Leçon 103

Conjugaison dans un groupe, exemples de sous-groupes distingués et de groupes quotients, applications.

1 Conjugaison dans un groupe

1.1 Action par conjugaison

On fixe G un groupe.

Définition 1 (PER *p.*15)**.**
L'action de G sur lui-même par conjugaison est $\begin{array}{ccc} G\times G & \to & G \\ (g,h) & \mapsto & ghg^{-1} \end{array}$.

Définition 2 (PER *p.*9)**.** On note $\mathrm{Int}(G)$ l'image du morphisme associé à l'action par conjugaison. Ses éléments sont appelés automorphismes intérieurs de G.

Définition 3 (PER *p.*15)**.** L'orbite de $g \in G$ pour cette action est la classe de conjugaison $C_g = \{xgx^{-1} \mid x \in G\}$.
Le stabilisateur de $g \in G$ pour cette action est le centralisateur $N_G(g) = \{x \in G \mid xg = gx\}$.

Proposition 4 (PER *p.*15)**.** Si G est fini, le cardinal d'une classe de conjugaison divise $|G|$.

Exemple 5. $x \in Z(G) \iff C_x = \{x\} \iff N_G(x) = G$.
Si G n'a qu'une classe de conjugaison, $G = \{e_G\}$.
Si G est fini et n'a que deux classes de conjugaisons, G est cyclique d'ordre 2.
Si G est de cardinal fini n et a n classes de conjugaisons, G est abélien.

Proposition 6 (PER *p.*16)**.** Le centre d'un p-groupe n'est jamais trivial.

1.2 Conjugaison dans les groupes classiques

Cas $G = \mathfrak{S}_n$:

Lemme 7 (SZP *p.*265)**.** Soit $\sigma \in \mathfrak{S}_n$. On a $\sigma(i_1, \dots, i_r)\sigma^{-1} = (\sigma(i_1), \dots, \sigma(i_r))$.

Définition 8 (SZP *p.*265)**.** Soit $\sigma \in \mathfrak{S}_n$. Si $\sigma = \sigma_1 \cdots \sigma_r$ est la décomposition en produit de cycles à supports disjoints de σ (en comptant les "cycles de longueur 1") avec $\ell(\sigma_1) \geqslant \cdots \geqslant \ell(\sigma_r)$ $(\ell((i_1, \dots, i_s)) = s)$, on appelle type de σ la suite $\ell(\sigma_1) \geqslant \cdots \geqslant \ell(\sigma_r)$.

Théorème 9 (SZP *p.*265)**.** Deux permutations sont conjuguées si et seulement si elles ont même type.

Corollaire 10 (SZP *p.*267)**.** Si $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Cas $G = D_n$:

Proposition 11. Les classes de conjugaison de D_n sont :

1. Si $n \in 2\mathbb{N}^*$: $\{\mathrm{id}\}$, $\{r^{n/2}\}$, $\{s, r^2s, \dots, r^{2n-2}s\}$, $\{rs, \dots, r^{2n-1}s\}$, $\{r^h, r^{-h}\}$ pour $1 \leqslant h \leqslant \dfrac{n}{2} - 1$.
2. Si $n \in 2\mathbb{N}+1$: $\{\mathrm{id}\}$, $\{s, rs, \dots, r^{n-1}s\}$, $\{r^h, r^{-h}\}$ pour $1 \leqslant h \leqslant \dfrac{n-1}{2}$.

Cas d'un corps fini :

Lemme 12 (Développement 1, SZP *p.*773)**.** Pour tout $n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d|n} \Phi_d$. En particulier, $\Phi_n \in \mathbb{Z}[X]$.

Lemme 13 (Développement 1, SZP *p.*773)**.** Si $n, d \in \mathbb{N}^*$ et $q \geqslant 2$, $q^d - 1 \mid q^n - 1 \implies d \mid n$.

Si d divise n strictement, on a $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$.

Théorème 14 (Développement 1, SZP *p.*773)**.** Tout corps gauche fini est commutatif.

1.3 Conjugaison en géométrie

Principe 15. Si G est un groupe de transformations géométriques et si $g, h \in G$, h et ghg^{-1} ont la même nature géométrique et les caractéristiques géométriques de ghg^{-1} sont les caractéristiques géométriques de h translatées par g.

Soit E un espace affine euclidien.

Proposition 16 (SZP *p.*388)**.** Si $\vec{u} \in \vec{E}$ et $g \in \mathrm{GA}(E)$, on a $g \circ t_{\vec{u}} \circ g^{-1} = t_{\vec{g}(\vec{u})}$.

Proposition 17. Soit $\varphi \in \mathrm{GA}(E)$.

1. Soit s une réflexion d'hyperplan H. $\varphi \circ s \circ \varphi^{-1}$ est une réflexion d'hyperplan $\varphi(H)$.
2. Soit r une rotation de centre O et d'angle θ (ici, $\dim E = 2$). $\varphi \circ r \circ \varphi^{-1}$ est la rotation de centre $\varphi(O)$ et d'angle θ.
3. Soit r une rotation d'axe D (ici, $\dim E = 3$). $\varphi \circ r \circ \varphi^{-1}$ est une rotation d'axe D.

Soit E un espace vectoriel de dimension finie.

Définition 18 (SZP *p.*297-298)**.** Soit $u \in \mathrm{GL}(E) \backslash \{\mathrm{id}_E\}$ fixant un hyperplan.

1. u est une transvection $\iff$ u n'est pas diagonalisable $\iff$ $\det u = 1$.
2. u est une dilatation $\iff$ u est diagonalisable (sa valeur propre $\lambda \neq 1$ est appelée son rapport) $\iff$ $\det u \neq 1$.

Proposition 19 (SZP *p.*300)**.**

1. Toutes les transvections sont conjuguées dans $\mathrm{GL}(E)$.
2. Si $n \geqslant 3$, elles sont conjuguées dans $\mathrm{SL}(E)$.

Proposition 20 (SZP *p.*298)**.** Deux dilatations sont conjuguées dans $\mathrm{GL}(E)$ si et seulement si elles ont le même rapport λ.

2 Sous-groupes distingués

On fixe un groupe G et un sous-groupe H de G.

Définition 21 (ESC $p.405$)**.** On définit les relations d'équivalents $\sim_d$ et $\sim_g$ sur G par

$$\forall g_1, g_2 \in G, \quad g_1 \sim_g g_2 \iff \exists h \in H g_1 = g_2 h,$$

$$\forall g_1, g_2 \in G, \quad g_1 \sim_d g_2 \iff \exists h \in H g_1 = h g_2$$

et on pose G/H et $H\backslash G$ les ensembles quotients respectifs.

Proposition 22 (ESC $p.406$)**.** L'application $g \mapsto g^{-1}$ de G induit une bijection entre G/H et $H\backslash G$.
Dans le cas où ces ensembles sont finis, on note $|G : H|$ leur cardinal commun.

Théorème 23 (de Lagrange, ESC $p.405$)**.** Si G est fini, on a $|G| = |G : H||H|$.

Définition 24 (PER $p.11$)**.** On dit que H est distingué dans G (noté $H \triangleleft G$) s'il est stable par $\mathrm{Int}(G)$. De manière équivalente, H est distingué dans G si pour tout $g \in G$, $gH = Hg$.

Exemple 25 (PER $p.12$)**.** On a toujours $\{e_G\}, G \triangleleft G$.
Si G est abélien, tout sous-groupe de G est distingué. La réciproque est fausse : H_8.
Si E est un espace affine, le groupe des translations est distingué dans $\mathrm{GA}(E)$.

Proposition 26 (PER $p.11$)**.** Si $f : G \to G'$ est un morphisme de groupes, on a $\ker(f) \triangleleft G$.

Exemple 27 (PER $p.12$)**.** On a $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ et $\mathrm{SL}(E) \triangleleft \mathrm{GL}(E)$.

Proposition 28 (PER $p.12$)**.** Le centre $Z(G)$ de G est distingué dans G.

Proposition 29. Si $|G : H| = 2$ alors $H \triangleleft G$.

Exemple 30 (SZP $p.391$)**.** On a $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$.
Si E est un espace affine euclidien alors $\mathrm{O}^+(E)$ est distingué dans $\mathrm{O}(E)$.

Théorème 31 (SZP $p.243$)**.** Soient H, K deux sous-groupes de G tels que

$$H \cap K = \{e_G\}, \quad G = HK, \quad H, K \triangleleft G.$$

On a $G \simeq H \times K$.

Application 32. Si E est un espace affine euclidien et $X \subset E$, $\mathrm{Is}(X) \simeq \mathrm{Is}^+(X) \times \mathbb{Z}/2\mathbb{Z}$ dès que $\mathrm{Is}^-(X) \neq \emptyset$.

Application 33 (Lemme Chinois, PER $p.21$)**.** Soient G et H deux groupes cycliques d'ordre p et q respectivement. Si $p \wedge q = 1$ alors $G \times H$ est cyclique d'ordre pq.

Application 34 (SZP $p.244$)**.** Si $|G| = p^2$ avec $p \in \mathbb{P}$ alors G est cyclique ou le produit de deux groupes cycliques d'ordre p.

Définition 35 (PER $p.12$)**.** G est simple si $G \neq \{e_G\}$ et si G n'admet pas de sous-groupes distingués autres que $\{e_G\}$ et G.

Théorème 36 (PER $p.12$)**.** Un groupe abélien est simple si et seulement s'il est cyclique d'ordre premier.

Théorème 37 (PER $p.12$)**.** Si $n = 3$ ou $n \geqslant 5$, $\mathfrak{A}_n$ est simple.

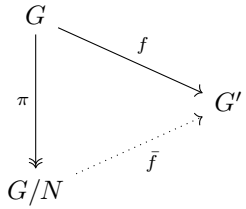
3 Groupes quotients

Théorème 38 (SZP $p.228$)**.** Soit $H \triangleleft G$. Il existe une unique structure de groupe sur G/H tel que la projection canonique soit un morphisme de groupe. Pour $g, g' \in G$, on a alors $(gH)(g'H) = (gg')H$ et $(gH)^{-1} = g^{-1}H$. G/H est le groupe quotient de G par H.

Corollaire 39 (SZP $p.229$)**.** On a $H \triangleleft G$ si et seulement si il existe un morphisme de groupes $f : G \to G'$ tel que $H = \ker(f)$.

Théorème 40 (de correspondance, SZP $p.231$)**.** La surjection canonique $\pi : G \mapsto G/H$ induit une bijection entre les sous-groupes (resp. sous-groupes distingués) de G/H et les sous-groupes (resp. sous-groupes distingués) de G contenant H.

Théorème 41 (de factorisation, SZP $p.229$)**.** Soit $f : G \to G'$ un morphisme de groupes et soit $N \subset G$ un sous-groupe distingué vérifiant $N \subset \ker(f)$. Notons $\pi : G \to G/N$ l'application canonique. Il existe un unique morphisme $\bar{f} : G/N \to G'$ vérifiant $f = \bar{f} \circ \pi$.



Théorème 42 (d'isomorphisme, SZP $p.232$)**.**

1. Soit $f : G \to G'$ un morphisme de groupe. f induit un isomorphisme de groupes $G/\ker(f) \simeq \mathrm{Im}(f)$.
2. Si $H \triangleleft G$ et $K \subset G$ sont des sous-groupes de G, on a $K \cap H \triangleleft K$ et
$$K/H \cap K \simeq KH/H.$$
3. Si $K \triangleleft H \triangleleft G$ alors $H/K \triangleleft G/K$ et on a
$$\frac{G/K}{H/K} \simeq G/H.$$

Exemple 43. On a $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^*$.
On a $\mathrm{GA}(E)/\{\text{Translations}\} \simeq \mathrm{GL}(\vec{E})$.
On a $G/Z(G) \simeq \mathrm{Int}(G)$.
On a $\mathrm{SO}(2) \simeq \mathbb{R}/2\pi\mathbb{Z}$.

4 Applications

4.1 Théorème de Dixon

Lemme 44 (CAL $p.305$)**.** Si $G/Z(G)$ est cyclique alors G est abélien.

Application 45 (CAL $p.305$)**.** Soit G un groupe fini de cardinal n non abélien et soit p la probabilité que deux éléments de G, tirés uniformément commutent. Alors on a

1. $p \leqslant \frac{5}{8}$,
2. $p = \frac{k}{n}$ où k est le nombre de classes de conjugaisons dans G,
3. $p = \frac{5}{8}$ pour $G = H_8$.

4.2 Groupe dérivé

Définition 46 (PER $p.13$)**.** On définit $D(G) = \langle xyx^{-1}y^{-1}; x, y \in G\rangle$.

Proposition 47 (PER $p.13$)**.** $D(G)$ est le plus petit (pour l'inclusion) sous-groupe distingué de G induisant un quotient abélien.

Exemple 48 (PER $p.13$)**.** $D(G) = \{e_G\} \iff G$ est abélien.
$D(\mathfrak{S}_5) = \mathfrak{A}_5$
$D(H_8) = \{1, -1\}$
Si G est simple et non abélien alors $D(G) = G$.
$D(\mathrm{GL}_n(\mathbb{K}) = \mathrm{SL}_n(\mathbb{K})$ sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$
$D(\mathrm{SL}_n(\mathbb{K}) = \mathrm{SL}_n(\mathbb{K})$ sauf si $n = 2$ et $\mathbb{K} \in \{\mathbb{F}_2, \mathbb{F}_3\}$.

4.3 Théorèmes de Sylow

On fixe G un groupe fini d'ordre $p^\alpha m$ avec $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$ et $m \wedge p = 1$.

Définition 49 (PER, $p.18$)**.** Un p-Sylow de G est un sous-groupe de G d'ordre p^α.

Exemple 50 (PER, $p.18$)**.** Si $p \in \mathbb{P}$ et $n \geqslant 1$, le sous-groupes des matrices triangulaires supérieures strictes est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Lemme 51 (PER, $p.19$)**.** Si $H \subset G$ et si G admet un p-Sylow S, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Théorème 52 (PER, $p.18$-19)**.**

1. G admet un p-Sylow.
2. Tous les p-Sylow de G sont conjugués.
3. Si n_p désigne le nombre de p-Sylow de G, on a $n_p \in m$ et $n_p \equiv 1 \pmod p$.

Corollaire 53 (PER, $p.19$)**.** Soit S un p-Sylow de G. On a $S \triangleleft G \iff n_p = 1$.

Application 54. Si $|G| = pq^m$ avec $m \geqslant 1$, $p, q \in \mathbb{P}$ et $p < q$ alors G n'est pas simple.
Si $|G| = pqr$ avec $p, q, r \in \mathbb{P}$ tous distincts, G n'est pas simple.

Application 55 (Développement 2)**.** A_5 est le seul groupe simple d'ordre 60.

4.4 Produit semi-direct

Définition 56 (PER, $p.22$)**.** Soient N et H deux groupes et $\varphi : H \to \mathrm{Aut}(N)$ un morphisme de groupes. Le produit semi direct de N par H relativement à φ est le produit cartésien $N \times H$ muni de la loi

$$(n, h)(n', h') = (n\varphi(h)(n'), hh').$$

On le note $N \rtimes_\varphi H$.

Théorème 57 (PER, $p.22$)**.** Avec les notations précédentes,

1. $G = N \rtimes_\varphi H$ est un groupe.
2. $N' = N \times \{e_H\}$ et $H' = \{e_N\} \times H$ sont des sous-groupes de G isomorphes à N et H.
3. $N' \triangleleft G$.
4. $G = N'H'$.
5. $N' \cap H' = \{e_G\}$.
6. L'action de H sur N correspond, dans G, à la conjugaison par H sur N.

Exemple 58 (PER, $p.23$)**.** Un produit semi-direct est un produit direct si et seulement si l'action est trivial.

Théorème 59 (Critère de dévissage, PER, $p22$)**.** Soit G un groupe possédant deux sous-groupes H, N vérifiant

$$N \triangleleft G, \quad G = NH, \quad N \cap H = \{e_G\}.$$

Alors, $G \simeq N \rtimes H$ où l'action est la conjugaison.

Exemple 60 (PER, $p.23$-24)**.** Si $\sigma = (12) \in \mathfrak{S}_n$, on a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \langle\sigma\rangle$.
Le groupe diédral D_n est un produit semi-direct.
H_8 n'est pas un produit semi-direct.

Lemme 61 (PER, $p.24$)**.** Si $p \in \mathbb{P}$, on a $\mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Application 62 (PER, $p.27$)**.** Soit G de cardinal pq avec $p, q \in \mathbb{P}$ et $p < q$.

1. Si $p \nmid q - 1$, $G \simeq \mathbb{Z}/pq\mathbb{Z}$.
2. Si $p \mid q - 1$ alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ où $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ et la classe d'isomorphie ne dépend pas de l'action (non triviale).

Références

[PER] : D. Perrin - Cours d'algèbre.
[ESC] : J-P. Escofier - Toute l'algèbre de la licence (6ème édition).
[SZP] : A. Szpirglas - Mathématiques Algèbre L3.
[CAL] : P. Caldero - Carnet de voyage en Analystan.

Développements

[Développement 1] : Lemme 12, Lemme 13 et Théorème 14.
[Développement 2] : Application 55.

Développement 1

Théorème de Wedderburn

Preuve du Lemme 12 :
Soit $n \in \mathbb{N}^*$. L'ordre d'une racine n-ième de l'unité étant un diviseur de n, on a

$$\begin{aligned}\mathbb{U}_n &= \{z \in \mathbb{C}^* \mid z^n = 1\} \\ &= \bigsqcup_{d|n} \{z \in \mathbb{C}^* \mid o(z) = d\} \\ &= \bigsqcup_{d|n} \mathbb{U}_d^*\end{aligned}$$

et donc

$$\begin{aligned}X^n - 1 &= \prod_{z \in \mathbb{U}_n} (X - z) \\ &= \prod_{d|n} \prod_{z \in \mathbb{U}_d^*} (X - z) \\ &= \prod_{d|n} \Phi_d.\end{aligned}$$

En particulier, si d divise strictement n et si $q > 2$, on a

$$\frac{q^n - 1}{q^d - 1} = \prod_{\substack{k|n \\ k \nmid d}} \Phi_k(q) = \Phi_n(q) \prod_{\substack{k|n \\ k \nmid d \\ k \neq n}} \Phi_k(q)$$

donc $\Phi_n(q) \mid \dfrac{q^n - 1}{q^d - 1}$.

Preuve du Lemme 13 :
Soient $n, d \in \mathbb{N}^*$ et $q \geqslant 1$ tels que $q^d - 1 \mid q^n - 1$. On pose la division euclidienne $n = dq + r$ de n par d. On a

$$q^d - 1 \mid q^{dq+r} - 1 - (q^d - 1) = q^{dq+r} - q^d = q^d(q^{d(q-1)+r} - 1)$$

et comme $q^d \wedge q^d - 1 = 1$, le lemme de Gauss nous donne $q^d - 1 \mid q^{d(q-1)+r} - 1$. En itérant, on trouve $q^d - 1 \mid q^r - 1$ mais $0 \leqslant r < d$ et $q \geqslant 2$ donc $r = 0$, c'est-à-dire $d \mid n$.

Preuve du Théorème 14 :
Soit $\mathbb{K}$ un corps fini. On considère l'action par conjugaison de $\mathbb{K}^*$ sur lui-même. Remarquons que le centre $Z(\mathbb{K})$ de $\mathbb{K}$ est un sous-corps commutatif de $\mathbb{K}$. Ainsi, si $q = |Z(\mathbb{K})|$, il existe $n \in \mathbb{N}$ tel que $|K| = q^n$. De même, si $g \in \mathbb{K}$, $C_{\mathbb{K}}(g) = \{h \in \mathbb{K} \mid gh = hg\}$ est un sous-corps de $\mathbb{K}$ contenant $Z(\mathbb{K})$ donc il existe $n_g \in \mathbb{N}$ tel que $|C_{\mathbb{K}}(g)| = q^{d_g}$. De plus, si $g \in \mathbb{K}^*$, on a $N_{\mathbb{K}^*}(g) = C_{\mathbb{K}}(g)^*$.

Raisonnons par l'absurde et supposons que $\mathbb{K}^* \backslash Z(\mathbb{K})^*$. Si $\mathcal{R}$ est un système de représentants des orbites non ponctuelles, l'équation au classes donne alors

$$\begin{aligned}q^n - 1 &= \sum_{g \in \mathcal{R}} |\mathbb{K}^* : N_{\mathbb{K}^*}(g)| \\ &= \sum_{\substack{g \in \mathcal{R} \\ g \in Z(\mathbb{K})^*}} 1 + \sum_{\substack{g \in \mathcal{R} \\ g \notin Z(\mathbb{K})^*}} |\mathbb{K}^* : N_{\mathbb{K}^*}(g)| \\ &= q - 1 + \sum_{\substack{g \in \mathcal{R} \\ g \notin Z(\mathbb{K})^*}} \frac{q^n - 1}{q^{n_g} - 1}.\end{aligned}$$

Dans la dernière somme, n_g est un diviseur strict de n pour tout g d'après le Lemme 13 et donc $\Phi_n(q)$ divise cette même somme. De plus, $\Phi_n(q) \mid q^n - 1$ donc $\Phi_n(q) \mid q - 1$. Or, on a

$$\begin{aligned}|\Phi_n(q)| &= \left| \prod_{z \in \mathbb{U}_n^*} (q - z) \right| \\ &= \prod_{z \in \mathbb{U}_n^*} |q - z| \\ &> \prod_{z \in \mathbb{U}_n^*} |q - |z|| \\ &= \prod_{z \in \mathbb{U}_n^*} (q - 1) \\ &\geqslant q - 1\end{aligned}$$

car $1 \notin \mathbb{U}_n^*$ étant donné que $n \geqslant 2$ et car $q \geqslant 2$. On aboutit donc à une absurdité et on en conclut que $\mathbb{K}^* = Z(\mathbb{K})^*$, donc que $\mathbb{K}$ est commutatif.

Développement 2

Groupe simple d'ordre 60

Unicité :
Soit G un groupe simple d'ordre 60. On va montrer que G agit non trivialement sur un ensemble à 5 éléments. Nous allons raisonner par l'absurde en supposant l'hypothèse

$$(H) : G \text{ n'admet pas de sous-groupe strict d'indice } \leqslant 5.$$

Pour $p \in \mathbb{P}$, notons $E_p(G)$ l'ensemble des p-Sylow de G et n_p le cardinal de $E_p(G)$. L'action de G sur ses 2-Sylow étant transitive, n_2 est l'indice d'un stabilisateur, donc d'un sous-groupe de G. Comme $|G| = 60 = 2^2 \cdot 3 \cdot 5$, on a $n_2 \mid 15$ donc $n_2 \in \{1, 3, 5, 15\}$ mais par (H), on ne peut avoir que $n_2 \in \{1, 15\}$. G étant simple, on ne peut pas avoir $n_2 = 1$ d'où $n_2 = 15$.
Comptons maintenant le nombre d'éléments présents dans ces 2-Sylow. Soient S_1 et S_2 deux 2-Sylow distincts de G. Si $g \in S_1 \cap S_2$. Considérons le centralisateur $N_G(g)$ de g dans G. On a

$$\begin{cases} o(N_G(g)) > 4 \text{ car } N_G(g) \supset S_1 \cup S_2, \\ 4 \mid o(N_G(g)) \text{ car } N_G(g) \subset S_1, \\ o(N_G(g)) \mid 60 \text{ car } N_G(g) \subset G. \end{cases}$$

Ainsi, on a $o(N_G(g)) \in \{12, 20, 60\}$ mais (H) implique que $o(N_G(g)) \neq 12, 20$ donc $o(N_G(g)) = 60$ et $g \in Z(G) = \{e_G\}$ (car G simple d'ordre non premier). Ainsi, on a $S_1 \cap S_2 = \{e_G\}$.
G contient donc $3 \cdot 15 = 45$ éléments d'ordre 2 ou 4.
Comptons maintenant les éléments d'ordre 5 de G. On a $n_5 \mid 12$ et $n_5 \equiv 1 \pmod 5$ donc $n_5 \in \{1, 6\}$ et une fois de plus, G est simple donc $n_5 \neq 1$ ce qui implique que $n_5 = 6$. Les 5-Sylow de G étant de cardinal premier 5, deux 5-Sylow distincts s'intersectent trivialement et G possède $4 \cdot 6 = 24$ éléments d'ordre 5.
On a donc montré que G possède au moins $45 + 24 = 69$ éléments, ce qui est absurde puisque $|G| = 60$. On en conclut que l'hypothèse (H) est erronée.
Soit $K \subset G$ un sous-groupe strict d'indice inférieur ou égal à 5.
Si $|G : H| = 5$, l'action (transitive donc non-triviale) de G sur G/H fournit un morphisme $G \to \mathfrak{S}_5$. Ce morphisme étant non-trivial et G étant simple, il est injectif et G s'identifie à sous-groupe d'indice 2 de S_5. Par unicité, de ce dernier, on obtient un isomorphisme entre G et $\mathfrak{A}_5$.
Si $|G : H| \leqslant 4$, le même raisonnement implique que G est isomorphe à un sous-groupe de $\mathfrak{S}_{|G:H|}$, ce qui est absurde puisque

$$|G| = 60 > |G : H|! = |\mathfrak{S}_{|G:H|}|.$$

Existence : Montrons que $\mathfrak{A}_5$ est simple. Le groupe $\mathfrak{A}_5$ contient :

- 1 neutre,
- 20 3-cycles,
- 24 5-cycles,
- 15 bitranspositions.

Soit $H \triangleleft \mathfrak{A}_5$ différent de $\{\text{id}\}$. Si H contient un 3-cycle, il les contient tous et comme ils engendrent $\mathfrak{A}_5$, on a $H = \mathfrak{A}_5$.
Supposons que H ne contienne pas de 3-cycle. Supposons de plus que H contienne un 5-cycle. Les 5-Sylow de $\mathfrak{A}_5$ étant de cardinal 5, ils sont engendrés par les 5-cycles. Or, $\mathfrak{A}_5$ agit transitivement sur ses 5-Sylow donc H contient tous les 5-Sylow de $\mathfrak{A}_5$ et donc tous les 5-cycles de $\mathfrak{A}_5$. Puisque $25 \not| \ |\mathfrak{A}_5|$, H contient également une bitransposition $(ij)(kl)$. On a alors

$$(ij)(kl)(klijm) = (mlj) \in H,$$

ce qui est absurde.
Ainsi, H ne peut pas contenir de 5-cycle et il ne contient que des bitranspositions. Pour tout $g \in H$, on a donc $g^2 = \text{id}$ et donc H est un 2-groupe. Il est même de cardinal 2 ou 4 d'après le théorème de Lagrange. Si H était de cardinal 2, il contiendrait un élément non nul et central dans $\mathfrak{A}_5$ ce qui est absurde donc H est de cardinal 4. H est donc un 2-Sylow distingué de $\mathfrak{A}_5$ mais ce dernier admet plusieurs 2-Sylow : $\{\text{id}, (12)(34), (13)(24), (14)(23)\}$ et $\{\text{id}, (23)(45), (24)(35), (25)(35)\}$ par exemple, donc H ne peut pas être distingué, ce qui est absurde.
Ainsi, le seul cas possible est le cas $H = \mathfrak{A}_5$ et donc $\mathfrak{A}_5$ est simple.

Les 6 minutes :

- La conjugaison est une action d'un groupe sur lui-même.
- Calcul direct de classes de conjugaison.
- Interprétation géométrique.
- Sous-groupe distingué pour structure de groupe sur le quotient.
- Utilité des quotients pour la classification.
- Caractérisation interne des produits directs, exemple en géométrie et en arithmétique.
- Les groupes simples sont des briques élémentaires.
- Théorèmes de Sylow, produits semi-directs et application à la classification.