neq x$ ($\sigma \neq Id$). On fixe $z \notin \{x, y, \sigma(y)\}$, ce qui est possible car $n \geq 5$.

On pose finalement $\gamma = (x\ y\ z)$ et $\sigma' = [\sigma, \gamma]$.
Alors $\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \underbrace{\sigma}_{\in H}(\overbrace{\gamma\sigma^{-1}\gamma^{-1}}^{}) \in H$, et
 $\in H,\ H \triangleleft A_n$

$$\sigma' = (\sigma(x\ y\ z)\sigma^{-1})(x\ y\ z)^{-1}$$
$$= (\sigma(x)\ \sigma(y)\ \sigma(z))(y\ x\ z).$$
$$= (y\ \sigma(y)\ \sigma(z))(y\ x\ z).$$

Ainsi $\mathrm{Supp}(\sigma') \subset \{x, y, z, \sigma(y), \sigma(z)\}$ qui a au plus 5 éléments.
Soit ℓ le type de σ'. On distingue les cas.

- si $\ell = [1,1,1,1,1]$, alors $\sigma' = Id$, donc $\sigma\gamma = \gamma\sigma$, ce qui implique $\sigma(y) = \sigma\gamma(x) = \gamma\sigma(x) = \gamma(y) = z$, ce qui est faux.
- si $\ell = [2,2,1]$, alors $\sigma' = (i\ j)(k\ l)$, avec i, j, k, l 2 à 2 $\neq$.
  Soit $m \notin \{i, j, k, l\}$ $(n \geq 5)$. On note $\rho = (i\ j\ m) \in A_n$.
  Alors $\sigma'' := [\sigma', \rho] \in H$ et
  $$\sigma'' = (\sigma'\rho\sigma'^{-1})\rho^{-1} = (\sigma'(i)\ \sigma'(j)\ \sigma'(m))(j\ i\ m)$$
  $$= (j\ i\ m)(j\ i\ m)$$
  $$= (j\ m\ i), \text{ qui est un 3-cycle.}$$

- si $\ell = [3,1,1]$: c'est bon.
- si $\ell = [5]$, $\sigma' = (i\ j\ k\ l\ m)$. On note $\rho = (i\ j\ k) \in A_n$.
  Alors de même $\sigma'' := [\sigma', \rho] \in H$ et
  $$\sigma'' = (\sigma'\rho\sigma'^{-1})\rho^{-1} = (\sigma'(i)\ \sigma'(j)\ \sigma'(k))(j\ i\ k)$$
  $$= (j\ k\ l)(j\ i\ k)$$
  $$= (j\ i\ l).$$

$\square$

Corollaire.

Pour $n \geq 5$, $D(A_n) = A_n$
Pour $n \geq 2$, $D(S_n) = A_n$

Faux pour $n=4$. $D(A_4) \triangleleft A_4$, $D(A_4) \simeq V_4$.

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

Corollaire

Pour $n \geq 5$, les sg distingués de S_n sont $\{1\}, A_n, S_n$.

Preuve

Soit $H \triangleleft S_n$. Alors $H \cap A_n \triangleleft A_n \Rightarrow H \cap A_n = \{1\}$ ou A_n

1) Si $H \cap A_n = A_n$, on a $H = A_n$ ou S_n.

2) Si $H \cap A_n = \{1\}$. ε induit un iso: $\varepsilon : H \to \varepsilon(H)$

avec $\varepsilon(H) \subset \{-1, +1\}$. Donc $|H| = |\varepsilon(H)| \leq 2$.

Si $|H| = 2$, alors $H = \{1, \sigma\}, \sigma \in S_n$.

Si $\tau \in S_n$ ~~tout~~, alors $\tau\sigma\tau^{-1} \in H$, $\tau\sigma\tau^{-1} \neq id$

donc $\tau\sigma\tau^{-1} = \sigma \Rightarrow \tau\sigma = \sigma\tau$, donc σ central.

Or $Z(S_n) = \{id\}, (n \geq 3)$. $H = \{1\}$.

$\square$

Pq $Z(S_n) = \{id\}$ si $n \geq 3$? si $n=2$, $S_n = Z(S_n)$.

Soit $\sigma \in Z(S_n)$, $n \geq 3$. Soit $x \neq y$. On a

$(\sigma(x)\,\sigma(y)) = \sigma(x\,y)\sigma^{-1} = (x\,y)\sigma\sigma^{-1} = (x\,y)$.

$\Rightarrow \sigma\{x, y\} = \{x\,y\}$.

Soit $y \neq z \neq x$.

(possible car $n \geq 3$), $\{x\} = \{x, y\} \cap \{x, z\}$.

$$\{\sigma(x)\} = \sigma(\{x\})$$
$$= \sigma(\{x,y\} \cap \{x,z\})$$
$$= \sigma(\{x,y\}) \cap \sigma(\{x,z\})$$
$$= \{x,y\} \cap \{x,z\} = \{x\} \quad \sigma(x) = x \ \forall x.$$

Autre app.:

| Soit $H < S_n$, $[S_n : H] = n$. Alors $H \simeq S_{n-1}$.

Preuve $n \leq 4$, à la main.

Si $n \geq 5$. On pose $G = S_n$, et $X = G/H$. (⚠ ≠ groupe)

Alors $G \curvearrowright X$ via $(g, \tilde{g}H) \mapsto (g\tilde{g})H$.

Ainsi on a $\varphi : G \to S(X) \simeq S_n$, $[G : H] = n$.

$\operatorname{Ker} \varphi \triangleleft G \Rightarrow \operatorname{Ker} \varphi = \{\{id\}, A_n, G\}$.

→ $\operatorname{Ker} \varphi \neq G$, sinon φ trivial, $G \neq H$.

→ Si $\operatorname{Ker} \varphi \subset H$, $\left\{ \begin{array}{l} |H| = \dfrac{|G|}{n} = (n-1)! \\ |A_n| = \dfrac{n!}{2} \end{array} \right.$

et $\dfrac{n!}{2} = (n-1)! \times \dfrac{n}{2} > (n-1)!$

donc $\operatorname{Ker} \varphi \neq A_n$ $\operatorname{Ker} \varphi = \{1\}$.

φ injectif. $|G| = |S(X)|$, donc φ iso.

Or $H = \operatorname{Stab}(1)$, $\varphi(H)$ stab. d'un point dans S_n
$\Rightarrow H \simeq S_{n-1}$.

Dans la même ordre.

$S_n \hookrightarrow A_{n+2}$, mais S_n ne s'injecte pas dans A_{n+1}.

(I) (II)

(I) : on compose avec transposition

$\varphi : S_n \to A_{n+2}$

$\sigma \mapsto \begin{cases} \sigma \text{ si } \sigma \in A_n \\ \sigma \circ (n+1\ n+2) \text{ si } \sigma \notin A_n \end{cases}$

(II) Si $S_n \hookrightarrow A_{n+1}$. Alors $S_n \simeq H$, $H < A_{n+1}$, d'indice $\frac{n+1}{2}$.

$X = A_{n+1} / \cancel{\ } H$.

$A_{n+1} \curvearrowright X$, $(g, \tilde{g}H) \mapsto (g\tilde{g}H) \in X$.

$\varphi : A_{n+1} \to S(X) \simeq S_{\frac{n+1}{2}}$.

Ker $\varphi = \{id\}$ ou $\underline{\text{Ker } \varphi = \{A_{n+1}\}}$

$\hookrightarrow \Rightarrow$ φ trivial impossible

$\forall g \in A_{n+1}$, $\sigma_g = id$

$\Rightarrow \forall g \in A_{n+1}, \forall h \in A_{n+1}$, $ghH = gH$.

$\Rightarrow A_{n+1} = H$.

$\hookrightarrow$ φ inj. $A_{n+1} \hookrightarrow S_{(\frac{n+1}{2})}$

$|A_{n+1}| = \cancel{\ } \frac{(n+1)!}{2} > \left(\frac{n+1}{2}\right)!$.