G

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

Leçons : 103, 104, 105, 108

Réf. : Perrin, Cours d'algèbre p. 28

Th. Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$

1) M.q. $\mathcal{A}_5$ est simple par dénombrement

$\mathcal{A}_5$ contient 60 éléments :

id ; 15 doubles transpositions (disjointes), 20 3-cycles et 24 5-cycles.

Soit $H \triangleleft \mathcal{A}_5$, $H \neq \{id\}$.

- si H contient un 3 cycle, alors il les contient tous car les 3-cycles sont conjugués dans $\mathcal{A}_5$ (vrai si $n \geq 5$)
- si H contient une double-transposit°, alors il les contient toutes car elles sont également conjuguées dans $\mathcal{A}_5$.

En effet, soient $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$ deux doubles-transpositions.

Alors il existe $\sigma \in \mathcal{A}_5$ tq $\sigma(a) = a'$ $\sigma(b) = b'$ et $\sigma(e) = e'$ car $(a\,b\,e)$ et $(a'b'e')$ sont conjugués dans $\mathcal{A}_5$. σ envoie alors $\{c\,d\}$ sur $\{c'd'\}$, et $\sigma \tau \sigma^{-1} = \tau'$

- si H contient un 5-cycle σ : alors $\langle \sigma \rangle \subset H$.

On $|\mathcal{A}_5| = 60 = 5 \times 2^2 \times 3$ donc $\langle \sigma \rangle$ est un 5-Sylow de $\mathcal{A}_5$. Ceux-ci étant conjugués dans $\mathcal{A}_5$, H contient tous les 5-Sylow de $\mathcal{A}_5$ donc H contient tous les 5-cycles.

$H \leq \mathcal{A}_5$ donc $|H| \mid 60$.

Si H ne contient qu'un seul des trois types d'éléments ci-dessus, alors $|H| \in \{1+15, 1+20, 1+24\} = \{16, 21, 25\}$, absurde

Par conséquent, H contient au moins deux types d'éléments, donc $|H| \geq 1+15+20 = 36$, et $|H| \mid 60$ donc $|H| = 60$ et par cardinalité :

$H = \mathcal{A}_5$.

Donc, $\boxed{\mathcal{A}_5 \text{ est simple}}$.

2) $n > 5$

Soit $H \triangleleft \mathcal{A}_n$, $H \neq \{id\}$. Deux remarques :

(1) Si H contient un 3-cycle, ceux-ci étant conjugués dans $\mathcal{A}_n$, alors il les contient tous. $\mathcal{A}_n$ étant engendré par les 3-cycles, on a alors $H = \mathcal{A}_n$

(2) Soit $\sigma \in H$, et $\tau \in \mathcal{A}_n$. Alors $\rho = \underbrace{\tau \sigma \tau^{-1}}_{\substack{\in H \\ \text{car } H \triangleleft \mathcal{A}_n}} \underbrace{\sigma^{-1}}_{\in H} \in H$

Méthode : construire un élément ρ de H qui admet (au moins) $n-5$ pts fixes et tq $\rho \neq id$. En notant $F = \{5 \text{ pts restants}\}$, on a alors $\mathcal{A}(F) \simeq \mathcal{A}_5$.

On montre alors qu'on peut prolonger un 3-cycle de F en un 3-cycle de $\mathcal{A}_n$ qui appartient à H, et on utilise la remarque (1).

a°/ Construction de ρ

Soit $\sigma \in H$, $\sigma \neq id$. On pose $E = \{1 \dots n\}$.

$\exists a \in E \,/\, b = \sigma(a) \neq a$. Soit $c \in E$ tq $c \neq a, b, \sigma(b)$.

Alors : b, $\sigma(b)$ et $\sigma(c)$ sont distincts

en effet : $b = \sigma(b) \iff \sigma(a) = \sigma^2(a) \iff a = \sigma(a)$ absurde

$b = \sigma(c) \iff \sigma(a) = \sigma(c) \iff a = c$ absurde

$\sigma(b) = \sigma(c) \iff b = c$ absurde

Soit $\tau = (a\,c\,b) \in \mathcal{A}_n$. On pose $\boxed{\rho = \tau \sigma \tau^{-1} \sigma^{-1}} \in H$ d'après (2)

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

De plus $\varrho \neq id$ car $\varrho(b) = \tau(\sigma(b)) \neq c$

car sinon $\sigma(b) = \tau^{-1}(c) = b$.

$$F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$$ contient au plus 5 éléments ($c = \sigma(a)$),

$$\begin{cases} \varrho(F) = F \text{ et } \varrho_{|E \setminus F} = id_{E\setminus F} \\ \varrho_{|F} \neq id_{|F} \end{cases}$$

Quitte à rajouter dans F des éléments de E stables par ϱ, on peut supposer $\boxed{|F| = 5}$.

b/ Plongement de $A(F)$ dans A_n et conclusion

Soit $A(F)$ l'ensemble des permutations paires de $F \subset E$

Alors $A(F) \simeq A_5$ et on peut plonger $A(F)$ dans A_n par le morphisme

$$A(F) \longrightarrow A_n$$
$$u \longmapsto \overline{u} \text{ tq } \overline{u}_{|F} = u \text{ et } \overline{u}_{|E\setminus F} = id_{E\setminus F}$$

Soit $H_0 = \{u \in A(F) \,/\, \overline{u} \in H\}$. M.q. $H_0 = A(F)$

- $H_0 \neq \{id_{|F}\}$ car $\varrho_{|F} \in A(F)$ et $\overline{\varrho_{|F}} = \varrho \in H$ et $\varrho_{|F} \neq id$
- soit $u \in H_0$, et $v \in A(F)$.

Alors $vuv^{-1} \in A(F)$

et $\overline{vuv^{-1}} = \underbrace{\overline{v}}_{\in A_n}\ \underbrace{\overline{u}}_{\in H}\ \underbrace{\overline{v^{-1}}}_{\in A_n} \in H$ car $H \triangleleft A_n$

donc $H_0 \triangleleft A(F)$

Or, $A(F) \simeq A_5$ qui est simple donc $A(F)$ est simple donc $\boxed{H_0 = A(F)}$

Il existe donc $u \in A(F)$ un 3-cycle qui se prolonge en $\overline{u} \in A_n$ qui est un 3-cycle également, et tel que $\overline{u} \in H$.

Donc H contient un 3-cycle (de A_n), donc d'après (1), $\boxed{H = A_n}$,

et $\boxed{A_n \text{ est simple.}}$