Fiche 1 : les corrigés de certains exercices

Exercice 6 *Soient G un groupe, N un sous-groupe distingué et $\pi : G \longrightarrow G/N$ l'homomorphisme canonique. Démontrer que la correspondance qui associe à chaque sous-groupe L de G/N le sous-groupe $\pi^{-1}(L)$ représente une bijection entre les sous-groupes de G/N et les sous-groupes de G contenant N. De plus, cette correspondance préserve les sous-groupes distingués et les indices des sous-groupes.*

Réponse : Nous vérifierons les conclusions en plusieurs étapes. Nous gardons la notation de l'énoncé. Soulignons un point mineur mais important : la notation π^{-1} est utilisée pour noter l'image inverse d'une partie de l'ensemble d'arrivée, en l'occurrence le groupe G/N. L'homomorphisme canonique n'est pas nécessairement une injection, et par conséquent il n'est pas possible de parler de son inverse. En fait, π devient intéressant quand il n'est pas injectif.

Etape 1 Si $L \leq G/N$ alors $\pi^{-1}(L)$ est un sous-groupe de G contenant N.

Soit $H = \pi^{-1}(L)$. Que H soit un sous-groupe de G est une conséquence générale. Si vous en doutez ou si vous ne voyez pas comment faire, c'est un bon moment pour combler cette lacune qui ne doit plus exister parmi vos connaissances.

Vérifions que H contient N. Il suffira de montrer que $\pi^{-1}(\{1\}) = \ker(\pi) = N$. Rappelons que l'élément neutre du groupe G/N est la classe N. D'après la définition de π, $\pi(g) = gN$. Alors, $\pi^{-1}(\{1\}) = \{g \in G \mid gN = N\}$. Comme N est un sous-groupe, $gN = N$ si et seulement si $g \in N$ (vérifiez si vous avez des doutes). Ainsi $N = \pi^{-1}(\{1\})$. Puisque L contient l'élément neutre de G/N, $H = \pi^{-1}(L)$ contient N.

Etape 2 Tout sous-groupe L de G est de la forme H/N avec $H = \pi^{-1}(L)$.

Cette conclusion est immédiate après la première étape. Soulignons que la notation est cohérente puisque H contient N et que, N étant distingué dans tout sous-groupe de G qui le contient, H/N est un groupe.

Etape 3 L'application Π qui associe à chaque sous-groupe sous-groupe de G/N son image inverse par rapport à π est une bijection entre les sous-groupes de G/N et ceux de G qui contiennent N.

Il reste à vérifier la bijectivité de Π. Pour ce faire, il suffit de lui trouver une application inverse. Celle-ci est l'application qui associe à tout sous-groupe H de G qui contient N le sous-groupe H/N. Notons que cette application de l'ensemble des sous-groupe de G contenant N vers l'ensemble des sous-groupes de G/N est induite par π. En effet,

$$H/N = \{hN \mid h \in H\} = \pi(H) \ .$$

Etape 4 La correspondance bijective de l'étape 3 préserve les sous-groupes distingués.

Nous montrerons que si H est un sous-groupe de G qui contient N alors H est distingué dans G si et seulement si H/N est distingué dans G/N. Rappelons d'abord que, N étant distingué, si $g \in G$ alors $gNg^{-1} = N$. Ainsi, pour tout $g \in G$, $N \leq gHg^{-1}$. Alors, $gHg^{-1} = H$ si et seulement si $gHg^{-1}/N = H/N$ si et seulement si $gN\ H/N\ (gN)^{-1} = gN$.

Etape 5 La correspondance bijective de l'étape 3 préserve les indices des sous-groupes.

Nous montrerons que si H est un sous-groupe de G contenant N alors l'application qui associe à une classe gH de H dans G, la classe $gN\ H/N$ de H/N dans G/N est une bijection. Avant de procéder, soulignons que H n'est *pas* nécessairement distingué.

L'application définie dans le paragraphe précédent est une surjection. Pour voir que c'est une injection supposons que $gN\ H/N = g'N\ H/N$. Ceci équivaut à $(g'N)^{-1}(gN) \in H/N$, qui est équivalent à dire que $g'^{-1}g \in H$. Ce dernier n'est qu'une autre forme de l'égalité $g'H = gH$. Nous avons donc vérifié la propriété injective.

Etape 6 Généralisons un peu.

Que pouvons-nous dire de l'image par rapport à π d'un sous-groupe quelconque de G. Soit H un tel sous-groupe. Il n'est donc pas nécessaire que H contienne N. Néanmoins, comme N est distingué, la partie $HN = \{hn \mid h \in H \text{ et } n \in N\}$ est en fait un sous-groupe de G. Ce sous-groupe contient aussi N. Alors, les points qui précèdent nous montrent que l'application de l'étape 3 fait correspondre à HN le sous-groupe HN/N dans G/N. C'est en fait l'image direct de H par rapport à π. □

Exercice 7 (c)

(*i*) *Montrer que les sous-groupes de* $(\mathbb{R}, +)$ *sont soit monogènes, soit denses.*

(*ii*) *Donner un exemple de sous-groupe dense de* $(\mathbb{R}, +)$ *de type fini.*

(*iii*) *Tous les sous-groupes de* $(\mathbb{R}, +)$ *sont-ils de type fini ?*

Réponse : (i) Il suffira de montrer que si $H \leq G$ et que H n'est pas dense dans $\mathbb{R}$, alors H est monogène. Rappelons le sens du mot *dense* : H est un sous-groupe dense si pour tout $\alpha < \beta$, nombres réels, $]\alpha, \beta[\cap H \neq \emptyset$.

Nous pouvons supposer $H \neq \langle 0 \rangle$. Comme H est supposé ne pas être dense, il existe $\alpha < \beta \in \mathbb{R}$ tels que $]\alpha, \beta[\cap \mathbb{R} = \emptyset$. Nous pouvons supposer que $\alpha,\ \beta \in \mathbb{R}^+$ puisque sinon $\alpha < \beta < 0$, et dans ce cas, ils peuvent être remplacés par $-\alpha$ et $-\beta$.

Posons maintenant

$$\alpha_0 = \inf\{\alpha \in \mathbb{R}_+ \mid \text{il existe } \beta \in \mathbb{R} \text{ tel que } \beta > \alpha \text{ et que }]\alpha, \beta[\cap H = \emptyset\} \ .$$

Un tel α_0 existe. Nous montrerons que $\alpha_0 = 0$. Par l'absurde, supposons que $0 < \alpha_0$. D'après la définition de α_0, pour tout $\delta \in \mathbb{R}_+^*$, il existe α_δ tel que $\alpha_\delta \in]\alpha_0, \alpha_0 + \delta[$, et que, à droite de α_δ, il existe un intervalle ouvert $]\alpha_\delta, \beta_\delta[$ dont l'intersection avec H est vide. Puisque δ est arbitraire, nous pouvons fixer une valeur strictement inférieure à α_0. Alors

$$0 < \alpha_0 - \delta < \alpha_\delta - \delta < \alpha_0 \ .$$

Cette translation de valeur δ fait apparaître dans $]0, \alpha_0[$ un intervalle ouvert non vide à droite de $\alpha_\delta - \delta$ qui n'intersecte pas H (voyez-vous pourquoi ?). Or, $]0, \alpha_0[\cap H$ est dense dans $]0, \alpha_0[$. Cette contradiction montre que $\alpha_0 = 0$.

Une conséquence du paragraphe précédent est qu'il existe un plus petit élément *strictement* positif de H. Notons-le α. Par récurrence, et en translatant l'intervalle $]0, \alpha[$, nous en déduisons que $]n\alpha, (n+1)\alpha[\cap H = \emptyset$ pour tout $n \in \mathbb{N}$. Ceci s'étend à tous les intervalles de la même forme, cette fois-ci avec $n \in \mathbb{Z}$, après passage à l'inverse dans le groupe G. Nous avons donc montré que $H = \langle \alpha \rangle$.

(ii) Pour répondre à ce point, nous pouvons utiliser le point (i). Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Posons $H = (\{a + b\alpha \mid a, b \in \mathbb{Z}\}, +)$. Alors $H \leq G$. Le sous-groupe H est engendré par 1 et α. Par conséquent, il est de type fini. Maintenant vérifions qu'il n'est pas monogène.

Par l'absurde supposons qu'il existe $r \in \mathbb{R}$ tel que $H = \langle r \rangle$. Comme $1 \in \{a + b\alpha \mid a, b \in \mathbb{Z}\}$, nécessairement $\alpha \in \mathbb{Q}$. Or, $\alpha \in \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ aussi sans pour autant appartenir à $\mathbb{Q}$. Par conséquent il n'existe pas de $n \in \mathbb{Z}$ tel que $nr = \alpha$.

(iii) Tous les sous-groupes de $(\mathbb{R}, +)$ ne sont pas de type fini. Il existe plusieurs approches pour voir pourquoi. Une qui est légèrement insolite mais intéressante nécessite un modeste recours à l'arithmétique des cardinaux. Néanmoins, elle est très efficace. En effet, il suffit de vérifier qu'un groupe de type fini est forcément dénombrable. Ensuite, comme l'ensemble des nombres réels n'est pas dénombrable (pouvez-vous montrer pourquoi ?), le groupe $(\mathbb{R}, +)$, qui est un sous-groupe de lui-même, n'a aucune chance d'être de type fini.

Une autre approche utilise l'arithmétique élémentaire comme c'est fréquemment fait dans ce cours. Elle permet en particulier de trouver des sous-groupes *dénombrables* qui ne sont pas de type fini. En effet, le sous-groupe $(\mathbb{Q}, +)$ n'est pas de type fini : si $X = \left\{ \frac{p_i}{q_i} \mid 1 \leq\ n\ ,\ p_i \in \mathbb{N}\ ,\ q_i \in \mathbb{N}^* \right\}$ est une partie finie arbitrairement choisie de $\mathbb{Q}$, alors l'élément $\frac{1}{p}$, où p est un nombre premier qui n'apparaît dans la factorisation première d'aucun des q_i, n'appartient pas au sous-groupe engendré par X. Les détails sont laissés aux lecteurs. □

Exercice 8 (c) (v) *Montrer que* $\liminf \frac{\phi(n)}{n} = 0$.

Réponse : Nous vérifierons l'énoncé suivant :

$$\lim_{n\to+\infty} \frac{\phi(n!)}{n!} = 0 \ .$$

Cette conclusion est suffisante pour déduire l'énoncé de l'exercice.

Montrons d'abord que si $n \in \mathbb{N}^*$ et d un diviseur de n, alors

$$\frac{\phi(d)}{\phi(n)} \geq \frac{d}{n} \ .$$

D'après le théorème de la factorisation unique des nombres naturels, il existe k nombre premiers $p_1 < \ldots < p_k$ et k nombres naturels non nuls $\alpha_1, \ldots, \alpha_k$ tels que $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Alors, d est de la forme $d = p_{i_1}^{\beta_{i_1}} \ldots p_{i_j}^{\beta_{i_j}}$, où $\beta_{i_r} \in \{1, \ldots, \alpha_{i_r}\}$ et $r \in \{1, \ldots, j\}$. Par conséquent,

$$\begin{aligned}
\frac{\phi(d)}{\phi(n)} &= \frac{p_{i_1}^{\beta_{i_1}-1}(p_{i_1}-1)\ldots p_{i_j}^{\beta_{i_j}-1}(p_{i_j}-1)}{p_1^{\alpha_1-1}(p_1-1)\ldots p_{i_1}^{\alpha_{i_1}-1}(p_{i_1}-1)\ldots p_{i_j}^{\alpha_{i_j}-1}(p_{i_j}-1)\ldots p_k^{\alpha_k-1}(p_k-1)} \\
&= \frac{p_{i_1}^{\beta_{i_1}}\ldots p_{i_j}^{\beta_{i_j}}}{p_1^{\alpha_1-1}(p_1-1)\ldots p_{i_1}^{\alpha_{i_1}}\ldots p_{i_j}^{\alpha_{i_j}}\ldots p_k^{\alpha_k-1}(p_k-1)} \\
&\geq \frac{d}{p_1^{\alpha_1}\ldots p_k^{\alpha_k}} \\
&= \frac{d}{n}
\end{aligned}$$

Maintenant, nous utiliserons la conclusion technique que nous venons d'obtenir pour démontrer que

$$\lim_{n\to+\infty} \frac{n!}{\phi(n!)} = +\infty \ .$$

Ceci sera suffisant pour conclure. Le point technique nous permet de conclure que

$$\begin{aligned}
\frac{n!}{\phi(n!)} &= \frac{\sum_{d|n!}\phi(d)}{\phi(n!)} \\
&= \sum_{d|n!} \frac{\phi(d)}{\phi(n!)} \\
&\geq \sum_{d|n!} \frac{d}{n!} \ .
\end{aligned}$$

Comme $d = 1.2.\ldots.(k-1).(k+1)\ldots n \ \ (1 \leq k \leq n)$ est un diviseur de $n!$, nous concluons que pour tout $n \in \mathbb{N}^*$,

$$\frac{n!}{\phi(n!)} \geq \sum_{k=1}^{n} \frac{1}{k} \ .$$

Alors

$$\lim_{n\to+\infty} \frac{n!}{\phi(n!)} \geq \lim_{n\to+\infty} \sum_{k=1}^{n} \frac{1}{k} = +\infty \ .$$

□

Exercice 11

(*a*) *Soit G un groupe fini d'ordre n tel que pour tout diviseur d de n, il y ait au plus d éléments g de G vérifiant $g^d = 1$. Montrer que G est cyclique.*

(*b*) *Montrer que le groupe multiplicatif d'un corps commutatif fini est cyclique. En déduire que* $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}, +)$ (*p premier*) *est isomorphe à* $\mathbb{Z}_{p-1}$.

Réponse (a) Supposons par l'absurde qu'il existe un groupe fini G d'ordre n qui satisfait les hypothèses de l'exercice sans pour autant être cyclique. Forcément $G \neq \{1\}$ et G n'est engendré par aucun de ses éléments.

Nous vérifions d'abord un point technique qui sera utile. Pour tout $g \in G$, le sous-groupe $\langle g \rangle$ est distingué dans G. En effet, le sous-groupe engendré par g contient exactement $|g|$ éléments qui satisfont l'équation $x^{|g|} = 1$. D'après l'hypothèse générale de l'exercice, G n'a pas d'autres éléments qui satisfont cette équation puisque $|g|$ est un diviseur de n. Or, pour tout diviseur d de $|G|$, tout $h \in G$, et tout $x \in G$, $x^d = 1$ si et seulement si hxh^{-1}. Par conséquent, $h\langle g \rangle h^{-1} = \langle g \rangle$ pour tout $h \in H$.

Maintenant, parmi les éléments de G, fixons g d'ordre maximal. D'après l'hypothèse contradictoire, il existe $h \in G \setminus \langle g \rangle$. Nous arriverons à une contradiction en explicitant un sous-groupe *cyclique* de G qui contient $\langle g \rangle$ proprement.

Premièrement, montrons que si d est un diviseur commun de $|g|$ et de $|h|$ alors d est aussi un diviseur de $|\langle g \rangle \cap \langle h \rangle|$. En effet, si d divise $|g|$, alors, en utilisant des connaissances antérieures sur les groupes cycliques ou l'exercice 8.(a) de cette fiche, nous déduisons que $\langle g \rangle$ contient un sous-groupe d'ordre d. Par conséquent, $\langle g \rangle$ contient d éléments qui satisfont l'équation $x^d = 1$. D'après l'hypothèse de l'exercice, $\langle g \rangle$ contient alors tous les éléments de G satisfaisant cette équation. Le même raisonnement s'applique bien sûr au sous-groupe $\langle h \rangle$. Alors, l'intersection $\langle g \rangle \cap \langle h \rangle$ contient tous ces éléments, et par conséquent, le sous-groupe qu'ils forment. Ainsi, $d \mid |\langle g \rangle \cap \langle h \rangle|$.

De la conclusion du paragraphe précédent découle que si $d = |g| \wedge |h|$, alors $d = |\langle g \rangle \cap \langle h \rangle|$. Posons $h' = h^d$. Nous montrerons que $\langle g, h' \rangle$ est un sous-groupe cyclique de G qui est strictement plus grand que G, ce qui contredira notre choix de g d'ordre maximal. Notons que $|h'| = \frac{|h|}{d}$ et que ce nombre est premier avec $|g|$ d'après le choix de d.

Vérifions maintenant que $h' \notin \langle g \rangle$. Comme $|h'| \wedge |g| = 1$, si $h' \in \langle g \rangle$ alors la seule possibilité est que $h' = 1$. Or ceci impliquerait que $h \in \langle g \rangle$ (voyez-vous pourquoi ?), et contredirait le choix $h \in G \setminus \langle g \rangle$. Par conséquent, $h' \notin \langle g \rangle$. En fait, $\langle h' \rangle \cap \langle g \rangle = 1$ vu que $|h'| \wedge |g| = 1$.

D'après ce que nous avons vérifié au tout début, $\langle h' \rangle \lhd G$ et $\langle g \rangle \lhd G$. Il en découle, en utilisant la conclusion $\langle h' \rangle \cap \langle g \rangle = 1$, que g et h' commutent (vérifiez les détails). Cette conclusion et celle du paragraphe précédent comme quoi $|h'| \wedge |g| = 1$ impliquent que le produit gh' engendre le sous-groupe $\langle g, h' \rangle$ (vérifiez les détails). Or, $\langle g \rangle < \langle g, h' \rangle$ puisque $h' \in G \setminus \langle g \rangle$. Ceci contredit le choix maximal de $|g|$.

(b) La vérification du premier énoncé du point (b) utilisera la conclusion du point (a). Nous montrerons un résultat plus fort : si $(K, +, ., 0, 1)$ est un corps commutatif quelconque, alors tout groupe fini du groupe multiplicatif $(K^*, .)$ est cyclique.

Soient H un sous-groupe fini de $(K^*, .)$ et $d \in \mathbb{N}^*$ un diviseur de $|H|$. Pour pouvoir appliquer le point (a) il suffira de montrer que H a au plus d éléments d'ordre d. En d'autres termes, nous devons compter le nombre de solutions de l'équation $x^d = 1$. C'est une équation définie en utilisant la loi interne . et l'élément neutre multiplicatif. Or, comme K est un corps, y est définie aussi un loi interne additive. En utilisant l'addition nous pouvons reformuler notre équation : $x^d - 1 = 0$. Maintenant, il s'agit d'une équation polynômiale, et notre objectif consiste à majorer le nombre des racines du polynôme $x^d - 1$. Comme K est un corps commutatif, il en existe au plus d. Cette majoration est suffisante pour appliquer le résultat du point (a) et conclure.

Le deuxième énoncé est une conséquence immédiate de l'exercice 9.(b). □

Exercice 19 *Soit G un groupe. On dit qu'un sous groupe H de G est maximal si $H \neq G$ (un sous-groupe* propre*), et si pour tout sous-groupe N de G, $H \subset N \subset G$ implique $N = G$ ou $N = H$.*

(*a*) *Les sous-groupes maximaux sont-ils nécessairement isomorphes entre eux ?*

(*b*) *Montrer que l'intersection de deux sous-groupes commutatifs distincts est incluse dans le centre de G.*

(*c*) *Si G est fini, simple et non commutatif, alors G contient deux sous-groupes maximaux H et H' tels que $H \cap H' \neq \{e\}$ (on utilisera le fait que G ne peut être la réunion des conjugués de H).*

(*d*) *Un groupe simple, fini et non commutatif contient un sous-groupe maximal non commutatif.*

Réponse : (a) La réponse à la question est négative. Il n'est pas nécessaire d'aller très loin pour trouver des groupes avec des sous-groupes maximaux qui ne sont pas isomorphes. En effet, les groupes d'ordre 6 sont tous des exemples de ce phénomène. Considérons donc $(\mathbb{Z}/6\mathbb{Z}, +)$ et $\mathfrak{S}_3$ (d'ailleurs, à isomorphisme près c'est la liste complète) des groupes d'ordre 6.). Le premier a deux sous-groupes maximaux, l'un d'ordre 3, l'autre d'ordre 2, engendrés par les classes $\overline{2}$ et $\overline{3}$ respectivement. Ces deux sous-groupes n'ont aucune chance d'être isomorphes. Notons aussi que ces deux sous-groupes maximaux s'intersectent trivialement, contrairement à ce qui sera démontré dans le point (c) ci-dessous ; $(\mathbb{Z}/6\mathbb{Z}, +)$ est loin d'être simple et non commutatif.

Quant au groupe symétrique $\mathfrak{S}_3$, il a trois sous-groupes d'ordre 2 qui sont tous conjugués, notamment $\langle(1,2)\rangle$, $\langle(1,3)\rangle$, $\langle(2,3)\rangle$, et un seul d'ordre 3, qui est $\langle(1,2,3)\rangle$. Tous ces sous-groupes sont maximaux. Ceux qui sont d'ordre 2 sont isomorphes, voire conjugués. Mais ils ne sont pas isomorphes au sous-groupes $\langle(1,2,3)\rangle$. Notons comme dans le paragraphe précédent que les intersections deux à deux de ces quatre sous-groupes sont toutes égales à $\{1\}$. Le groupe $\mathfrak{S}_3$ n'est pas commutatif mais il n'est pas simple non plus puisque $\langle(1,2,3)\rangle$ est distingué.

Avant de passer au point (b), donnons un exemple de groupe dans lequel tous les sous-groupes non triviaux, propres ou non, sont isomorphes. Il s'agit, comme vous avez peut-être déjà deviné, de $(\mathbb{Z}, +)$. Les sous-groupes maximaux sont exactement ceux qui sont de la forme $(p\mathbb{Z}, +)$ avec p un nombre premier.

(b) Soient H et H' deux sous-groupes maximaux et distincts de G qui sont commutatifs par hypothèse. Si $x \in H \cap H'$ alors le *centralisateur dans G de x*, $C_G(x) = \{g \in G \mid gx = xg\}$, qui est un sous-groupe (vérifiez si vous n'avez jamais essayé) de G, contient à la fois H et H'. Comme ces deux sous-groupes sont distincts, l'inclusion $H \subset C_G(x)$ est stricte. Or, H est supposé maximal. Ainsi $C_G(x) = G$, ce qui est équivalent à dire que $x \in Z(G)$ (le centre de G). Bien sûr, nous aurions pu faire le même raisonnement avec H' au lieu de H.

(c) Soit maintenant G un groupe fini, simple et non commutatif. En particulier, $G \neq \{1\}$. Nous montrerons par l'absurde que G a deux sous-groupes maximaux H et H' qui ont une intersection non triviale, c'est à dire différente de $\{1\}$.

Pour mieux comprendre la notion de sous-groupe maximal, montrons certaines conclusions relativement simples mais importantes. Pourquoi est-ce que G a un sous-groupe maximal ? Plus généralement, est-il vrai que tout élément de G est contenu dans un sous-groupe maximal ? Les réponses sont toujours affirmatives. Si $g \in G$, alors on considère la famille suivante de sous-groupes propres de G :

$$\mathcal{H}_g = \{H < G \mid g \in H\} .$$

Cette famille n'est pas vide puisqu'elle contient $\langle g\rangle$. En effet, comme G n'est pas commutatif, G ne peut pas être monogène non plus. Comme G est fini, $\mathcal{H}_g$ est une famille finie. Alors, on choisit un élément de $\mathcal{H}_g$ d'ordre maximal. Notons que H peut contenir d'autres sous-groupes maximaux que cette méthode de choix en donne mais il nous suffit d'en trouver un.

Le paragraphe précédent a montré que la non commutativité et la finitude de G suffisent pour mettre tout élément de g dans un sous-groupe maximal de G. En particulier, G a des sous-groupes maximaux non triviaux. Montrons qu'il en existe au moins deux avant d'attaquer le coeur de l'exercice. La simplicité jouera un rôle important.

Dans tout groupe G, si H est un sous-groupe maximal, alors pour tout $g \in G$ le conjugué gHg^{-1} est maximal aussi (la vérification est un bon exercice ; en fait vous pouvez remplacer la conjugaison par un automorphisme quelconque de G). Par conséquent, si G a un seul sous-groupe maximal H, alors H sera stable par rapport à la conjugaison. Il sera donc distingué. Or, dans notre exercice G est supposé simple. Puisque $H \neq G$ et que H est distingué dans G qui est simple, forcément $H = \{1\}$. Or G n'est pas commutatif, et nous avons vu que comme conséquence de cette hypothèse, tout élément de G est contenu dans un sous-groupe maximal. En particulier, les sous-groupes maximaux de G ne sont pas triviaux.

Nous avons utilisé toutes les hypothèses de l'exercice crucialement pour conclure qu'il a au moins deux sous-groupes maximaux distincts. Maintenant, nous montrerons qu'il existe deux sous-groupes maximaux H et H' distincts dont l'intersection est non triviale. Dans le raisonnement, la finitude de G est indispensable. Par l'absurde supposons que pour toute paire de sous-groupes maximaux, distincts H et H' de G, $H \cap H' = \{1\}$.

La stratégie de la preuve est de compter le nombre d'éléments dans l'ensemble $\bigcup_{g\in G} gHg^{-1}$ avec H maximal. Les conjugués d'un sous-groupe H sont fortement liés au *normalisateur* de H, $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ (vérifiez que $N_G(H)$ est en effet un sous-groupe qui contient H si vous ne l'avez jamais fait). Il y a une bijection entre les conjugués de H et les classes de $N_G(H)$ dans G qui associe à tout conjugué gHg^{-1} la classe $gN_G(H)$. En particulier le cardinal de l'ensemble $\{gHg^{-1} \mid g \in G\}$ est égal à $[G : N_G(H)]$.

Dans notre exercice, le lien entre H et son normalisateur est très particulier. Comme $H \leq N_G(H) \leq G$, et que H est maximal, soit $H = N_G(H)$, soit $N_G(H) = G$. La deuxième possibilité est équivalente à ce que H soit distingué dans G. Or G est simple, H est un sous-groupe propre et non trivial de G. Par conséquent H ne peut pas être distingué dans G. Alors, la seule possibilité est que $H = N_G(H)$ (H est *autonormalisant*). Comme G est fini, nous pouvons alors écrire l'égalité suivante :

$$|\{gHg^{-1} \mid g \in G\}| = \frac{|G|}{|H|} \ .$$

Comme tout conjugué de H est aussi maximal dans G, et que d'après l'hypothèse contradictoire, deux conjugués distincts s'intersectent trivialement,

$$|\bigcup_{g\in G} gHg^{-1}| = \frac{|G|}{|H|}(|H| - 1) + 1 \ . \quad (*)$$

Deux possibilités se présentent. Soit G contient au moins deux classes de conjugaison de sous-groupes maximaux, soit tous les sous-groupes maximaux de G sont conjugués. Etudions d'abord le premier cas.

Si H et H' sont deux sous-groupes maximaux non conjugués, alors il découle de l'hypothèse contradictoire que

$$\bigcup_{g\in G} gHg^{-1} \cap \bigcup_{g\in G} gH'g^{-1} = \{1\}$$

(voyez-vous pourquoi ?). Bien sûr, l'identité (*) s'applique à H' aussi, et nous en concluons l'inégalité suivante :

$$\frac{|G|}{|H|}(|H| - 1) + \frac{|G|}{|H'|}(|H'| - 1) + 1 \leq |G|$$

qui devient après une légère manipulation

$$|G| + 1 \leq \frac{|G|}{|H|} + \frac{|G|}{|H'|} \ .$$

Or H et H' sont des sous-groupes non triviaux, donc d'ordre au moins 2. Nous aboutissons à la conséquence

$$|G| + 1 \leq \frac{|G|}{|H|} + \frac{|G|}{|H'|} \leq \frac{|G|}{2} + \frac{|G|}{2} = |G|$$

qui est clairement impossible. Cette contradiction finit la preuve quand G contient deux sous-groupes maximaux qui ne sont pas conujugués.

Il reste à étudier la possibilité que G ne possède qu'une seule classe de conjugaison de sous-groupes maximaux. Nous avons déjà vu que tout élément de G est contenu dans un sous-groupe maximal. Par conséquent,

$$G = \bigcup_{g \in G} gHg^{-1}$$

où H est un sous-groupe maximal de G. Comme deux conjugués distincts de H s'intersectent trivialement et que $H = N_G(H)$, le raisonnement de comptage ci-dessus montre que

$$|G| = \frac{|G|}{|H|}(|H| - 1) + 1 \ .$$

Ceci entraîne $|G| = |H|$, une conclusion contradictoire puisque $H \neq G$. La preuve est finie.

(d) Ce point est une conséquence des points (b) et (c). C'est un bon entraînement de fournir les détails du raisonnement. □