Développement: simplicité du groupe alterné

Adrien Fontaine

28 octobre 2012

Théorème 1

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

On utilise pour démontrer ce résultat, quelques propriétés des p-sous-groupes de Sylow, notamment le fait qu'ils soient tous conjugués entre eux. Ce théorème et bien d'autres seront rappelés dans la partie 4 de cette leçon qui y est consacrée.
On aura besoin dans la démonstration du résultat suivant :

Proposition 1

Les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$.

Démonstration : Ceci découle du résultat suivant :

Lemme 1

Soient $n \geq 3$, $(a_1, ..., a_{n-2}) \in \{1, ..., n\}$ deux à deux distincts, et $(b_1, ..., b_{n-2}) \in \{1, ..., n\}$ deux à deux distincts. Alors il existe $\sigma \in \mathfrak{A}_n$ telle que

$$\forall i \in \{1, ..., n-2\}, \sigma(a_i) = b_i$$

Démonstration : Soit $(a_{n-1}, a_n) \in \{1, ..., n\}$ et $(b_{n-1}, b_n) \in \{1, ..., n\}$ tels que $\{a_1, ..., a_n\} = \{1, ..., n\}$ et $\{b_1, ..., b_n\} = \{1, ..., n\}$. On considère alors $\sigma \in \mathfrak{S}_n$ tel que $\forall i \in \{1, ..., n\}, \sigma(a_i) = b_i$. Si, $\varepsilon(\sigma) = 1$ alors c'est terminé. Sinon, on compose σ par (a_{n-1}, a_n) (ce qui ne change pas les images des $(a_i)_{1 \leq i \leq n-2}$ mais multiplie la signature par -1). ■

On a également besoin de la proposition suivante :

Proposition 2

Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1...a_p)$ et si $\tau \in \mathfrak{S}_n$, on a :

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

Démonstration : Si $x \notin \{\tau(a_1), ..., \tau(a_p)\}$, $\tau^{-1}(x) \notin \{a_1, ..., a_p\}$ et donc :

$$\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$$

Et si $x = \tau(a_i)$, $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$, d'où,

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

■

On peut maintenant montrer que les $3-$ *cycles* sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$. Soient $\rho = (a_1 a_2 a_3)$ et $\tau = (b_1 b_2 b_3)$ deux 3-cycles dans $\mathfrak{A}_n$. Comme $n-2 \geq 3$, il existe une permutation $\sigma \in \mathfrak{A}_n$ telle que $\forall 1 \leq i \leq 3, \sigma(a_i) = b_i$, et donc $\tau = \sigma\rho\sigma^{-1}$ d'après la proposition. ■

Enfin, on utilise également le résultat suivant :

Proposition 3

Les cycles d'ordre 3 *engendrent* $\mathfrak{A}_n$ *pour* $n \geq 3$

Démonstration : En effet, $\mathfrak{A}_n$ est engendré par les produits pairs de transpositions et on a les formules :

$$(a,b)(b,c) = (a,b,c)$$
$$(a,b)(a,c) = (a,c,b)$$
$$(a,b)(c,d) = (a,b)(a,c)(a,c)(c,d) = (a,c,b)(a,c,d)$$

■

On est maintenant en mesure de démontrer le théorème :

Théorème 2

Le groupe $\mathfrak{A}_n$ *est simple pour* $n \geq 5$.

Démonstration : La démonstration se fait en 2 étapes. D'abord pour $n = 5$ puis pour $n > 5$ par réduction au cas $n = 5$.

1. Le théorème pour n=5
   Décrivons les éléments de $\mathfrak{A}_5$:
   - Tout d'abord il y a le neutre, soit 1 élément.
   - Ensuite il y a les éléments d'ordre 3, ce sont les 3-cycles. Pour déterminer un 3-cycle, il faut choisir les deux points fixes, ce qui nous fait $\binom{2}{5} = 10$ possibilités, puis on détermine l'image des 3 points qui ne sont pas fixes par la permutation. Or une fois fixée l'image d'un élément, les images des deux autres sont automatiquement déterminées. On a donc deux possibilités pour les images des points du 3-cycle qui ne sont pas fixes. Soit au total, $10 \times 2 = 20$ 3-cycles.
   - Ensuite il y a les éléments d'ordre 5, ce sont les 5-cycles. Cette fois-ci, il n'y a pas de point fixe et il suffit de déterminer les images des points de la permutation. Pour 1, on a 4 possibilités $(2,3,4,5)$ puis pour 2, on a 3 possibilités (tout sauf 2 lui même et l'image de 1 qui est déjà prise, et ainsi de suite. Au total, on a donc $4 \times 3 \times 2 = 24$ 5-cycles
   - Enfin, on a les produits de deux transpositions à supports disjoints. Ce sont les éléments d'ordre 2. Pour déterminer, une telle permutation, il faut se donner un point fixe (5 possibilités) et un choix de 2 éléments parmi les 4 restants qui correspondent à une des deux permutations (l'autre étant alors automatiquement déterminée), soit $\binom{2}{4} = 6$ possibilités. Mais attention, en procédant ainsi, on compte deux fois certains éléments : en effet, si on choisit par exemple 1 et 2 dans $\{1,2,3,4\}$ et qu'ensuite on choisit 3 et 4, on considère en fait la même permutation qui est : $(12)(34) = (34)(12)$. Il faut donc penser à diviser par 2 pour obtenir le nombre de permutations d'ordre 2. Finalement, on a donc $5 \times 6/2 = 15$ possibilités.

   On a donc dénombrer $1 + 20 + 24 + 15 = 60$ éléments de $\mathfrak{A}_5$ et $\mid \mathfrak{A}_5 \mid = 60$ donc on a bien décrit tous les éléments de $\mathfrak{A}_5$.
   De plus, les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_5$ d'après la proposition 1. Les éléments d'ordre 2 le sont aussi : si $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$, il existe $\sigma \in \mathfrak{A}_5$ tel que

$\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ d'après le lemme 1. Alors :

$$\begin{aligned}\sigma\tau\sigma^{-1} &= \sigma(ab)(cd)(e)\sigma^{-1}\\ &= \sigma(ab)\sigma^{-1}\sigma(cd)\sigma^{-1}\sigma(e)\sigma^{-1}\\ &= (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))(\sigma(e))\\ &= (a'b')(\sigma(c)\sigma(d))(e')\\ &= (a'b')(c'd')(e')\\ &= \tau'\end{aligned}$$

Soit alors $H \triangleleft \mathfrak{A}_5$, $H \neq \{1\}$. Si H contient un élément d'ordre 3 (resp. 2), alors H étant distingué, il les contient tous puisqu'ils sont tous conjugués. Si il contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc tous les 5-sous-groupes de Sylow puisqu'ils sont tous conjugués, donc H contient tous les éléments d'ordre 5.
Mais H ne peut contenir un seul des trois types d'éléments précédents (en plus du neutre) car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ divisent 60 (le cardinale de H divise $\mid \mathfrak{A}_5 \mid = 60$ d'après le théorème de Lagrange). Donc, H contient au moins un des trois types, d'où $\mid H \mid \geq 15 + 20 + 1 = 36$. D'où, $\mid H \mid = 60$ et $H = \mathfrak{A}_5$.

2. Le théorème pour $n > 5$
Posons $E = \{1, ..., n\}$. Soit $H \triangleleft \mathfrak{A}_n$, $H \neq 1$ et soit $\sigma \in H, \sigma \neq 1$. On va se ramener au cas $n = 5$ 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.
Comme $\sigma \neq 1$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$, et soit τ le 3-cycle $\tau = (a, c, b)$, de sorte que $\tau^{-1} = (a, b, c)$ et soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. On a :

$$\rho = \underbrace{(\tau\sigma\tau^{-1})}_{\in H}\sigma^{-1} \in H$$

Et $\rho = (a, c, b)(\sigma(a), \sigma(b), \sigma(c))$.
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 $\rho_{|E\setminus F} = Id_{E\setminus F}$.
Quitte à rajouter des éléments à F, on peut supposer $\mid F \mid = 5$. Enfin, $\rho \neq 1$ car $\rho(b) = \tau(\sigma(b)) \neq b$ car $\sigma(b) \neq \tau^{-1}(b) = c$.
Soit alors $\mathfrak{A}(F)$ l'ensemble des permutations paires de F. $\mathfrak{A}(F)$ est isomorphe à $\mathfrak{A}_5$ et $\mathfrak{A}(F)$ se plonge dans $\mathfrak{A}_n$ par :

$$\begin{array}{rccc}\Phi & : & \mathfrak{A}(F) & \to & \mathfrak{A}_n\\ & & u & \mapsto & \bar{u}\end{array}$$

où $\bar{u}_{|F} = u$ et $\bar{u}_{|E\setminus F} = Id_{E\setminus F}$.
Posons, $H_0 = \{u \in \mathfrak{A}(F) / \bar{u} \in H\} = H \cap \mathfrak{A}(F)$.
Il est clair que $H_0 \triangleleft \mathfrak{A}(F)$ et on a $\rho_{|F} \in H_0$ et $\rho_{|F} \neq Id_F$. Comme $\mathfrak{A}(F) \cong \mathfrak{A}_5$ est simple, on a $H_0 = \mathfrak{A}(F)$. Ainsi, si u est un cycle d'ordre 3 de $\mathfrak{A}(F)$, $\bar{u} \in H$ et $\bar{u}$ est encore un cycle d'ordre 3. Mais comme les 3 cycles sont tous conjugués dans $\mathfrak{A}_n$, H contient tous les 3-cycles, et comme ils engendrent $\mathfrak{A}_n$, on a $H = \mathfrak{A}_n$.
Ce qui achève la démonstration. ■