DÉVELOPPEMENT 32

$\mathcal{A}_5$ EST LE SEUL GROUPE SIMPLE D'ORDRE 60

Proposition. — *Si G est un groupe simple d'ordre 60 alors G est isomorphe à $\mathcal{A}_5$.*

Démonstration. — On considère un groupe G d'ordre $60 = 2^2 \cdot 3 \cdot 5$ et on note n_5 le nombre de 5-Sylow de G. Puisque n_5 divise $2^2 \cdot 3 = 12$ et est congru à 1 modulo 5, on a $n_5 = 1$ ou 6. Si $n_5 = 1$ alors l'unique 5-Sylow de G est distingué dans G ce qui est impossible puisque G est simple donc $n_5 = 6$.

On note $\mathcal{E}_5$ l'ensemble des 5-Sylow de G. Les six 5-Sylow de G sont conjugués deux à deux donc G agit (de façon transitive) par automorphismes intérieurs sur l'ensemble $\mathcal{E}_5$ *i.e.* on a un morphisme non trivial $G \to \mathcal{S}(\mathcal{E}_5) \simeq \mathcal{S}_6$. Comme G est simple, ce morphisme est injectif (sinon le noyau serait un sous-groupe distingué de G) *i.e.* l'action est fidl̀e ; on en déduit que G est isomorphe à un sous-groupe H de $\mathcal{S}_6$.

Ce groupe H est simple d'ordre non premier (puisque c'est le cas de G) donc H n'est pas abélien or $D(H)$ est distingué dans H donc $H = D(H)$. Mais le fait que $H \subseteq \mathcal{S}_6$ implique que $D(H) \subseteq D(\mathcal{S}_6)$ or un commutateur de $\mathcal{S}_6$ est une permutation paire (car de la forme $xyx^{-1}y^{-1}$) *i.e.* $D(\mathcal{S}_6) \subseteq \mathcal{A}_6$ et on a donc $H \subseteq \mathcal{A}_6$.

Les 5-cycles de $\mathcal{A}_6$ engendrent les 5-Sylow de $\mathcal{A}_6$ (puisque ces 5-Sylow sont de la forme $\mathbb{Z}/5\mathbb{Z}$) or ces 5-Sylow sont conjugués dans $\mathcal{A}_6$. D'autre part, H contient un de ces 5-Sylow donc contient un 5-cycle. Puisque $\mathcal{A}_6$ contient $\mathrm{C}_6^5 4! = 144$ 5-cycles alors que H est d'ordre 60, c'est donc que H n'est pas distingué dans $\mathcal{A}_6$.

On note $(\mathcal{A}_6/H)_g$ l'ensemble des classes à gauche de $\mathcal{A}_6$ modulo H. Alors $\mathcal{A}_6$ agit par translation à gauche sur ces classes *i.e.* l'action est donnée par

$$y \cdot (xH) = (yx) \cdot H$$

et cette action induit une action de H sur $(\mathcal{A}_6/H)_g$ *i.e.* un morphisme $\phi : H \to \mathcal{S}((\mathcal{A}_6/H)_g)$. Supposons que le morphisme ϕ soit trivial *i.e.* $\phi(h) = \mathrm{id}$ pour tout $h \in H$, on a alors $h \cdot (xH) = xH$ pour tout $h \in H$ et tout $x \in \mathcal{A}_6$. La relation $h \cdot (xH) = xH$ signifie que $(hx)H = xH$ *i.e.* $hx \in xH$ d'où $xHx^{-1} = h$. On a donc $xHx^{-1} = H$ pour tout $x \in \mathcal{A}_6$ ce qui est impossible puisque H n'est pas distingué dans $\mathcal{A}_6$. Puisque H est simple et puisque le morphisme ϕ n'est pas trivial, le noyau de ϕ est réduit à 1_H *i.e.* l'action est fidèle donc $H \simeq \phi(H)$.

Notons que $h \cdot H = H$ pour tout $h \in H$ *i.e.* toute permutation $\sigma_h \in \phi(H)$ admet H pour point fixe. Comme $\mathcal{S}((\mathcal{A}_6/H)_g) \simeq \mathcal{S}_6$ (car H et $\mathcal{A}_6$ sont respectivement d'ordre 60 et 360), $\phi(H)$ est isomorphe à un sous-groupe de $\mathcal{S}_6$ dont les éléments ont un point fixe en commun donc $\phi(H)$ est isomorphe à un sous-groupe de $\mathcal{S}_5$.

Il découle de ce qui précède que G est isomorphe à un sous-groupe de $\mathcal{S}_5$. Mais G est d'ordre 60 donc est un sous-groupe d'indice 2 de $\mathcal{S}_5$ *i.e.* $G \simeq \mathcal{A}_5$. □

Leçons concernées

02 Groupes opérant sur un ensemble. Exemples et applications

04 Sous-groupes distingués, groupes quotients. Exemples et applications

05 Groupes finis. Exemples et applications

06 Groupe des permutations d'un ensemble fini. Applications

Compléments

Autre démonstration. —
Soit G un groupe simple d'ordre $60 = 2^2 \cdot 3 \cdot 5$ dont on note respectivement n_2, n_3 et n_5 le nombre des 2-Sylow, 3-Sylow et 5-Sylow ; on veut montrer que $n_2 = 5$.

- On sait que n_5 divise $2^2 \cdot 3 = 12$ et est congru à 1 modulo 5 donc $n_5 = 1$ ou 6. Si $n_5 = 1$ alors l'unique 5-Sylow est un sous-groupe distingué de G ce qui est impossible puisque G est simple donc $n_5 = 6$. Notons que ces 5-Sylow sont engendrés par chacun de leurs éléments non nuls, il en résulte que l'intersection de deux 5-Sylow distincts est triviale donc qu'il y a $24 = 4 \times 6$ éléments d'ordre 5 dans G.
- On sait que n_3 divise $2^2 \cdot 5 = 20$ et est congru à 1 modulo 3 donc $n_3 = 1, 4$ ou 10.
  - Si $n_3 = 1$ alors l'unique 3-Sylow est un sous-groupe distingué de G ce qui est impossible puisque G est simple.
  - Si $n_3 = 4$ alors les quatre 3-Sylow de G sont conjugués deux à deux donc G agit (de façon transitive) par automorphismes intérieurs sur l'ensemble $\mathcal{E}_3$ des 3-Sylow de G ; comme $\mathcal{E}_3$ est de cardinal 4, on a donc un morphisme non trivial $G \to S_4$ qui est injectif puisque G est simple (sinon le noyau serait un sous-groupe distingué de G) *i.e.* G est isomorphe à un sous-groupe de S_4 ce qui est impossible puisque $|G| = 60$ alors que $|S_4| = 24$.

  On a donc $n_3 = 10$. Notons que ces 3-Sylow sont engendrés par chacun de leurs éléments non nuls, il en résulte que l'intersection de deux 3-Sylow distincts est triviale donc qu'il y a $20 = 2 \times 10$ éléments d'ordre 3 dans G.
- On sait que n_2 divise $3 \cdot 5 = 15$ et est congru à 1 modulo 2 donc $n_2 = 1, 3, 5$ ou 15.
  - Si $n_2 = 1$ alors l'unique 2-Sylow est un sous-groupe distingué de G ce qui est impossible puisque G est simple.
  - Si $n_2 = 3$ alors les trois 2-Sylow de G sont conjugués deux à deux donc G agit (de façon transitive) par automorphismes intérieurs sur l'ensemble $\mathcal{E}_2$ des 2-Sylow de G ; comme $\mathcal{E}_2$ est de cardinal 3, on a donc un morphisme non trivial $G \to S_3$ qui est injectif puisque G est simple *i.e.* G est isomorphe à un sous-groupe de S_3 ce qui est impossible puisque $|G| = 60$ alors que $|S_3| = 6$.
  - Supposons que $n_2 = 15$, puisque G contient 20 éléments d'ordre 3 et 24 éléments d'ordre 5, G ne peut pas contenir plus de 15 éléments d'ordre 2 ou 4, il en résulte que les 2-Sylow ne sont pas distincts *i.e.* il existe deux 2-Sylow S et S' d'intersection non triviale. On note Γ le sous-groupe de G engendré par S et S' : son ordre divise 60, est un multiple de 4 (puisque Γ contient le 2-Sylow S) et est strictement supérieur à 4 (puisque Γ contient deux 2-Sylow distincts). L'ordre de Γ est donc $12, 20$ ou 60.
    - ◇ Supposons que $\Gamma = G$ alors, si on note $S \cap S' = \{1, u\}$, l'élément u commute avec tous les éléments de G *i.e.* $S \cap S'$ est un sous-groupe distingué de G ce qui est impossible puisque G est simple.
    - ◇ Si $|\Gamma| = 20$ alors le nombre de 5-Sylow de Γ divise 4 et est congru à 1 modulo 5 donc Γ admet un unique 5-Sylow H qui est donc distingué dans Γ. Pour tout $g \in \Gamma$, on a donc $gHg^{-1} = H$ et il s'ensuit que Γ est contenu dans le normalisateur $N_G(H)$ de H dans G. Considérons l'action de G par conjugaison sur l'ensemble des parties de G alors l'orbite de H est l'ensemble des 5-Sylow de G donc est de cardinal 6 et le stabilisateur de H est $N_G(H)$, par conséquent, $N_G(H)$ est d'ordre $\frac{60}{6} = 10$. Cela contredit le fait que $N_G(H)$ contienne Γ.
    - ◇ Si $|\Gamma| = 12 = 2^2 \cdot 3$ alors on note respectivement m_2 et m_3 les nombres de 2-Sylow et de 3-Sylow de Γ. On sait que m_3 divise 4 et est congru à 1 modulo 3 donc $m_3 = 1$ ou 4 ; de même, m_2 divise 3 et est congru à 1 modulo 2 donc $m_2 = 1$ ou 3. Puisque Γ contient S et S' qui sont deux 2-Sylow, on a $m_2 = 3$ et on note S'' le troisème 2-Sylow. Si on note $S \cap S' = \{1, u\}$ alors l'élément u commute avec tous les éléments de Γ or S et S'' sont conjugués donc $u \in S''$. Les

éléments non nuls de Γ sont d'ordre $2, 3$ ou 4 ; comme il y a 2 (si $m_3 = 1$) ou 8 (si $m_3 = 4$) éléments d'ordre 3, il y a donc 9 ou 3 éléments d'ordre 2 ou 4. Mais les éléments de Γ d'ordre 2 ou 4 sont les éléments non nuls de $S \cup S' \cup S''$ *i.e.* (puisque $u \cap S \cap S' \cap S''$) il y en a 7 et on a donc une contradiction.

Il en résulte que $n_2 = 5$.

Le groupe G agit (transitivement) par conjugaison sur l'ensemble des cinq 2-Sylow de G, on a donc un morphisme de G dans S_5 qui est injectif puisque G est simple. Ainsi, G est isomorphe à un groupe d'indice 2 dans S_5 *i.e.* $G \simeq A_5$.

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

Lemme. — *Soit $\gamma = (i_1 \ \cdots \ i_k)$ un k-cycle et $\sigma \in \mathcal{S}_n$, alors $\sigma\gamma\sigma^{-1} = (\sigma(i_1) \ \cdots \sigma(i_k))$ et tout k-cycle est un conjugué de γ.*

Démonstration. — Notons $\gamma' = (\sigma(i_1) \ \cdots \sigma(i_k))$ et $A = \{i_1, \ldots, i_k\}$, on note de plus $i_{k+1} = i_1$. Soit $p \in \{1, \ldots, n\}$ alors

– si $p = \sigma(i_j)$ alors $\sigma\gamma\sigma^{-1}(p) = \sigma\gamma(i_j) = \sigma(i_{j+1}) = \gamma'(\sigma(i_j))$

– sinon $\sigma^{-1}(p) \notin A$ donc $\sigma\gamma\sigma^{-1}(p) = \sigma\gamma\sigma^{-1}(p) = p$

d'où $\sigma\gamma\sigma^{-1} = \gamma'$. Considérons maintenant un k-cycle $\rho = (j_1 \ \cdots \ j_k)$ et $B = \{j_1, \ldots, j_k\}$. Les complémentaires $\overline{A}$ de A et $\overline{B}$ de B ont même cardinal $n - k$ donc il existe une bijection σ de $\overline{A}$ sur $\overline{B}$; on pose de plus $\sigma(i_r) = j_r$ pour $1 \leq r \leq n$ alors $\sigma \in \mathcal{S}_n$ et on a $\sigma\gamma\sigma^{-1} = \rho$. □

Lemme. — *Si $n \geq 3$ alors $\mathcal{A}_n$ est engendré par les cycles $(i \ i+1 \ i+2)$ pour $1 \leq i \leq n+2$.*

Démonstration. — Les transpositions $(i \ i+1)$ engendrent $\mathcal{S}_n$ donc les produits d'un nombre pair de transpositions du type $(i \ i+1)$ engendrent $\mathcal{A}_n$. Il s'agit de montrer que tout produit $\sigma = (i \ i+1)(j \ j+1)$ est dans le sous-groupe H de $\mathcal{S}_n$ engendré par les cycles $(i \ i+1 \ i+2)$. Considérons un tel élément $\sigma = (i \ i+1)(j \ j+1)$ avec (quitte à considérer σ^{-1}) $i \leq j$ et raisonnons par récurrence sur l'entier $k = j - i$:

– si $k = 0$ alors $\sigma = (i \ i+1)(i \ i+1) = \mathrm{id} \in H$

– si $k = 1$ alors $\sigma = (i \ i+1)(i+1 \ i+2) = (i \ i+1 \ i+2) \in H$

– on suppose le résultat vrai au rang $k - 1$ alors

$$\sigma = (i \ i+1)(i+1 \ i+2)(i+1 \ i+2)(j \ j+1) = (i \ i+1 \ i+2)(i+1 \ i+2)(j \ j+1)$$

et l'hypothèse de récurrence donne $(i+1 \ i+2)(j \ j+1) \in H$, d'où $\sigma \in H$.

On a donc bien $H = \mathcal{A}_n$. □

Lemme. — *Les double-transpositions sont conjuguées dans $\mathcal{A}_5$.*

Démonstration. — Soit $\tau = (a \ b)(c \ d)(e)$ et $\tau' = (a' \ b')(c' \ d')(e)$ et σ un élément de $\mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma(\{c; d\}) = \{c; d\}$ et on a $\tau' = \sigma\tau\sigma^{-1}$. □

Dans ce qui suit, on considère un entier $n \geq 5$.

Lemme. — *Les 3-cycles sont conjugués dans $\mathcal{A}_n$.*

Démonstration. — Considérons un 3-cycle $\gamma = (1 \ 2 \ 3)$ alors il existe $\sigma \in \mathcal{S}_n$ tel que $\sigma\gamma\sigma^{-1} = (1 \ 2 \ 3)$. Si $\sigma \notin \mathcal{A}_n$ alors $(4 \ 5)\sigma \in \mathcal{A}_n$ et $((4 \ 5)\sigma)\gamma((4 \ 5)\sigma)^{-1} = (4 \ 5)\sigma\gamma\sigma^{-1}(4 \ 5) = (4 \ 5)(1 \ 2 \ 3)(4 \ 5) = (1 \ 2 \ 3)$. □

Proposition. — *$\mathcal{A}_n$ est simple.*

Démonstration sans les théorèmes de Sylow. — On considère un sous-groupe distingué H de $\mathcal{A}_n$ avec $H \neq \{\text{id}\}$. Il existe donc $\sigma \in H$ et $k \in \{1, \dots, n\}$ tels que $\sigma(k) \neq k$. On note $\ell = \sigma(k)$, on choisit $m \in \{1, \dots, n\} \setminus \{k, \ell, \sigma(\ell)\}$ et on pose $\gamma = (k\ m\ \ell)$ et $\rho = [\sigma, \gamma] = \sigma\gamma\sigma^{-1}\gamma^{-1}$. On a $\sigma \in H$ donc $\sigma^{-1} \in H$ or H est distingué dans $\mathcal{A}_n$ donc $\gamma\sigma^{-1}\gamma^{-1} \in H$ et il s'ensuit que $\rho \in H$.

On a $\sigma\gamma(\ell) = \sigma(k) = \ell$ mais, d'autre part, $m \neq \sigma(\ell)$ et γ est injectif donc $\ell = \gamma(m) \neq \gamma\sigma(\ell)$. On a donc $\sigma\gamma \neq \gamma\sigma$ *i.e.* $\rho \neq \text{id}$.

Puisque $\ell = \sigma(k)$, l'ensemble $X = \{k, \ell, m, \sigma(k), \sigma(\ell), \sigma(m)\}$ a au plus 5 éléments. Soit $a \notin X$ alors $\gamma^{-1}(a) = a$ et $\sigma^{-1}(a) \notin \{k, \ell, m\}$ donc $\gamma\sigma^{-1}(a) = \sigma^{-1}(a)$ et on a donc

$$\rho(a) = \sigma\gamma\sigma^{-1}\gamma^{-1}(a) = \sigma\gamma\sigma^{-1}(a) = \sigma\sigma^{-1}(a) = a$$

i.e. ρ laisse fixes au moins $n - 5$ points.

Si l'on décompose ρ en cycles disjoints alors ces cycles sont à support dans X donc ρ est soit un 3-cycle, soit un 5-cycle, soit un produit de deux transpositions *i.e.* ρ est de l'une des formes $\rho_1 = (x\ y\ z)$, $\rho_2 = (x\ y\ z\ t\ w)$ ou $\rho_3 = (x\ y)(z\ t)$. Dans les deux premiers cas, on pose $\tau = (x\ y)$ alors

$$[\tau\ \rho] = (x\ y)\rho(x\ y)^{-1}\rho = (x\ y)(\rho(x)\ \rho(y)) = (x\ y)(y\ \rho(y)) = (x\ y\ \rho(y))$$

et dans le troisième cas, on choisit $w \notin \{x, y, z, t\}$ et on pose $\tau = (x\ w)$ alors

$$[\tau\ \rho] = (x\ w)\rho_3(x\ w)^{-1}\rho_3 = (x\ w)(\rho_3(x)\ \rho_3(w)) = (x\ w)(y\ w) = (x\ w\ y).$$

Dans tous les cas, on a bien montré que H contient un 3-cycle.

Les 3-cycles sont conjugués dans $\mathcal{A}_n$ or H est un sous-groupe distingué de $\mathcal{A}_n$ qui contient un 3-cycle donc H contient le sous-groupe de $\mathcal{S}_n$ engendré par les 3-cycles *i.e.* $H = \mathcal{A}_n$. □

Démonstration pour $n = 5$. — $\mathcal{A}_5$ contient l'identité, 15 double-transpositions, 20 3-cycles et 24 5-cycles or les double-transpositions sont conjuguées dans $\mathcal{A}_5$, de même que les 3-cycles donc si un sous-groupe distingué H de $\mathcal{A}_5$ contient une double-transposition alors il les contient toutes, de même pour les 3-cycles ; en raisonnant sur les 5-Sylow, on voit que si H contient un 5-cycles alors il les contient tous. En comptant les éléments de H, on vérifie que $H = \{\text{id}\}$ ou $\mathcal{A}_5$. □

Corollaire. — $D(\mathcal{A}_n) = D(\mathcal{S}_n) = \mathcal{A}_n$

Démonstration. — C'est clair puisque $D(\mathcal{A}_n) \subseteq D(\mathcal{S}_n) \subseteq \mathcal{A}_n$ avec $\mathcal{A}_n$ simple non abélien. On peut le montrer directement en remarquant que $\sigma = (a\ b\ c)$ et σ^2 sont deux 3-cycles donc sont conjugués dans $\mathcal{A}_n$ *i.e.* il existe $\rho \in \mathcal{A}_n$ tel que $\sigma^2 = \rho\sigma\rho^{-1}$ *i.e.* $\sigma = \rho\sigma\rho^{-1}\sigma^{-1}$ ce qui signifie que tout 3-cycle est un commutateur de $\mathcal{A}_n$ et le résultat découle alors du fait que les 3-cycles engendrent $\mathcal{A}_n$. □

"Trous" dans la démonstration. —

Lemme. — *$D(G)$ est un sous-groupe distingué de G.*

Démonstration. — Soit $z \in G$ et $[x, y]$ un générateur de $D(G)$. Alors

$$z[x,y]z^{-1} = z(xyx^{-1}y^{-1})z^{-1} = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} = [zxz^{-1}, zyz^{-1}].$$

□

Lemme. — *$\mathcal{A}_n$ est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$.*

Démonstration. — Si H est un sous-groupe d'indice 2 de $\mathcal{S}_n$ alors H est distingué dans $\mathcal{S}_n$ et on a donc une surjection canonique $\pi : \mathcal{S}_n \to \mathcal{S}_n/H$ et un isomorphisme $\psi : \mathcal{S}_n/H \to \{\pm 1\}$. Alors $\theta = \pi \circ \psi$ est un morphisme surjectif de $\mathcal{S}_n$ sur $\{\pm 1\}$. Puisque les transpositions engendrent $\mathcal{S}_n$ et puisque θ est surjective, il existe une transposition τ telle que $\theta(\tau) = -1$. Soit τ' une autre transposition alors il existe $\sigma \in \mathcal{S}_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$ d'où $\theta(\tau') = \theta(\sigma)\theta(\tau)\theta(\sigma)^{-1} = \theta(\tau) = -1$. Ainsi, pour tout $\rho \in \mathcal{S}_n$, $\theta(\rho) = (-1)^k$ où k est le nombre de termes apparaissant dans une décomposition de ρ en produit de transpositions *i.e.* $\theta = \varepsilon$. Donc $\mathcal{A}_n$ est exactement le noyau de θ *i.e.* $\mathcal{A}_n = H$. □

Références

F. Combes, *Algèbre et géométrie*, Bréal, 1998.

I. Nourdin, *Leçons d'analyse, probabilités, algèbre et géométrie*, Dunod, 2001.

D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

M. Savoyant, *Le groupe simple d'ordre* 60, R.M.S. novembre-décembre 1999.