103 — Exemples de sous-groupes distingués et de groupes quotients. Applications

Dans tout ce qui suit G désigne un groupe.

I] Définitions et premiers exemples

1) Quotient par un sous-groupe

DEF 1. Une relation d'équivalence $\mathcal{R}$ sur G est dite compatible à gauche (resp. à droite) avec la loi de G si :

$\forall x, y, g \in G,\ x\mathcal{R}y \Rightarrow gx\mathcal{R}gy$ (resp. $x\mathcal{R}y \Rightarrow xg\mathcal{R}yg$).

PROP 2. Une relation d'équivalence $\mathcal{R}$ sur G est compatible à gauche (resp. à droite) avec la loi de G si et seulement si il existe un sous-groupe H de G tel que $\forall x, y \in G,\ x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$ (resp. $yx^{-1} \in H$)

DEF 3. Soit H un sous groupe de G. On note $(G/H)_g$ (resp $(G/H)_d$) l'ensemble quotient de G par la relation $\mathcal{R}_g$ (resp. $\mathcal{R}_d$) définie par :

$\forall x, y \in G,\ x\mathcal{R}_g y \Leftrightarrow x^{-1}y \in H$ (resp $x\mathcal{R}_d y \Leftrightarrow yx^{-1} \in H$)

PROP 4. Les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents. Si $(G/H)_g$ est fini, on note $[G:H] = |(G/H)_g|$ l'indice de H dans G

EX 5. Si G agit sur un ensemble X alors le stabilisateur d'un point $x \in X$ sous cette action est un sous groupe de G noté Stab_x et G/Stab_x est en bijection avec l'orbite de x.

App 6. Soit $X \subset \mathfrak{S}_n$ l'ensemble des k-cycles. On peut déterminer $|X|$ en considérant l'action par conjugaison de $\mathfrak{S}_n$ sur X

2) Lien entre sous-groupe distingué et groupe quotient

DEF 7. Un sous groupe H de G est distingué si il est stable par automorphismes intérieurs. On note $H \lhd G$: $\forall g \in G, \forall h \in H,\ ghg^{-1} \in H$.

REM 8. On a $H \lhd G$ si et seulement si $\mathcal{R}_g = \mathcal{R}_d$

PROP 9. Soit $\varphi : G \to G'$ un morphisme de groupes. On a $\mathrm{Ker}\,\varphi \lhd G$

EX 10.
- Tout sous groupe d'un groupe abélien est distingué.
- Dans $\mathfrak{S}_3$, le sous groupe $\{id, (123), (132)\}$ est distingué.
- Le centre $Z(G)$ est distingué dans G, de même que tout sous-groupe de $Z(G)$
- Le groupe des homothéties est distingué dans $GL_n(K)$.
- $A_n \lhd \mathfrak{S}_n$ où A_n est le groupe alterné.
- $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

TH 11. On peut munir G/H d'une loi de groupe faisant de la projection un morphisme de groupe si et seulement si H est distingué dans G

EX 12.
- $\mathbb{Z}$ est abélien, ses groupes quotients sont les $\mathbb{Z}/n\mathbb{Z}$ pour $n \in \mathbb{N}$.
- Pour $n \in \mathbb{N}^*$, le groupe quotient $\mathbb{R}^n/\mathbb{Z}^n$ est appelé tore de dimension n.
- On définit $PGL_n(K)$ comme $GL_n(K)/K^* I_d$ où K est un corps

PROP 13. Soit $\varphi : G \to G'$ un morphisme de groupes et $H \lhd G$. Si $H \subset \mathrm{Ker}\,\varphi$ alors il existe un unique morphisme $\tilde{\varphi} : G/H \to G'$ tel que $\varphi = \tilde{\varphi} \circ \pi$ où $\pi : G \to G/H$ est la projection canonique.

APP 14.
- $\mathbb{R}/\mathbb{Z} \simeq S^1$ via $\varphi : \theta \mapsto e^{2i\pi\theta}$
- $\mathfrak{S}_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$ via la signature
- $GL_n(K)/SL_n(K) \simeq K^*$ via le déterminant.
- $O_n(K)/SO_n(K) \simeq \mathbb{Z}/2\mathbb{Z}$ si car $K \neq 2$
- Notons $\mathbb{H}_1$ le groupe des quaternions unité. On a $\mathbb{H}_1/\{-1,1\} \simeq SO_3(\mathbb{R})$ via l'action par conjugaison de $\mathbb{H}_1$ sur les quaternions purs

PROP 15. Soient K, H deux sous groupes distingués de G vérifiant $H \subset K$. Alors $K/H \lhd G/H$ et $G/H \big/ K/H \simeq G/K$.

EX 16. Soient $n \in \mathbb{N}^*$ et $d|n$, on a $\mathbb{Z}/n\mathbb{Z} \big/ d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$

3) Application aux p-groupes

DEF 17. Soit p premier, G est un p-groupe si il existe $k \in \mathbb{N}$ tel que $|G| = p^k$

LEM 18. Si $G/Z(G)$ est cyclique alors G est abélien.

PROP 19. Si G est un p-groupe alors pour tout diviseur d de $|G|$, G admet un sous groupe d'ordre d.

PROP 20 Soit p premier, les seuls groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

II] Extension d'un sous groupe distingué par un groupe quotient.

Dans cette partie A et B sont des groupes

1) Quelques exemples

DEF 21. On dit que G est une extension de A par B s'il existe un sous groupe distingué H de G tel que $A\simeq H$ et $B\simeq G/H$.

Groupe cyclique. $\mathbb{Z}/ab\mathbb{Z}$ est une extension de $\mathbb{Z}/a\mathbb{Z}$ par $\mathbb{Z}/b\mathbb{Z}$ via $H = b\mathbb{Z}/b\mathbb{Z}$.

Groupe diédral. Le groupe D_n des isométries du plan conservant un n-gone regulier est une extension de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$ via le sous groupe H des rotations de D_n.

Groupe linéaire. $GL_n(K)$ est une extension de $SL_n(K)$ par $K^\times$ via $H = SL_n(K)$, mais aussi de $K^\times$ par $PGL_n(K)$ via le sous groupe H des homothéties de $GL_n(K)$

Groupe de permutations $\mathfrak{S}_n$ est une extension de A_n par $\mathbb{Z}/2\mathbb{Z}$ via $H = A_n$

Groupe affine. Le groupe affine $GA(\mathcal{E})$ d'un espace affine $\mathcal{E}$ dirigé par un espace vectoriel E est une extension de E par $GL(E)$ via le sous-groupe H des translations de $GA(\mathcal{E})$

Groupe des quaternions unités. $\mathbb{H}_1$ est une extension de $\mathbb{Z}/2\mathbb{Z}$ par $SO_3(\mathbb{R})$

2) Extension scindée, produit semi direct

DEF 22. Une suite $(\varphi_i)_i$ de morphismes est dite exacte si : $\forall i, \mathrm{Im}\,\varphi_i = \mathrm{Ker}\,\varphi_{i+1}$

PROP 23 G est une extension finie de A par B si et seulement si on a une suite exacte de la forme $1\to A\to G\to B\to 1$

DEF 24 On dit que G est une extension scindée de A par B si on a une suite exacte de la forme $1\to A\to G\xrightarrow{\pi} B\to 1$ et que π admet une section, c'est à dire un morphisme $s: B\to G$ tel que $\pi\circ s = id_B$

EX 25. D_n, $GL_n(K)$, $\mathfrak{S}_n$, $GA(\mathcal{E})$ sont des extensions scindées de $\mathbb{Z}/n\mathbb{Z}$, $SL_n(K)$, A_n, E par $\mathbb{Z}/2\mathbb{Z}$, $K^\times$, $\mathbb{Z}/2\mathbb{Z}$, $GL(E)$ respectivement.

C-EX 26. • $\mathbb{Z}/ab\mathbb{Z}$ est une extension scindée de $\mathbb{Z}/a\mathbb{Z}$ par $\mathbb{Z}/b\mathbb{Z}$ $\iff a\wedge b = 1$.
• $GL_n(K)$ n'est pas une extension scindée de $K^\times$ par $PGL_n(K)$
• Le groupe des quaternions unités $\mathbb{H}_1$ n'est pas une extension scindée de $\mathbb{Z}/2\mathbb{Z}$ par $SO_3(\mathbb{R})$

DEF 27. Etant donné un morphisme $\varphi: B\to \mathrm{Aut}(A)$, on appelle produit semi-direct de A par B via φ le groupe noté $A\rtimes_\varphi B$ dont l'ensemble sous jacent est $A\times B$ et dont la loi est donnée par
$\forall (a_1,b_1),(a_2,b_2)\in A\times B$, $(a_1,b_1)\cdot(a_2,b_2) = (a_1\varphi(b_1)(a_2), b_1b_2)$

REM 28. $(G\simeq A\rtimes B$ et $B\lhd G) \iff (G\simeq A\times B)$.

EX 29. • $\mathfrak{S}_3 \simeq \mathbb{Z}/3\mathbb{Z}\rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ avec $\varphi: 1\mapsto (1\mapsto 2)$
• $D_4 \simeq \mathbb{Z}/4\mathbb{Z}\rtimes_\varphi\mathbb{Z}/2\mathbb{Z}$ avec $\varphi: 1\mapsto(1\mapsto 3)$

C EX 30. Le groupe des quaternions $\mathbb{H}_8$ ne se décompose pas en produit semi direct non trivial.

TH 31. G est une extension scindée de A par B si et seulement si G est isomorphe à un produit semi-direct $A\rtimes B$

3) Applications à la description des groupes

Lemme Chinois. $(a\wedge b = 1)\iff(\mathbb{Z}/ab\mathbb{Z}\simeq \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z})$

Groupe diédral. $D_n\simeq \mathbb{Z}/n\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$

Groupe des permutations $\mathfrak{S}_n\simeq A_n\rtimes\mathbb{Z}/2\mathbb{Z}$

Groupe linéaire. $GL_n(K)\simeq SL_n(K)\rtimes K^\times$

Groupe affine. $GA(\mathcal{E})\simeq E\rtimes GL(E)$.

LEM-32. Si p est le plus petit facteur premier de $|G|$ et H est un sous groupe de G d'indice p alors H est distingué dans G.

Groupes d'ordre pq ($p<q$ premiers). Les seuls groupes d'ordre pq sont $\mathbb{Z}/pq\mathbb{Z}$ si $p \nmid q-1$ et $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ si $p \mid q-1$. DEV-1

III Décomposition en suite de sous-groupes distingués et simplicité

1) Résolubilité

DEF-33. Le groupe dérivé de G noté $D(G)$ est le groupe engendré par les commutateurs, i.e. les éléments $xyx^{-1}y^{-1}$ pour $x,y \in G$

PROP 34. $D(G)$ est distingué dans G et pour $H \triangleleft G$ on a :

$$G/H \text{ abélien} \iff D(G) \subset H$$

EX-35. • G est abélien $\iff D(G)=\{1\}$. • $D(\mathfrak{S}_3)=\{id,(123),(132)\}$

• $D(\mathbb{H}_8)=\{-1,1\}$ • Si $n\neq 2$ ou $K \neq \mathbb{F}_2$ alors $D(GL_n(K))=SL_n(K)$.

• Si $n=2$ et $K=\mathbb{F}_2$ alors, $GL_n(K)=SL_n(K)$ et $D(GL_n(K)) \simeq A_3$.

DEF-36. Une suite de sous-groupes distingués est une famille $(G_i)_{0\leq i\leq n}$ de sous-groupes de G vérifiant : $G_0=\{1\}$, $G_n=G$ et $\forall i \in [\![0,n-1]\!]$, $G_i \triangleleft G_{i+1}$.

DEF-37. G est résoluble si il admet une suite de sous-groupes distingués pour laquelle les quotients G_{i+1}/G_i sont abéliens

EX-38. • Tout groupe abélien est résoluble. • $\mathbb{H}_8$ est résoluble

• $\mathfrak{S}_3$ est résoluble : $\{id\} \triangleleft \{id,(123),(132)\} \triangleleft \mathfrak{S}_3$

• $\mathfrak{S}_4$ est résoluble : $\{id\} \triangleleft V_4 \triangleleft A_4 \triangleleft \mathfrak{S}_4$ où V_4 est l'ensemble des double-transpositions

PROP 39. G est résoluble si et seulement si il existe $n\in\mathbb{N}^*$ tel que $D^n(G)=D\circ\cdots\circ D(G)=\{1\}$.

APP 40. Le groupe $T_n(\mathbb{C}) \subset GL_n(\mathbb{C})$ des matrices triangulaires supérieures est résoluble.

TH-41. (Lie-Kolchin) Si G est un sous-groupe résoluble connexe de $GL_n(\mathbb{C})$ alors G est conjugué à un sous-groupe de $T_n(\mathbb{C})$.

2) Exemples de groupes simples et suites de composition

DEF-42. G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G

EX-43 • Les seuls groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ où p est premier.

• $SO_3(\mathbb{R})$ est simple.

APP 44. Si $\varphi : G \to G'$ est un morphisme et G est simple alors φ est le morphisme trivial ou est injectif.

TH-45. Pour tout $n\geq 5$, A_n est simple. DEV-2

APP 46. • Pour $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble car $D(\mathfrak{S}_n)=A_n$ et $D(A_n)=A_n$.

• A_2 et A_3 sont simples mais pas A_4 dans lequel V_4 est distingué.

DEF 47. Une suite de composition est une suite de sous-groupes distingués $(G_i)_{0\leq i\leq n}$ telle que $\forall i\in[\![0,n-1]\!]$, G_{i+1}/G_i est simple.

PROP 48. Dans la définition précédente, G_i est un sous-groupe distingué maximal de G_{i+1}.

EX-49. • $\{1\} \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft \mathbb{Z}/4\mathbb{Z} \triangleleft \mathbb{Z}/12\mathbb{Z}$ est une suite de composition.

• Si $n\in\mathbb{N}^*$ s'écrit $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ alors on a la suite de composition :

$$\{1\} \triangleleft \mathbb{Z}/p_1\mathbb{Z} \triangleleft \mathbb{Z}/p_1^2\mathbb{Z} \triangleleft \cdots \triangleleft \mathbb{Z}/p_1^{\alpha_1}p_2\mathbb{Z} \triangleleft \mathbb{Z}/p_1^{\alpha_1}p_2^2\mathbb{Z} \triangleleft \cdots \triangleleft \mathbb{Z}/n\mathbb{Z}.$$

• Si $n\in\mathbb{N}^*$ et $n\neq 4$, $\{1\} \triangleleft A_n \triangleleft \mathfrak{S}_n$ est une suite de composition.

DEF-50. Deux suites de composition $(G_i)_{0\leq i\leq n}$ et $(G'_j)_{0\leq j\leq s}$ sont dites équivalentes si $n=s$ et $\prod_{i=0}^{n-1} G_{i+1}/G_i \simeq \prod_{j=0}^{n-1} G'_{j+1}/G'_j$.

TH-51. (Jordan-Hölder) Deux suites de composition de G sont équivalentes.

APP 52. • La décomposition en facteurs premiers dans $\mathbb{Z}$ est unique à ordre près

• Si G admet une suite de composition, la longueur de cette suite fournit une notion de dimension. On peut étendre cette notion aux modules sur un anneau.

Détermination des groupes d'ordre pq avec $p<q$ premiers

Thm Soient p et q deux nombres premiers tels que $p<q$

1) Si $p \nmid (q-1)$, alors l'unique groupe d'ordre pq est le groupe cyclique d'ordre pq

2) Si $p \mid (q-1)$, alors il y a exactement deux groupes d'ordre pq : le groupe cyclique d'ordre pq et le produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.

Lemme. Soit G un groupe, et soit p le plus petit facteur premier de G. Si A est un sous-groupe de G d'indice p, alors A est distingué dans G.

Preuve (du lemme) Soit A un sous-groupe de G d'indice p.

A agit par translation à gauche sur $(G/A)_g$: $\begin{cases} A \times (G/A)_g \longrightarrow (G/A)_g \\ (a, xA) \longmapsto (ax)A \end{cases}$

On remarque que : $(A \lhd G) \Leftrightarrow (\forall x \in G,\ \mathrm{Stab}(xA) = A)$

Comme : $(\forall x \in G,\ |\mathrm{Orb}(xA)| = |A| / |\mathrm{Stab}(xA)|)$, il s'agit de montrer que :

$\forall x \in G,\ |\mathrm{Orb}(xA)| = 1$.

Or on a la formule : $p = |(G/A)_g| = \sum_{xA \in (G/A)_g} |\mathrm{Orb}(xA)|$.

Donc on a : $\forall x \in G,\ |\mathrm{Orb}(xA)| < p$

Comme par ailleurs : $(\forall x \in G,\ |\mathrm{Orb}(xA)| \mid |G|)$, on a bien : $(\forall x \in G,\ |\mathrm{Orb}(xA)| = 1)$

Ce qui montre que A est distingué dans G. $\square$

Preuve (du théorème). Soit G un groupe d'ordre pq

Par théorème de Cauchy (ou de Sylow), il existe $a, b \in G$ d'ordres q, p respectivement

On note $A = \langle a \rangle$ et $B = \langle b \rangle$

$[G:A] = p$ donc d'après le lemme précédent, $A \lhd G$.

On a donc une suite exacte de la forme $1 \longrightarrow A \longrightarrow G \xrightarrow{\pi} B \longrightarrow 1$

On va montrer que π admet une section.

$\pi_{|B} : B \to \mathbb{Z}/p\mathbb{Z}$ est bijective car : $\begin{cases} \mathrm{Ker}(\pi_{|B}) = A \cap B = \{1\} \\ |B| = |\mathbb{Z}/p\mathbb{Z}| \end{cases}$

Ainsi : $\exists\, b_0 \in B,\ \pi(b_0) = 1$

On définit alors $s \begin{cases} \mathbb{Z}/p\mathbb{Z} \to G \\ \bar{k} \mapsto b_0^k \end{cases}$ et on vérifie que : $\pi \circ s = \mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$.

Comme G est une extension scindée de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$, $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$

avec $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ car $x \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est déterminé par $x(1)$

$\cong \mathbb{Z}/(q-1)\mathbb{Z}$ car le groupe des inversibles d'un corps fini est cyclique.

On a la distinction de cas suivante :

1) $p \nmid (q-1)$. $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ n'admet aucun sous groupe d'ordre p donc φ est nécessairement trivial et $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/(pq)\mathbb{Z}$.

2) $p \mid (q-1)$. $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet un unique sous-groupe H d'ordre p

Si φ est trivial alors on a encore : $G \cong \mathbb{Z}/(pq)\mathbb{Z}$.

Supposons φ non trivial et montrons que : $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$.

dès que $\psi\ \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un autre morphisme non trivial

Or φ, ψ induisent des isomorphismes $\tilde{\varphi}, \tilde{\psi} : \mathbb{Z}/p\mathbb{Z} \to H$

Donc $\beta = \tilde{\psi}^{-1} \circ \tilde{\varphi} \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ et l'application

$\begin{cases} \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \\ (a, b) \longmapsto (a, \beta(b)) \end{cases}$ est un isomorphisme $\square$

Simplicité du groupe alterné

Théorème. Pour tout $n \geq 5$, le groupe A_n est simple.

La preuve consiste à montrer la simplicité de A_5 dans un premier temps. Puisque A_5 est d'ordre 60, on peut facilement dénombrer des éléments d'une classe de conjugaison. Dans un second temps, on se sert de cela pour montrer que tout sous-groupe distingué non-nul de A_n contient un 3-cycle.

Preuve. • Montrons que A_5 est simple. Par dénombrement, on peut montrer que A_5 contient les éléments suivants :

— l'identité

— 15 double-transpositions $\quad (i\,j)(k\,l)$, $|\{i,j,k,l\}| = 4$

— 20 cycles de longueur 3 $\quad (i\,j\,k)$, $|\{i,j,k\}| = 3$

— 24 cycles de longueur 5 $\quad (i\,j\,k\,l\,m)$, $\{i,j,k,l,m\} = [\![1,5]\!]$.

Les cycles d'ordre 3 sont conjugués dans A_5. En effet, prenons $\tau = (a\,b\,c)$ et $\tau' = (a'\,b'\,c')$. Considérons $\sigma \in \mathfrak{S}_n$ vérifiant $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(c) = c'$. Si σ n'est pas dans A_5 alors posons $e, e' \in [\![1,5]\!]$ tels que $\{a,b,c,e,e'\} = [\![1,5]\!]$, on a $\sigma' := \sigma(e\,e') \in A_5$ et $\sigma'\tau\sigma'^{-1} = \tau'$, sinon on a $\sigma\tau\sigma^{-1} = \tau'$.

Les double-transpositions sont conjuguées dans A_5. En effet, prenons $\tau = (a\,b)(c\,d)$ et $\tau' = (a'\,b')(c'\,d')$ et notons e, e' tels que $[\![1,5]\!] = \{a,b,c,d,e\} = \{a',b',c',d',e'\}$. Par la même méthode que précédemment on peut prendre $\sigma \in A_5$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$. On a alors : $\sigma\tau\sigma^{-1} = (a'\,b')(\sigma(c)\,\sigma(d))$. Or, $\varepsilon(\sigma\tau\sigma^{-1}) = \varepsilon(\tau) = 1$. Donc on a nécessairement $\sigma(\{c,d\}) = \{c',d'\}$ de sorte que $\sigma\tau\sigma^{-1} = \tau'$.

Soit $H \triangleleft A_5$ avec $H \neq \{id\}$. D'après ce qui précède, si H contient une double-transposition ou un 3-cycle alors il les contient tous. De plus, les 5-Sylow étant conjugués dans A_5, s'il contient un 5-cycle, il les contient tous. Or, $|A_5| = 60$ et H ne peut pas contenir qu'un seul type des trois éléments, 3-cycles, 5-cycles, double-transpositions car $|H| \mid 60$. Donc, $|H| \geq 1+15+20=36$ et $|H|=60$.

• Montrons que A_n est simple pour $n \geq 5$. Soit $H \lhd A_n$ avec $H \neq \{id\}$. Soit $\sigma \in H \setminus \{id\}$, il existe $a, b \in [\![1,n]\!]$ tels que $\sigma(a)=b \neq a$. Prenons aussi $c \notin \{a, b, \sigma(b)\}$. Posons $\tau=(a\,c\,b)$ et $\rho=\tau\sigma\tau^{-1}\sigma^{-1}= (a\,c\,b)(\sigma(a)\,\sigma(b)\,\sigma(c))$. Comme $b=\sigma(a)$, l'ensemble $F=\{a,b,c,\sigma(a),\sigma(b),\sigma(c)\}$ a au plus 5 éléments. Quitte à lui rajouter des éléments qui ne sont pas dans le support de ρ, on peut supposer que $|F|=5$. On a : $\rho(F)=F$ et $\rho_{|[\![1,n]\!]\setminus F}=id_{[\![1,n]\!]\setminus F}$. De plus, $\rho(b)=\tau\sigma(b)\neq b$ donc ρ n'est pas l'identité.

Comme F a 5 éléments, le groupe $A(F)$ des permutations paires de F est isomorphe à A_5. De plus, il se plonge dans A_n via le morphisme injectif :

$$i : A(F) \longrightarrow A_n$$
$$u \longmapsto \begin{cases} u & \text{sur } F \\ id_{[\![1,n]\!]\setminus F} & \text{sur } [\![1,n]\!]\setminus F \end{cases}$$

Notons $H_0=i^{-1}(H)$, on a $H_0 \lhd A(F)$. On remarque que $\rho \in i^{-1}(H)$. Or, $\rho_{|F} \neq id_F$ donc $H_0 \neq \{id\}$. Mais comme $A(F) \simeq A_5$ est simple, on déduit que $H_0=A(F)$. Ainsi, si on prend $u \in A(F)$ un cycle d'ordre 3, $i(u)$ reste un cycle d'ordre 3 dans A_n et appartient à H.

Dans A_n les 3-cycles sont conjugués. Cela se montre de la même manière que dans A_5. Ainsi, H étant distingué dans A_n, il contient tous les 3-cycles. Or, les 3-cycles engendrent A_n donc $H=A_n$. ∎