A_5 est l'unique groupe simple d'ordre 60

Preuve : - $G \curvearrowright G/_H$ avec $|G/_H| = 5$
- pas de sous-groupe d'indice ≤ 5
- On compte le nbre x tq $o(x) = 2$ ou 4 ; $x+q$ dat ≥ 5
  → compte n_2 dm S_5
- $G \curvearrowright H$ implique $\phi : G \to \mathfrak{S}_5$.

ref: Szpirglas, L3 Algèbre p277

Théorème : Soit G un groupe simple de cardinal 60, alors $G \simeq A_5$.

Pour montrer que G est isomorphe à un sous-groupe de $\mathfrak{S}_5$ on va le faire agir sur un ensemble bien choisi de cardinal de manière à ce que l'action soit fidèle.

Preuve : Soit G un groupe simple d'ordre 60.
On veut faire agir G sur un ensemble de cardinal 5, par exemple $G/_H$ où H est un sous-groupe d'indice 5 (qui n'est pas distingué car G est simple).

Étape 1 : Il existe un sous-groupe de G d'indice ≤ 5.
On ne peut montrer son existence par le théorème de Sylow car il serait d'ordre $12 = 2^2 \cdot 3$. On raisonne donc par l'absurde en supposant :

Il n'existe pas de sous-groupe strict de G d'indice ≤ 5.

On a : $|G| = 60 = 2^2 \cdot 3 \cdot 5$.
On note $S_2(G)$ l'ensemble des 2-Sylows de G et n_2 son cardinal. Par le théorème de Sylow on a :

$$\begin{cases} n_2 \mid 15 \\ n_2 \equiv 1 [2] \end{cases} \quad \text{i.e } n_2 = 1, 3, 5 \text{ ou } 15.$$

On fait agir G par conjugaison sur $S_2(G)$, on sait qu'elle est transitive (les 2-Sylows étant tous conjugués).
Or pour un 2-Sylow quelconque l'indice de son stabilisateur est le cardinal de son orbite donc $[G : \mathrm{Stab}(S)] = n_2$ où $S \in S_2(G)$
Si $n_2 = 1$ alors l'unique 2-Sylow est distingué, ce qui est absurde car G est simple.
Si $n_2 = 3$ ou $n_2 = 5$ alors pour $H \in S_2(G)$ son stabilisateur est un sous-groupe strict d'indice n_2 i.e 3 ou 5 donc ≤ 6.
Absurde.
Ainsi $\underline{n_2 = 15}$.

On va maintenant faire du dénombrement dans G. On commence pour les éléments d'ordre 2 ou 4.

Soit S et S' des 2-Sylows de G alors $S \cap S' = \{1\}$.

En effet S et S' sont d'ordre 2^2 donc abelien*. Soit $g \in S \cap S'$ alors on pose:

$$C(g) = \{h \in G \mid gh = hg\}$$

Comme S et S' sont abélien on a $S \cup S' \subset C(g)$, or S et S' sont distincts donc $|S \cup S'| > 4$ donc $|C(g)| > 4$.

De plus $S \subset C(g)$ donc $4 \mid |C(g)|$ et de plus $|C(g)| \mid G = 60$ aussi:

$$|C(g)| = 12, 20 \text{ ou } 60.$$

Or si $|C(g)| = 12$ ou 20 alors c'est un sous-groupe d'indice 3 ou 5, absurde. Ainsi $|C(g)| = 60$ donc $C(g) = G$ donc $g \in Z(G)$.

Or $Z(G)$ est distingué dans G donc $Z(G) = G$ ou $Z(G) = \{e\}$ si $Z(G) = G$ alors G est abélien de cardinal non premier donc n'est pas simple*. Ainsi $g = e$ et donc:

$$S \cup S' = \{e\}.$$

L'intersection de deux 2-Sylows quelconques est trivial et il y a $n_2 = 15$ 2-Sylow ainsi l'ensemble des éléments G d'ordre 2 ou 4 est de cardinal $15 \times (4-1) = 45$

(Inclus dans un 2-Sylow car $\langle g \rangle$ est un p-sous-groupe de G + théorème de Sylow).

On dénombre maintenant les éléments d'ordre 5.

Soit n_5 le nombre de 5-Sylow on sait que:

$$\begin{cases} n_5 \mid 12 = 2 \times 2 \times 3 \\ n_5 \equiv 1 \ [5] \end{cases} \quad \text{donc } n_5 = 1 \text{ ou } 6$$

Par simplicité de G, $n_5 \neq 1$ donc $n_5 = 6$.

Chacun des 5-Sylow est cyclique donc deux 5-Sylows distincts ont une intersection réduite à $\{e\}$.

Ainsi l'ensemble des éléments d'ordre 5 est donc de cardinal $6 \times (5-1) = 24$.

Or on a $45 + 24 = 69 > 60$ Absurde. Il existe donc un sous-groupe H de G d'indice ≤ 5.

Soit H un sous-groupe d'indice ≤ 5.

Étape 2: Si $[G : H] \leq 4$.

On fait agir naturellement G sur G/H (de cardinal ≤ 4). Ceci induit un morphisme non trivial*:

$$\phi : G \longrightarrow \mathfrak{S}_4.$$

Ce morphisme est injectif. En effet $\ker(\phi)$ est un sous-groupe distingué de G et $\ker(\phi) \neq G$ donc $\ker(\phi) = \{e\}$.

Or $|G| = 60 > |\mathfrak{S}_4| = 24$, ce qui est absurde.

Étape 3: H est donc d'indice 5 dans G.

Ainsi l'action de G sur G/H de cardinal 5 induit donc un morphisme injectif (même argument):

$$\phi : G \longrightarrow \mathfrak{S}_5.$$

Or $|\mathfrak{S}_5| = 5 \times 4 \times 3 \times 2$ donc $\mathrm{Im}(G)$ est un sous-groupe d'indice 2 dans $\mathfrak{S}_5$

donc $\mathrm{Im}(G)$ est distingué dans $\mathfrak{S}_5$. ✓

donc $\mathrm{Im}(G) = \mathcal{A}_5$. ✓

On donc un isomorphisme $G \overset{\phi}{\simeq} \mathcal{A}_5$.

∎

Rmq: - Si G n'est pas simple on on a d'autre:

$$\mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Liste des résultats que l'on utilise + preuves.

Lemme: Tout groupe d'ordre p^2 est abélien.

Preuve: On sait que $|Z(G)| \geq p$ (voir l'action de G sur G par conjugaison).

On a donc $|Z(G)| = p$ ou p^2. Par l'absurde supposons que $|Z(G)| = p$.

Soit $x \in G \setminus Z(G)$ (existe) alors le stabilisateur de x est un ss-groupe de G contenant $Z(G) \cup \{x\} \supsetneq Z(G)$

donc d'ordre $> p$ i.e p^2 donc son stab est G i.e $x \in Z(G)$. Absurde.

∎

Lemme: Soit G un groupe abélien tel que $|G|$ ne soit pas premier alors G n'est pas simple.

Preuve: Soit $g \in G$ tel que $o(g) \neq |G| = nm$ avec $n \wedge m = 1$ et $n, m \neq 1$.

g existe car si $g \in G$ est tel que $o(g) = |G|$ alors g^m est d'ordre $1 < n < |G|$.

Or G est abélien donc $\langle g \rangle$ est distingué dans G et de cardinal $\neq |G|$ donc G n'est pas simple $\neq 1$ ☑

Lemme: Soit H un sous-groupe d'indice 2 de G alors H est distingué dans G.

Preuve: H est un sous-groupe stricte de G donc par $g \in G \setminus H$ on a:

$$G = H \cup gH.$$

Or on a une bijection entre les classes à droites et à gauche avec l'application $xH \longmapsto Hx$. Il existe donc une seule classe à droite non triviale. Comme $g \notin H$, cette classe est Hg et on a aussi:

$$G = H \cup Hg.$$

On en déduit $gH = Hg$ dès que $g \in H$ d'où le résultat. ☑

Théorème: Si $n \neq 4$, le groupe $\mathcal{A}_n$ est simple.

Rmq: Pour $n = 4$, A_4 n'est pas simple. Son groupe dérivé $D(A_4)$ est non trivial:

$$D(A_4) = \{Id, (12)\circ(34), (13)\circ(24), (14)\circ(23)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Preuve:

Cas où $n \leq 3$: On a $\mathcal{A}_2 \simeq \{1\}$ et $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

Cas où $n \geq 5$:

dans A_n

Soit $H \lhd A_n$ et $H \neq \{Id\}$. Les 3-cycles engendrent A_n et deux 3-cycles sont toujours conjugués ^{V}, donc il suffit de montrer que H contient un 3-cycles et on aura $A_n = H$.

Soient $\sigma \neq id$ dans H et τ un 3-cycle. H étant distingué dans A_n, $\tau\sigma\tau^{-1} \in H$ est $\sigma^{-1} \in H$ ainsi:

$$\rho = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in H.$$

Or ρ c'est le produit de τ et $\sigma\ \underbrace{\tau^{-1}\sigma^{-1}}_{=\tau'}$ qui sont deux 3-cycles. Ainsi ρ permute au plus 6 éléments.

Vérifions que l'on peut choisir τ tel que $\rho \neq id$.

Il existe déjà $1 \leq i \neq j \leq n$ tel que $\sigma(i) = j$. On choisit $k \notin \{i, j, \sigma(i)\}$ (possible car $n \geq 4$) et on prend

Le 3-cycle $\tau = (i\ k\ j)$. On a alors $\tau^{-1} = \tau^2 = (i\ j\ k)$ et

$$\rho(j) = \tau\sigma\tau^{-1}\sigma^{-1}(j) = \tau\sigma(j) \neq j.$$

On pose maintenant $F = \{i, j, k, \sigma(i), \sigma(j), \sigma(k)\}$, qui est de cardinal au plus 5 (car $\sigma(i) = j$) et il contient le support de ρ. On a avec $X = \{1, \dots, n\}$:

$$\rho|_{X \setminus F} = Id \text{ et } \rho(F) = F.$$

Quitte à ajouter des éléments à F on peut supposer que $|F| = 5$ et on considère le sous-groupe de A_n définie par :

$$\mathcal{A} := \{\sigma \in \mathcal{A}_n \mid \sigma(k) = k \text{ si } k \notin F\}.$$

Alors $\mathcal{A}$ est un sous-groupe de $\mathcal{A}_n$ isomorphe à $\mathcal{A}_5$ et $H \cap \mathcal{A}$ est distingué dans $\mathcal{A}$. De plus cette intersection n'est pas réduite à l'identité car $\rho \in \mathcal{A} \cap H$.
Si on montre la simplicité de $\mathcal{A}_5$ alors $\mathcal{A}$ est simple donc $H \cap \mathcal{A} = \mathcal{A}$ donc $\mathcal{A} \subset H$ ainsi H contient un 3-cycles.

Cas $n = 5$: On commence par décrire les 60 éléments de A_5. Pour cela on les regroupes par classes de conjugaison :

- identité
- les produits de 2 transpositions à supports disjoints (15 élément)
- les cycles d'ordres 3 (20 éléments)
- les cycles d'ordres 5 (24 éléments)

On sait que les 3 cycles sont conjugués dans A_5 on a de même pour les doubles transpositions. De plus les 3-cycles ou les produits de 2 transpo engendre A_5.

Soit $H \trianglelefteq A_5$ alors si H contient un 3-cycles ou une double transpo alors H les contients tous (car distingués) et donc $H = A_5$.
Soit σ 5-cycle appartenant à H alors $\langle\sigma\rangle$ est un 5-Sylow de A_5 car $\#A_n = 5 \times 4 \times 3$. Or les 5-Sylow étant tous conjugués et H distingués donc H contient tous les 5-Sylows de A_5 i.e toutes les 5-cycles.
Ainsi $|H| \geqslant 24$ or $|H| | 60$ donc $|H| = 30$ ou 60. Dans les deux cas H contient au moins un

trois cycles ou une double transpo.

Corollaire: Si $n \neq 4$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id\}$, A_n et $\mathfrak{S}_n$. p269.

Preuve: Pour $n = 2$, on a $\mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$ donc ok.

Supposons $n \geq 3$ et $n \neq 4$ et soit $H \triangleleft \mathfrak{S}_n$. On a $H \cap A_n \triangleleft A_n$, ce qui implique $H \cap A_n = \{Id\}$ ou A_n.

Cas 1: $H \cap A_n = \{I_n\}$.

Alors $\varepsilon|_H$ (où ε est la signature) est injective donc $|H| \leq 2$. Ainsi si $H = \{id, \sigma\}$ avec σ d'ordre 2. Or H est distingué dans $\mathfrak{S}_n$ implique:

$$\forall \sigma \in \mathfrak{S}_n, \sigma\tau\sigma^{-1} = \tau.$$

On en déduit que $\tau \in Z(\mathfrak{S}_n) = \{Id\}$ car $n \geq 3$ ce qui est Absurde.

Cas 2: $H \cap A_n = A_n$

Alors $H = A_n$ ou $A_n \not\subset H$ alors H d'indice < 2 donc $H = \mathfrak{S}_n$.