Le groupe $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60

Théorème
Le groupe $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60.

Lemme
Soient K un groupe et H un sous-groupe de simple de K, non distingué dans K. Si $[K : H] = n$ alors H est isomorphe à un sous-groupe de $\mathfrak{S}_{n-1}$.

Démonstration :
Soit G un groupe simple d'ordre $60 = 5 \times 12$.

- On note n_5 le nombre de 5-Sylow de G. D'après les théorèmes de Sylow on a :

$$\begin{cases} n_5 \equiv 1 \ [5] \\ n_5/12 \end{cases}.$$

  Donc $n_5 = 1$ ou $n_5 = 6$. Si $n_5 = 1$ alors le 5-Sylow est distingué dans G simple : absurde. Donc $n_5 = 6$.

- On note $X = \{H_1, ..., H_6\}$ l'ensemble des 5-Sylow de G. Comme les 5-Sylow sont conjugués on peut faire agir G sur X par conjugaison :

$$\begin{aligned} \varphi : G &\longrightarrow \mathfrak{S}(X) \simeq \mathfrak{S}_6 \\ g &\longmapsto (H_i \mapsto gH_ig^{-1}). \end{aligned}$$

  Montrons que l'action est fidèle. Le groupe $\mathrm{Ker}(\varphi)$ est distingué dans G donc $\mathrm{Ker}(\varphi) = \{e\}$ ou $\mathrm{Ker}(\varphi) = G$. Si $\mathrm{Ker}(\varphi) = G$ alors pour tout $g \in G$ et tout $i \in [\![1, 6]\!]$ on a : $gH_ig^{-1} = H_i$. Ainsi les H_i sont distingués, ce qui contredit le fait que $n_5 = 6$. Donc $\mathrm{Ker}(\varphi) = \{e\}$. Par suite :

$$G \simeq \mathrm{Im}(\varphi) < \mathfrak{S}_6.$$

- Considérons le groupe dérivé $D(G)$ de G, $D(G)$ est distingué dans G donc $D(G) = G$ ou $D(G) = \{e\}$. Si $D(G) = \{e\}$ alors G est abélien, or les seuls groupes abéliens simples sont les groupes cycliques d'ordre premier. Par suite $D(G) = G$. De plus $D(\mathfrak{S}_6) = \mathfrak{A}_6$ donc $D(G) = G$ est isomorphe à un sous-groupe de $\mathfrak{A}_6$.

- Comme $\mathfrak{A}_6$ est simple, G n'est pas distingué dans $\mathfrak{A}_6$. On peut donc appliquer le lemme à $K = \mathfrak{A}_6$ et $H = G$, comme $[\mathfrak{A}_6 : G] = 6$ on en déduit que G est isomorphe à un sous-groupe de $\mathfrak{S}_5$.

- A nouveau $D(\mathfrak{S}_5) = \mathfrak{A}_5$, donc G est isomorphe à un sous-groupe de $\mathfrak{A}_5$ et pour des raisons de cardinalité :

$$G \simeq \mathfrak{A}_5.$$

$\square$

Montrons maintenant le lemme :

Preuve :
On considère l'action de H sur K/H :

$$\begin{aligned}\varphi : H &\longrightarrow \mathfrak{S}(K/H) \simeq \mathfrak{S}_n\\ h &\longmapsto (xH \mapsto hxH).\end{aligned}$$

Comme H est simple on a $\mathrm{Ker}(\varphi) = H$ ou $\mathrm{Ker}(\varphi) = \{e\}$. Si $\mathrm{Ker}(\varphi) = H$ pour tous $h \in H$ et $x \in K$, $hxH = xH$ et

$$\begin{aligned}hxH = xH &\iff hx \in xH\\ &\iff x^{-1}hx \in H.\end{aligned}$$

Donc H est distingué dans K, ce qui contredit l'hypothèse. D'où $\mathrm{Ker}(\varphi) = \{e\}$ et par suite

$$G \simeq \mathrm{Im}(\varphi) < \mathfrak{S}_n.$$

De plus pour tout $h \in H$ on a $\varphi(h)(eH) = eH$. Donc toutes les permutations $\varphi(h)$ laisse fixe l'élément eH : elles ne permutent donc que $n-1$ éléments. On en déduit que G est isomorphe à un sous-groupe de $\mathfrak{S}_{n-1}$. $\square$

Détails supplémentaires

On peut utiliser un résultat plus faible que la simplicit de $\mathfrak{A}_6$:

Lemme
Soit G un sous-groupe d'ordre 60 de $\mathfrak{A}_6$, alors G n'est pas distingué dans G.

Preuve :
On raisonne par l'absurde ; on suppose G distingué dans $\mathfrak{A}_6$. Ainsi G possède un 5-Sylow d'ordre 5 et donc est engendré par un élément b d'ordre 5.
Montrons que G contient tous les éléments d'ordre 5 de $\mathfrak{A}_6$. Soit $a \in \mathfrak{A}_6$ d'ordre 5, comme $|\mathfrak{A}_6| = 5 \times 72$, $\langle a \rangle$ est un 5-Sylow de $\mathfrak{A}_6$. Donc $\langle a \rangle$ et $\langle b \rangle$ sont conjugués dans $\mathfrak{A}_6$. Il existe alors $\tau \in \mathfrak{A}_6$ et $k \in \mathbb{Z}$ tels que $b = \tau a^k \tau^{-1}$ et $b \in G$. Ainsi G contient tous les éléments d'ordre 5 de $\mathfrak{A}_6$. Par la décomposition en produits dde cycle à support disjoint il y a $\binom{6}{5}4! = 144$ éléments d'ordre 5 dans $\mathfrak{A}_6$. Absurde. $\square$

Proposition
Les seuls groupes abéliens simples sont les groupes cycliques premiers.

Démonstration :

- Un groupe cyclique G d'ordre premier est abélien et n'admet pas de sous-groupes non triviaux : c'est donc un groupe simple.

- Si G est un groupe abélien simple, $G \neq \{e\}$ donc il existe $x \neq e \in G$. Le sous-groupe $\langle x \rangle$ étant distingué dans le groupe simple G alors nécessairement $\langle x \rangle = G$. Le groupe G est donc monogène, et puisqu'il est simple, il ne peut-être que cyclique d'ordre premier.

$\square$

Proposition
Pour $n \geq 2$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Démonstration :
On a $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est, dans $\mathfrak{A}_n$ un commutateur. Soit $\sigma = (a, b, c)$ un 3-cycle, $\sigma^2 = (a, c, b)$ en est un autre, donc σ et σ^2 sont conjugués dans $\mathfrak{A}_n$: il existe $\tau \in \mathfrak{A}_n$ telle que $\sigma^2 = \tau\sigma\tau^{-1}$ d'où $\sigma = \tau\sigma\tau^{-1}\sigma^{-1}$. □