

Dev n° 9

Ref : Jean Etienne Rombaldi  
 "Mathématiques par l'agrégation :  
 Algèbre et géométrie"

Titre : Simplicité de  $\mathcal{A}_n$  (à  $n \geq 5$ ).

Notre but est :

Thm :

Si  $n \geq 5$ .

Alors,  $\mathcal{A}_n$  est simple. (ss-g distingué sont seulement  $\mathcal{A}_n, \{id\}$ .)

Par  $\approx$  faire montrons les lemmes suivants :

Lemme 1 :

Si  $n \geq 3$ ,  $\mathcal{A}_n$  est engendré par les 3-cycles.

Lemme 2 :

Si  $n \geq 5$ , alors les 3-cycles sont conjugués dans  $\mathcal{A}_n$ .

Démo : (Lemme 1)

Notons  $G$  le ss-g engendré par les 3-cycles.

On a bien  $G \subset \mathcal{A}_n$  (tout les él. de  $G$  on signature 1)

Soit  $\sigma \in \mathcal{A}_n$ . Comme  $S_n$  engendré par les transpositions\*, alors  $\sigma$  s'écrit comme produit d'un nombre pair de transpositions. (car transposition signature -1)

Or  $\forall i, j, k, l \in [1, n]$  distincts,

$$(ij)(ik) = (ikj) \quad \text{et} \quad (ij)(kl) = (ijkl)(jkl).$$

Donc, le produit de 2 transpositions distincts est un produit de 3-cycles.

Par conséquent,  $\sigma$  s'écrit comme un produit de 3-cycles.

Ainsi,  $\sigma \in G$ . D'où  $G = \mathcal{A}_n$ .

Démo : (Lemme 2)

les 3-cycles sont une classe de conjugaison dans  $S_n^*$ .

Pretons,  $(abc)$  et  $(def) \in \mathcal{A}_n$ .

Donc,  $\exists \sigma \in S_n$  t.q.  $\sigma (abc) \sigma^{-1} = (def)$ .

$\rightarrow$  Si  $\sigma \in \mathcal{A}_n$  : c'est fini.

$\rightarrow$  sinon : comme  $n \geq 5$ ,  $\exists i, j \notin \{a, b, c\}$  distincts.

On pose  $\sigma' = \sigma (ij) \in \mathcal{A}_n$  et  $\sigma' (abc) \sigma'^{-1} = (def)$

Donc, OK  $\square$

Démo : (Thm)

Soit  $H \triangleleft \mathcal{A}_n$  et  $H \neq \{id\}$ .

Il y a  $H = \mathcal{A}_n$ .

Grâce aux lemmes, il suffit de m.q.  $H$  possède un 3-cycle.

Soit  $\sigma \in H \setminus \{id\}$ .

...

Grâce aux lemmes, il suffit de m.q.  $H$  possède un 3-cycle.

Soit  $\sigma \in H \setminus \{id\}$ .

Alors,  $\exists a, b \in [1, n]$  distincts t.q.  $\sigma(a) = b$ .

Comme  $n \geq 5$ , alors,  $\exists c \notin \{a, b, \sigma(b)\}$ .

Prenons,  $\tau = (a \ b \ c)$  et  $\sigma_2 = \underbrace{\sigma \tau \sigma^{-1} \tau^{-1}}_{\in H} \in H$  car  $\tau \in \mathcal{A}_n$  et  $\sigma^{-1} \in H$  et  $H \triangleleft \mathcal{A}_n$ .

De plus,

$$\begin{aligned} \sigma_2 &= \sigma(a \ b \ c) \sigma^{-1} (a \ b \ c)^{-1} \\ &= (\sigma(a) \ \sigma(b) \ \sigma(c)) (a \ b \ c)^{-1} \\ &= (b \ \sigma(b) \ \sigma(c)) (a \ b \ c)^{-1} \end{aligned}$$

done  $\neq$  transpo.

Donc le support de  $\sigma_2$  a au plus 5 élé et  $\varepsilon(\sigma_2) = 1$ , donc  $\sigma_2$  vaut:

$\rightarrow \sigma_2 = id$  ( $\Rightarrow \sigma \tau = \tau \sigma$  impossible car  $\sigma \tau(a) = \sigma(b) \neq c = \tau(b) = \tau \sigma(a)$ )

$\rightarrow \sigma_2$  3-cycle  $\Rightarrow H$  possède un 3-cycle : ça conclut.

$\rightarrow \sigma_2$  est le produit de 2 transpo à supports disjoints :  $\sigma_2 = (ij)(\ell k)$ .

Prenons  $m \notin \{ij, k, \ell\}$  et posons

$$\sigma_3 = \underbrace{\sigma_2}_{\in H} \underbrace{(ij \ m) \sigma_2^{-1} (i \ m \ j)}_{\in H \triangleleft \mathcal{A}_n} = (j \ i \ m) (i \ m \ j) = (i \ j \ m) \in H$$

ça conclut

$\rightarrow \sigma_2$  est un 5-cycle :  $\sigma_2 = (i \ j \ k \ \ell \ m)$

$$\begin{aligned} \text{On pose } \sigma_3 &= \underbrace{(i \ j \ k) \sigma_2 (i \ k \ j)}_{\in H \triangleleft \mathcal{A}_n} \underbrace{\sigma_2^{-1}}_{\in H} \\ &= (i \ j \ k) (j \ \ell \ k) \\ &= (i \ j \ \ell) \in H \end{aligned}$$

ça conclut

Dans tout les cas on trouve un 3-cycle  $\in H$ , d'où  $\mathcal{A}_n$  simple  $\square$

### Annexe:

- $\mathcal{A}_1$  et  $\mathcal{A}_2$  sont triviaux donc simple.
- $\mathcal{A}_3 = \{id, (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}$  donc simple.
- $\mathcal{D} = \{id, (12)(34), (13)(24), (14)(23)\} \triangleleft \mathcal{A}_4$  ( $n=4$ , ça non simple)  
graphe bi-transposition
- Si  $n \geq 5$ ,  $\{Id\} \triangleleft \mathcal{A}_n \triangleleft S_n$ .
- $S_n$  engendré par les transpositions.

### Démo:

Montrons qu'une permutation est un produit de cycles. Soit  $\sigma \in \mathcal{S}_n$ .

- Existence :  $[1, n] = \bigsqcup_{k=1}^r \mathcal{O}_k$  (partition d'orbites). Posons  $c_k(i) = \begin{cases} i & \text{si } i \notin \mathcal{O}_k \\ \sigma(i) & \text{si } i \in \mathcal{O}_k \end{cases}$   
 $c_k$  est un cycle de longueur  $\ell_k = \dim \mathcal{O}_k$ . Comme les supports des cycles  $c_k$  sont disjoints alors  $\forall i \in [1, n], \exists ! k$  tel que  $i \in \mathcal{O}_k$  et  $c_1 \circ \dots \circ c_r(i) = c_k(i) = \sigma(i)$ . Donc  $\sigma = c_1 \circ \dots \circ c_r$ .

- Unicité : Si  $\sigma = \tau_1 \circ \dots \circ \tau_p$ . Ainsi,  $\text{Supp}(\sigma) = \bigsqcup_{i=1}^r \text{Supp}(c_i) = \bigsqcup_{j=1}^p \text{Supp}(\tau_j)$ .  
Ainsi,  $\forall k \in [1, n], \exists ! i \in [1, r], \exists ! j \in [1, p], k \in \text{Supp}(c_i)$  et  $k \in \text{Supp}(\tau_j)$ . Quitte à renuméroter, on peut supposer  $k \in \text{Supp}(c_1) \cap \text{Supp}(\tau_1)$ . Donc  $\sigma(k) = c_1(k) = \tau_1(k)$  et  $\forall N, \sigma^N(k) = c_1^N(k) = \tau_1^N(k)$ . Donc  $c_1 = \tau_1$ . En reproduisant ce raisonnement, on obtient  $r = p$  et  $\forall i \in [1, r], c_i = \tau_i$ .

- Montrons à présent qu'un cycle est un produit de transpositions.

Soit  $(x_1, x_2, \dots, x_r)$  un cycle.  $(x_1, x_2, \dots, x_r) = (x_1, x_2)(x_2, x_3) \dots (x_{r-1}, x_r)$ .

$\square$

Montrons qu'une permutation est un produit de cycles. Soit  $\sigma \in \mathfrak{S}_n$ .

- Existence :  $\llbracket 1, n \rrbracket = \bigsqcup_{k=1}^r \mathcal{O}_k$  (partition d'orbites). Posons  $c_k(i) = \begin{cases} i & \text{si } i \notin \mathcal{O}_k \\ \sigma(i) & \text{si } i \in \mathcal{O}_k \end{cases}$   
 $c_k$  est un cycle de longueur  $\ell_k = \dim \mathcal{O}_k$ . Comme les supports des cycles  $c_k$  sont disjoints alors  $\forall i \in \llbracket 1, n \rrbracket, \exists ! k$  tel que  $i \in \mathcal{O}_k$  et  $c_1 \circ \dots \circ c_r(i) = c_k(i) = \sigma(i)$ . Donc  $\sigma = c_1 \circ \dots \circ c_r$ .

- Unicité : Si  $\sigma = \tau_1 \circ \dots \circ \tau_p$ . Ainsi,  $\text{Supp}(\sigma) = \bigsqcup_{i=1}^r \text{Supp}(c_i) = \bigsqcup_{j=1}^p \text{Supp}(\tau_j)$ .  
Ainsi,  $\forall k \in \llbracket 1, n \rrbracket, \exists ! i \in \llbracket 1, r \rrbracket, \exists ! j \in \llbracket 1, p \rrbracket, k \in \text{Supp}(c_i)$  et  $k \in \text{Supp}(\tau_j)$ . Quitte à renuméroter, on peut supposer  $k \in \text{Supp}(c_1) \cap \text{Supp}(\tau_1)$ . Donc  $\sigma(k) = c_1(k) = \tau_1(k)$  et  $\forall N, \sigma^N(k) = c_1^N(k) = \tau_1^N(k)$ . Donc  $c_1 = \tau_1$ . En reproduisant ce raisonnement, on obtient  $r = p$  et  $\forall i \in \llbracket 1, r \rrbracket, c_i = \tau_i$ .

- Montrons à présent qu'un cycle est un produit de transpositions.

Soit  $(x_1, x_2, \dots, x_r)$  un cycle.  $(x_1, x_2, \dots, x_r) = (x_1, x_2)(x_2, x_3) \dots (x_{r-1}, x_r)$ . □

- Tous les 3-cycles sont conjugués dans  $S_n$ .

Démonstration.

Soit  $\sigma = (x_1 x_2 x_3)$  et  $\tau \in S_n$ . Posons  $\sigma'' = (\tau(x_1) \tau(x_2) \tau(x_3))$

- si  $x \notin \{x_1, x_2, x_3\}$ . Alors  $\sigma(x) = x$  et  $\tau(x) \notin \{\tau(x_1), \tau(x_2), \tau(x_3)\}$ .

$$\text{Donc } \sigma'(\tau(x)) = \tau(x).$$

$$\text{Donc, } \sigma'' \circ \tau(x) = \tau \circ \sigma(x) \Rightarrow \sigma''(x) = \tau \circ \sigma \circ \tau^{-1}(x)$$

$$\Leftrightarrow \sigma \text{ conjugué 3 cycles.}$$

- si  $x \in \{x_1, x_2, x_3\}$  alors,  $x = x_k, k \in \{1, 2, 3\}$ .

$$\text{Donc } \tau(\sigma(x)) = \tau(\sigma(x_k)) = \tau(x_{k+1}) \text{ et } \sigma''(\tau(x_k)) = \tau(x_{k+1})$$

$$\text{Donc } \tau \circ \sigma(x) = \sigma'' \circ \tau(x) \Rightarrow \sigma \text{ conjugué 3 cycles.}$$

Conclusion : 3 cycles conjugués à un 3 cycles □

- $|A_n| = \frac{n!}{2}$  car  $[S_n : A_n] = 2$  et  $|S_n| = n!$

- Question colle:

Autre groupe simple:  $\mathbb{Z}/p\mathbb{Z}$  avec  $p$  premier.  $SO_3(\mathbb{R})$   
R.g.:  $SL_n(\mathbb{C}) \triangleleft GL_n(\mathbb{C})$

**Théorème de Cauchy** — Soit  $G$  un groupe fini d'ordre  $n$ , et  $p$  un nombre premier qui divise  $n$ . Alors il existe (au moins) un élément de  $G$  d'ordre  $p$

La démonstration de McKay<sup>2</sup> est détaillée sur Wikiversité<sup>3</sup>.

#### Démonstration

[masquer]

On fait agir le groupe  $\mathbb{Z}/p\mathbb{Z}$  par permutation circulaire sur l'ensemble

$$E = \{(x_1, \dots, x_p) \in G^p, x_1 \dots x_p = e\}$$

où  $e$  désigne l'élément neutre du groupe  $G$ . L'équation aux classes affirme que  $\# E$  est la somme des cardinaux des orbites pour l'action de  $\mathbb{Z}/p\mathbb{Z}$ .

Or  $\# E = (\# G)^{p-1}$  car étant donné  $x_1, \dots, x_{p-1}$  quelconque  $x_p$  est totalement déterminé (et vaut  $x_{p-1}^{-1} \dots x_1^{-1}$ ).

Ainsi  $\# E$  est un multiple de  $p$ . Le cardinal d'une orbite est égal à l'indice du stabilisateur d'un de ses éléments. Or le groupe  $\mathbb{Z}/p\mathbb{Z}$  ayant pour cardinal un nombre premier, l'indice d'un stabilisateur vaut soit 1 soit  $p$ . L'équation aux classes permet alors de conclure que le nombre de stabilisateurs d'indice 1 est un multiple de  $p$ . Or ce multiple n'est pas nul puisque le stabilisateur de  $(e, \dots, e)$  est lui-même d'indice 1. On en conclut qu'il existe au moins  $p-1$  éléments de  $E$  dont le stabilisateur est d'indice 1 autrement dit qui sont invariants par permutation circulaire. Si  $(x, \dots, x)$  est un tel élément on aura  $x^p = e$ .

Thm:

Si  $n \geq 5$ , Alors  $\mathcal{A}n$  est simple.

Lemme (1):

Si  $n \geq 3$ ,  $\mathcal{A}n$  est engendré par les 3-cycles.

Lemme (2):

Si  $n \geq 5$ , Alors les 3-cycles sont conjugués dans  $\mathcal{A}n$ .

Démon: (1)

Notons  $G = \langle \text{3-cycles} \rangle$ .On a bien  $G \subset \mathcal{A}n$ .Soit  $\sigma \in \mathcal{A}n$ , alors  $\sigma$  s'écrit comme le produit d'un nombre pair de transposition.Or  $\forall i, j, k, \ell \in \llbracket 1, n \rrbracket$  distincts,

$$(ij)(ik) = (ikj) \quad \text{et} \quad (ij)(k\ell) = (ijk)(j\ell k)$$

Done, le produit de 2 transpo. distincts est un produit de 3-cycles.

Par conséquent,  $\sigma$  s'écrit comme un produit de 3-cycles.Ainsi,  $\sigma \in G$ . D'où  $G = \mathcal{A}n$ .  $\square$ 

Démon: (2)

Les 3-cycles sont une classe de conjugaison dans  $S_n$ .Prenons,  $(abc)$  et  $(def) \in \mathcal{A}n$ .Done,  $\exists \sigma \in S_n$  t.q.  $\sigma(abc)\sigma^{-1} = (def)$  $\rightarrow$  si  $\sigma \in \mathcal{A}n$ : c'est fini. $\rightarrow$  sinon: comme  $n \geq 5$ ,  $\exists i, j \notin \{a, b, c\}$  distincts.On pose  $\sigma' = \sigma(ij) \in \mathcal{A}n$  et  $\sigma'(abc)\sigma'^{-1} = (def)$  $\square$ 

Démon: (thm)

Soit  $H \triangleleft \mathcal{A}n$  et  $H \neq \{\text{id}\}$ .M.q.  $H = \mathcal{A}n$ .Soit  $\sigma \in H \setminus \{\text{id}\}$ Alors,  $\exists a, b \in \llbracket 1, n \rrbracket$  distincts t.q.  $\sigma(a) = b$ .Comme  $n \geq 5$ , alors,  $\exists c \notin \{a, b, \sigma(b)\}$ .Posons,  $\tau = (abc)$  et  $\sigma_2 = \underbrace{\sigma \tau}_{\in H} \underbrace{\sigma^{-1} \tau^{-1}}_{\in H} \in H$ 

De plus,

$$\begin{aligned} \sigma_2 &= \sigma(abc) \sigma^{-1} (abc)^{-1} \\ &= (\sigma(a) \sigma(b) \sigma(c)) (abc)^{-1} \\ &= (b \sigma(b) \sigma(c)) (abc)^{-1} \end{aligned}$$

Done, support de  $\sigma_2$  a au plus 5élé., et  $E(\sigma_2) = 1$ .Done,  $\sigma_2$  vaut: $\rightarrow \sigma_2 = \text{id} \Leftrightarrow \sigma \tau = \tau \sigma$  impossible car  $\sigma \tau(a) = \sigma(b) \neq c = \tau(b)$  $\rightarrow \sigma_2 = \text{3-cycle} \Rightarrow H$  possède un 3-cycle. OK $\rightarrow \sigma_2 = (**)(**)$  à supp disjoint:  $\sigma_2 = (ij)(\ell k)$ Prenons  $m \notin \{i, j, k, \ell\}$ 

$$\begin{aligned} \sigma_3 &= \sigma_2 (ijm) \sigma_2^{-1} (imj) = (jim)(imj) \\ &= (ijm) \in H \quad \text{OK} \end{aligned}$$

 $\rightarrow \sigma_2$  5-cycle:  $\sigma_2 = (ijklm)$ 

$$\begin{aligned} \text{On pose } \sigma_3 &= \sigma_2 (ijk) \sigma_2^{-1} (ikj) \sigma_2^{-1} \\ &= (ijk)(jpk) \\ &= (ij\ell) \in H. \end{aligned}$$

 $\square$