Devoir Confiné (4h)

Correction du problème 1 – (Groupes résolubles et théorème de Sylow généralisé)

Le but du théorème est de démontrer une généralisation du premier théorème de Sylow, pour les groupes résolubles, cette notion étant définie et étudiée dans la partie III.

Questions préliminaires

1. Soit G un groupe, H et K deux sous-groupes tels que $K \lhd G$. Les deux questions sont indépendantes.
   (a) Soit $h \in H$. Puisque K est un sous-groupe distingué de G, $hKh^{-1} = K$, donc $hK = Kh$. Ceci étant vrai pour tout H, $\boxed{HK = KH}$.
   D'après un résultat rappelé (produit de groupe), on en déduit que HK est un groupe. On a clairement $H \subset HK$ et $K \subset HK$. Ainsi, par propriété de minimalité, $\langle H \cup K \rangle \subset HK$.
   Réciproquement, par stabilité par produit, pour tout $h \in H \subset \langle H \cup K \rangle$ et $k \in K \subset \langle H \cup K \rangle$, $hk \in \langle H \cup K \rangle$. Ainsi, $HK = \langle H \cup K \rangle$.
   Ainsi, $\boxed{HK = \langle H \cup K \rangle}$.
   (b) Soit $k \in H \cap K$ et $h \in H$.
   - Puisque $K \lhd G$, $hkh^{-1} \in K$.
   - Puisque $h, k \in H$, par stabilité de H par produit et inverse, $hkh^{-1} \in H$.

   Ainsi, $hkh^{-1} \in H \cap K$. On en déduit que $\boxed{H \cap K \lhd H}$.
2. Soit G un groupe, $H \lhd G$ et $K \lhd G/H$. Soit $k \in \pi_{G,H}^{-1}(K)$ et $g \in G$. En notant $\overline{k}$ la classe modulo H de k, on a $\overline{g}\overline{k}\overline{g}^{-1} \in K$, car $K \lhd G/H$. Ainsi, $\overline{gkg^{-1}} \in K$, et donc $gkg^{-1} \in \pi_{G,H}^{-1}(K)$.
   On en déduit que $\boxed{\pi_{G,H}^{-1}(K) \lhd G}$.
3. Soit H et K deux sous-groupes de G tels que $HK = KH$ et $H \lhd G$ et $K \lhd G$
   (a) D'après la question 1(a), $HK = KH =< H \cup K >$. Soit $hk \in HK$. On a alors l'existence de h' et k' dans H et K respectivement, tels que $hk = k'h'$. Or, puisque $H \lhd K$, il existe $h'' \in H$ tel que $hk = kh''$. On a donc $kh'' = k'h'$, d'où $(k')-1k = h'(h'')^{-1} \in H \cap K = \{e\}$. On en déduit que :

   $$(k')^{-1}k = h'(h'')^{-1} = \mathrm{e} \qquad \text{donc:} \qquad k' = k \qquad \text{et} \qquad h' = h''.$$

   En échangeant le rôle de H et K, on obtient également $h = h'$. Ainsi $\boxed{hk = kh}$.
   (b) Soit $\varphi : H \times K \longrightarrow HK$ définie par $\varphi((h,k)) = hk$.
   - φ est un morphisme de groupes. En effet,

   $$\varphi((h_1,k_1)(h_2,k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2,$$

   d'après la question précédente. Ainsi,

   $$\varphi((h_1,k_1)(h_2,k_2)) = \varphi((h_1,k_1))\varphi((h_2,k_2)).$$

   - φ est surjective, par définition de HK
   - Soit $(h,k) \in \mathrm{Ker}(\varphi)$, on a donc $hk = \mathrm{e}$, donc $h = k^{-1} \in H \cap K$. Puisque $H \cap K = \{e\}$, il vient $(h,k) = (e,e)$. Ainsi, $\mathrm{Ker}(\varphi) = \{(e,e)\}$.
     Il en résulte que φ est injective.

   Ainsi, $\boxed{\varphi \text{ est un isomorphisme}}$.

Partie I – Théorèmes d'isomorphisme

1. **Deuxième théorème d'isomophisme**

   Soit G un groupe, et H et K deux sous-groupes tels que $H \subset K$, $K \lhd G$ et $H \lhd G$

   (a) Puisque $K \lhd G$, pour tout $g \in G$, $gKg^{-1} = K$. En particulier, pour $h \in H \subset G$, $hKh^{-1} = K$. Ainsi, $K \lhd H$.

   (b) Pour commencer, les objets de H/K sont des classes hK, pour $h \in G$. Ainsi,

   $$H/K = \pi_{G,K}(H),$$

   et c'est donc un sous-groupe de G/H, en tant qu'image directe d'un sous-groupe par un morphisme.
   On note $\overline{x}$ la classe modulo K d'un élément x de G.
   Soit $\overline{g} \in G/K$, représenté par $g \in G$, et $\overline{h} \in H$, représenté par $h \in H$. Par définition de la loi quotient,

   $$\overline{g}\overline{h}\overline{g}^{-1} = \overline{ghg^{-1}}$$

   Or, puisque $H \lhd G$, $ghg^{-1} \in H$, donc $\overline{g}\overline{h}\overline{g}^{-1} \in H/K$.
   Ainsi, $\boxed{H/K \lhd G/K}$

   (c) Soit $\pi_{G,H} : G \mapsto G/H$. Par définition, $\mathrm{Ker}(\pi_{G,H}) = H$. Ainsi,

   $$K \subset H = \mathrm{Ker}(\pi_{G,H}).$$

   D'après un résultat admis en préambule (quotient d'un morphisme), $\boxed{\pi_{G,H} \text{ passe au quotient}}$. Par définition même du passage au quotient, l'application obtenue vérifie $\boxed{\pi_{G,H} = \overline{\pi}_{G,H} \circ \pi_{G,K}}$.

   (d) Soit $\pi_{G,K}(g)$ un élément de G/K. On a donc

   $$\overline{\pi}_{G,H}(\pi_{G,K}(g)) = \pi_{G,H}(g).$$

   Ainsi, $\pi_{G,K}(g) \in \mathrm{Ker}(\overline{\pi}_{G,H})$ si et seulement si $\pi_{G,H}(g) = 0$, si et seulement si $g \in H$.
   Ainsi les éléments de $\mathrm{Ker}(\overline{\pi}_{G,H})$ sont les classes modulo K des éléments de H, soit :

   $$\boxed{\mathrm{Ker}(\overline{\pi}_{G,H}) = H/K}.$$

   Puisque $\overline{\pi}_{G,H}$ est surjective (puisque $\pi_{G,H}$ l'est), on déduit du premier théorème d'isomophisme qu'en le passant au quaotient modulo H/K, on obtient un isomophisme :

   $$\boxed{(G/K)/(H/K) \xrightarrow{\simeq} G/H} \qquad \text{(Deuxième théorème d'isomophisme).}$$

2. **Normalisateur**

   Soit G un groupe, et H un sous-groupe de G.
   - $eHe^{-1} = H$, donc $e \in N_G(H)$.
   - Soit $x, y \in N_G(H)$. Ainsi,
     $$xyH(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H,$$
     puisque x et y sont dans $N_G(H)$. Ainsi, $xy \in N_G(H)$.
   - Soit $x \in N_G(H)$. Alors $xHx^{-1} = H$, donc en multipliant par x^1 à gauche et x à droite, $H = x^{-1}Hx$. Ainsi, $x^{-1} \in N_G(H)$.

   Par la caractérisation des sous-groupes, on en déduit que $\boxed{N_G(H) \text{ est un sous-groupe de } G}$.
   Par ailleurs, étant donné $h \in H$, $hH \subset H$ par stabilité, ainsi que $h^{-1}H \subset H$, de quoi on déduit $H \subset hH$. Ainsi, $hH = H$. De même, $Hh^{-1} = H$. Donc

   $$hHh^{-1} = Hh^{-1} = H,$$

   et on a donc $h \in N_G(H)$, et finalement, $\boxed{H \subset N_G(H)}$.

3. **Troisième théorème d'isomophisme**

   Soit G un groupe et H et K deux sous-groupes de G tels que $H \subset N_G(K)$.

(a) Par définition de $N_G(K)$, $K \lhd N_G(K)$. Par hypothèse $H \subset N_G(K)$. Par la question préliminaire 1 on en déduit que $\boxed{HK \text{ est un sous-groupe de } G}$ et que $\boxed{H \cap K \lhd H}$

(b) Montrons d'abord que $K \lhd HK$. Soit $k_0 \in K$ et $hk \in HK$. On a alors

$$(hk)k_0(hk)^{-1} = h(kk_0k^{-1})h^{-1}.$$

Comme $k, k_0 \in K$, il en est de même de kk_0k^{-1}, puisque K est un groupe. Ainsi, puisque $H \subset N_G(K)$, il vient

$$(hk)k_0(hk)^{-1} \in K,$$

et donc $\boxed{K \lhd HK}$. Cela permet de considérer le quotient HK/K.

Soit alors $\varphi : H \longrightarrow HK/K$ défini par $\varphi(h) = \overline{h \times e}$.

- $\varphi(h_1h_2) = \overline{h_1h_2} = \overline{h_1}\,\overline{h_2} = \varphi(h_1)\varphi(h_2)$. Ainsi, φ est un morphisme de groupes.
- Soit x un élément de HK/K. Il existe $h \in H$ et $k \in K$ tel que $x = \overline{hk}$. Or, comme on considère les classes modulo K et que $k \in K$, $\overline{hk} = \overline{h} = \varphi(h)$. Ainsi, φ est surjective.
- Soit $h \in H$. On a alors $h \in \mathrm{Ker}(\varphi)$ ssi $\varphi(h) = 0$ ssi $\overline{h} = \overline{e}$ ssi $h \in K$. Ainsi, $\mathrm{Ker}(\varphi) = H \cap K$.
- D'après le premier théorème d'isomophisme, on en déduit qu'enn passant φ au quotient par son noyau, l'application obtenue $\boxed{\overline{\varphi} : H/(H \cap K) \xrightarrow{\simeq} HK/K \text{ est un isomorphisme}}$ (Troisième théorème d'isomophisme).

4. **Lemme du papillon (Zassenhaus)**

Soit G un groupe et U et V deux sous-groupes de G. Soit H et K deux sous-groupes distingués de U et V respectivement.

(a) D'après la question préliminaire 1a, puisque $H \lhd U$ et $U \cap K \leqslant U$, $H(U \cap K)$ est un $\boxed{\text{sous-groupe de } U, \text{ donc de } G}$. De même pour $H(U \cap V)$, et par un argument symétrique (dans V cette fois), pour $(H \cap V)K$ et $(U \cap V)K$.

(b) Soit $hk \in H(U \cap K)$ et $h'v \in H(U \cap V)$, où $h, h' \in H$, $k \in U \cap K$ et $v \in U \cap V$. Alors

$$\begin{aligned}(h'v)(hk)(h'v)^{-1} &= h'vhkv^{-1}(h')^{-1} \\ &= h'h''vkv^{-1}(h')^{-1} \qquad \text{où } h'' \in H, \text{ puisque } h \in H \lhd U \ni v\end{aligned}$$

Or, $vkv^{-1} \in U$ comme produit de trois éléments de U. Comme $H \lhd U$, on a donc l'existence de $h''' \in H$ tel que

$$h'h''vkv^{-1}(h')^{-1} = h'h''h'''vkv^{-1}.$$

Comme $h'h''h'' \in H$, $vkv^{-1} \in U$ et $vkv^{-1} \in K$ (car $K \lhd V$), on en déduit que $(h'v)(hk)(h'v)^{-1} \in H(U \cap K)$, donc que $\boxed{H(U \cap K) \lhd H(U \cap V)}$.

Un raisonnement symétrique amène $\boxed{(K \cap V)K \lhd (U \cap V)K}$.

(c) On pose $H_0 = U \cap V$, $K_0 = H(U \cap K)$. On a alors :

- pour tout $u \in H_0 = U \cap V$,

$$\begin{aligned}uK_0 &= uH(U \cap K) \\ &= Hu(U \cap K) && \text{car } u \in U \text{ et } H \lhd U \\ &= H(uU \cap uK) \\ &= H(Uu \cap Ku) && \text{car } u \in V \text{ et } K \lhd V \\ &= H(U \cap V)u = K_0u\end{aligned}$$

Ainsi, $H_0 \subset N_G(K_0)$.

- Par définition de H_0 et K_0, $H_0 \cap K_0 = (U \cap V) \cap (H(U \cap K))$. Or :
  - Soit $hu \in (U \cap V) \cap (H(U \cap K))$, avec $h \in H$ et $u \in U \cap K$. Ainsi, $h = (hu)u^{-1}$, avec $u^{-1} \in K \subset V$, et $hu \in V$. Donc $h \in V$.
    On en déduit que $hu \in (H \cap V)(U \cap K)$, donc $(U \cap V) \cap (H(U \cap K)) \subset (H \cap V)(U \cap K)$.

∗ Réciproquement, si $hu \in (H \cap V)(U \cap K)$, avec $h \in H \cap V$ et $u \in U \cap K$, alors puisque $H \subset U$, $h \in U$. De même, $K \subset V$, donc $h \in V$. Enfin, $h \in H$ et $u \in U \cap K$, donc $hu \in H(U \cap K)$.
On en déduit que $(H \cap V)(U \cap K) \subset (U \cap V) \cap (H(U \cap K))$.

∗ Ainsi, $\boxed{H_0 \cap K_0 = (U \cap V) \cap (H(U \cap K)) = (H \cap V)(U \cap K)}$

- Soit $x \in H_0K_0 = (U \cap V)H(U \cap K)$. Il existe alors $v \in U \cap V$, $h \in H$ et $k \in U \cap K$ tels que $x = vhk$. Puisque $H \lhd U$ et $v \in U$, il existe $h' \in U$ tel que $x = h'vk$. Or v et k sont dans le sous-groupe $U \cap V$ donc vk aussi. Ainsi, $x \in H(U \cap V)$
Réciproquement, si $x \in H(U \cap V)$, on peut écrire $x = hv$ avec $h \in H$ et $v \in U \cap V$. Comme avant, il existe $h' \in H$ tel que $x = vh' = vh'e$, ce qui montre que $x \in (U \cap V)H(U \cap K) = H_0K_0$.
Ainsi, $\boxed{H_0K_0 = H(U \cap V)}$.
- Le troisième théorème d'isomorphisme avec H_0 et K_0 amène donc :

$$\boxed{(U \cap V) \,/\, (H \cap V)(U \cap K) \simeq H(U \cap V) \,/\, H(U \cap K)}.$$

(d) On a aussi, par unn argument symétrique :

$$(U \cap V) \,/\, (H \cap V)(U \cap K) \simeq (U \cap V)K \,/\, (H \cap V)K.$$

Ainsi, en mettant bout à bout ces deux isomorphismes, on obtient :

$$\boxed{H(U \cap V) \,/\, H(U \cap K) \simeq (U \cap V)K \,/\, (H \cap V)K \qquad \text{(lemme du papillon).}}$$

Vous pourrez essayer de comprendre la référence au papillon en traçant le graphe de couverture de la relation d'inclusion pour les sous-groupes en jeu dans ce lemme. Cela fait un joli papillon, avec même des antennes.

Partie II – Suites de composition, théorèmes de Schreier et de Jordan-Hölder

1. Théorème de Schreier

(a)
- Soit $i \in [\![0, r-1]\!]$ et $j \in [\![0, s-2]\!]$. On a alors

$$G_{i,j+1} = G_{i+1}(H_{j+1} \cap G_i) \subset G_{i+1}(H_j \cap G_i) = G_{i,j}.$$

De plus, d'après la question I-4(a) appliquée avec $H = G_{i+1}$, $K = H_{j+1}$, $U = G_i$, $V = H_j$, on obtient

$$G_{i+1}(H_{j+1} \cap G_i) \lhd G_{i+1}(H_j \cap G_i) \qquad \text{soit:} \qquad G_{i,j+1} \lhd G_{i,j}$$

- Par ailleurs, on a $G_{i,1} = G_{i+1}(G \cap G_i) = G_{i+1}G_i = G_i$, puisque G_{i+1} est un sous-groupe de G_i.
- Il reste à montrer que $G_{i,1} \lhd G_{i-1,s-1}$. Or, en étendant les notations, il vient facilement que

$$G_{i-1,s} = G_i(\{e\} \cap G_{i-1}) = G_i\{e\} = G_i.$$

On est alors ramené au même argument que dans le premier point (provenant de la question préliminaire au lemme du papillon) : $G_{i-1,s} \lhd G_{i-1,s-1}$, donc $G_{i,1} \lhd G_{i-1,s-1}$.

Ainsi, $\boxed{(G_{i,j})_{(i,j) \in [\![1,r-1]\!] \times [\![1,s-1]\!]} \text{ est un raffinement de } (G_i).}$

(b) De même, on construit $H_{j,i} = (H_j \cap G_i)H_{j+1}$. On montre comme ci-dessus qu'il s'agit d'un raffinement de (H_j).

Par ailleurs, le lemme du papillon assure que pour tout $(i, j) \in [\![1, r-1]\!] \times [\![1, s-1]\!]$,

$$G_{i+1}(H_j \cap G_i)/G_{i+1}(H_{j+1} \cap G_i) \simeq (H_j \cap G_i)H_{j+1}/(H_j \cap G_{i+1})H_{j+1},$$

c'est-à-dire $G_{i,j}/G_{i,j+1} \simeq H_{j,i}/H_{j,i+1}$. Ceci étant aussi vrai pour $i = r-1$ et $j = s-1$, et en se souvenant que $G_{i,1} = G_{i-1,s-1}$ et de même $H_{j,1} = H_{j-1,r-1}$, on en déduit que les quotients des deux suites sont deux à deux isomorphes.

Ainsi, $\boxed{(G_{i,j}) \text{ et } (H_{j,i}) \text{ sont deux raffinements équivalents de } (G_i) \text{ et } (H_j)}$.

2. **Suite de Jordan-Hölder.**

Soit $\{e\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 = G$ une suite de composition. On dit qu'il s'agit d'une suite de Jordan Hölder si elle est maximale, i.e. qu'elle n'est raffinée par aucune suite de composition autre qu'elle-même.

(a) Puisque G est de cardinal fini et que les suites de composition sont constituées d'inclusions strictes, elles sont toutes finies, d'indice maximal s (qu'on va appeler longueur de la suite) borné par $|G|$. Ainsi, l'ensemble des longueurs des suites de composition est un sous-ensemble de $\mathbb{N}$, majoré et non vide (la suite $\{0\} \lhd G$ étant une suite de composition de lonngueur 1).

Ainsi, d'après la propriété fondamentale de $\mathbb{N}$, il existe une suite de composition de longueur maximale. Cette suite ne peut être raffinée par aucune autre suite de composition, puisque cela fournirait une suite de composition de longueur strictement plus grande.

Ainsi, il existe une suite de Jordan-Hölder.

(b) Soit (G_i) et (H_j) deux suites de Jordan-Hölder. Ce sont en particulier des suites de composition. D'après le théorème de Schreier, il existe donc un raffinement $(G_{i,j})$ de (G_i) et un raffinement $(H_{j,i})$ de (H_j) tels que $(G_{i,j})$ et $(H_{j,i})$ soient équivalentes. Or, comme (G_i) et (H_j) n'admettent pas de raffinement strict en tant que suites de Jordan-Hölder, on a $(G_{i,j}) = (G_i)$ et $(H_{j,i}) = (H_j)$.

On en déduit que (G_i) et (H_j) sont équivalentes.

(c) C'est le même argument que dans la question 1, en considérant cette fois la longueur maximale d'un raffinement d'une suite de composition (G_i) donnée.

Ce raffinement de lonngueur maximale est une suite de Jordan-Hölder.

(d) Supposons que (G_i) soit une suite de composition, et qu'il existe i tel que G_i/G_{i+1} ne soit pas simple. On va montrer qu'alors (G_i) n'est pas une suite de Jordan-Hölder.

En effet, il existe alors $K \lhd G_i/G_{i+1}$ tel que $K \neq \{\overline{e}\}$ et $K \neq G_i/G_{i+1}$. Considérons alors

$$H = \pi^{-1}_{G_i,G_{i+1}}(K).$$

On a alors $G_{i+1} = \pi^{-1}_{G_i,G_{i+1}}(\{\overline{e}\}) \subsetneq H \subsetneq G_{i+1}$, et de plus :

- $G_{i+1} \lhd G_i$, donc *a fortiori* $G_{i+1} \lhd H$ (cette propriété est moins forte !)
- Pour tout $g \in G_i$ et $h \in H$ (la barre désigne la classe dans le quotient par G_{i+1}) :

$$\overline{ghg^{-1}} = \overline{g}\overline{h}\overline{g}^{-1} \in K,$$

puisque $K \lhd G_i/G_{i+1}$. Ainsi,

$$ghg^{-1} \in \pi^{-1}_{G_i,G_{i+1}}(\overline{ghg^{-1}}) \subset \pi^{-1}_{G_i,G_{i+1}}(K) = H.$$

On en déduit que $H \lhd G_i$.

Par conséquent, en insérant le groupe H entre G_i et G_{i+1} on obtient un raffinement strict de (G_i), ce qui montre que (G_i) n'est pas une suite de Jordan-Hölder.

En contraposant : les quotients d'une suite de Jordan-Hölder sont simples.

Partie III – Groupes résolubles

1. **Sous-groupes et quotients d'un groupe résoluble.**

(a) Soit G un groupe résoluble, et $(G_i)_{i\in[\![0,r]\!]}$ une suite de composition telle que tous les quotients soient abéliens. Soit H un sous-groupe de G. On définit

$$H_i = G_i \cap H.$$

- On a, pour tout $i \in [\![0, r-1]\!]$,

$$H_{i+1} = G_{i+1} \cap H = G_{i+1} \cap (G_i \cap H),$$

puisque $G_{i+1} \subset G_i$. Or, $G_{i+1} \lhd G_i$ et $G_i \cap H \leqslant G_i$. Donc, d'après la question préliminaire 1(b), $H_{i+1} \lhd G_i$, et puisque $H_i \subset G_i$, on a bien $H_{i+1} \lhd H_i$

- Pour étudier le caractère abélien des quotients, on utilise le lemme suivant :
  Lemme : Soit $f : A \to B$ un morphisme de groupes injectif. Si B est abélien, alors A l'est aussi.
  Démonstration : Soit x et y dans A. On a donc

$$f(xy) = f(x)f(y) = f(y)f(x) = f(yx),$$

  en utilisant le fait que f est un morphisme, et que B est abélien. Par injectivité de f, on en déduit que $xy = yx$. Ainsi, A est abélien.
- On veut comparer H_i/H_{i+1} à G_i/G_{i+1}. Onn ne peut pas le faire directement sous forme d'une inclusion, car les éléments de H_i/H_{i+1} ne sont pas de même nature que ceux de G_i/G_{i+1}. Du point de vue ensembliste, les classes modulo H_{i+1} ne sont pas des classes modulo G_{i+1} (en général, leur cardinal n'est pas le même !)
  On va construire une injection de l'un dans l'autre : on définit pour commencer :

$$f : H_i \longrightarrow G_i/G_{i+1},$$

  qui à $h \in H_i \subset G_i$ associe sa classe $\overline{h}$ modulo G_{i+1}. Autrement dit, c'est la restriction de la projection canonique : $f = \pi_{|H_i}$, où pour simplifier, on a noté $\pi = \pi_{G_i,G_{i+1}}$. Son noyau est donc

$$\mathrm{Ker}(f) = \mathrm{Ker}(\pi) \cap H_i = G_{i+1} \cap H_i = G_{i+1} \cap G_i \cap H = G_{i+1} \cap H = H_{i+1}.$$

  Ainsi, d'après le théorème d'isomorphisme, on peut passer f au quotient sur son noyau, et on récupère un morphisme injectif $\overline{f} : H_i/H_{i+1} \to G_i/G_{i+1}$ (la surjectivité dans les hypothèses du théorème d'isomorphisme ne sert qu'à obtenir la bijectivité au bout, on n'en a pas besoin ; si on veut se ramener à l'énoncé précis du théorème d'isomophisme, il suffit de corestreindre f à son image pour récupérer la surjectivité). D'après le lemme ci-dessus, puisque G_i/G_{i+1} est abélien, il en est de même de H_i/H_{i+1}.
- Ainsi, quitte à enlever les termes égaux dans cette suite (pour avoir une suite strictement croissante), (H_i) est une suite de composition de H à quotients abéliens, donc $\boxed{H \text{ est résoluble.}}$

Voici un autre argument plus élémentaire pour l'étude du caractère abélien de H_i/H_{i+1}, mais que je trouve moins joli...

- Soit $\overline{h}$ et $\overline{k}$ dans H_i/H_{i+1}, représentés par des éléments h et k de $H_i \subset G_i$. Alors $\tilde{h}\tilde{k} = \tilde{k}\tilde{h}$, $\tilde{h}$ déisgnant la classe modulo G_{i+1}. Autrement dit, $hk(kh)^{-1} \in G_{i+1}$. Mais enn tant que produit d'éléments de H, c'est aussi dans H. Donc $hk(kh)^{-1} \in G_{i+1} \cap H = H_{i+1}$. On en déduit que

$$\overline{hk} = \overline{kh}$$

  (classes modulo H_{i+1} cette fois). Ainsi, H_i/H_{i+1} est abélien.

(b) Soit $(G_i)_{i\in[\![0,r]\!]}$ une suite de composition à quotients abéliens, et $H \lhd G$. Considérons $\pi = \pi_{G,H}$. Montrons que $(\pi(G_i))_{i\in[\![0,r]\!]}$ est une suite de composition de G/H (quitte, comme avant, à enlever les termes égaux.

- Comme π est un morphisme, les $\pi(G_i)$ sont des sous-groupes de G/H. De plus, $\pi(G_{i+1}) \lhd \pi(G_i)$. En effet, l'image directe étant croissante, on a bien l'inclusion $\pi(G_{i+1}) \subset \pi(G_i)$, et les deux étant munis d'une structure de groupe restrinte de la même structure de G/H, $\pi(G_{i+1})$ est un sous-groupe de $\pi(G_i)$.
- De plus, pour $x \in \pi(G_{i+1})$ et $y \in \pi(G_i)$, il existe $a \in G_{i+1}$ et $b \in G_i$ tels que $x = \pi(a)$ et $y = \pi(b)$. Alors :

$$yxy^{-1} = \pi(b)\pi(a)\pi(b)^{-1} = \pi(bab^{-1}) = \pi(a'),$$

  pour un certain $a' \in G_{i+1}$, puisque $G_{i+1} \lhd G_i$. Ainsi, $yxy^{-1} \in \pi(a')$. Donc $\pi(G_{i+1}) \lhd \pi(G_i)$.
  Nous avons en fait démontré le lemme plus général :
  Lemme : Si $H \lhd K \leqslant G$, et si $f : G \to G'$ est un morphisme, alors $f(H) \lhd f(G)$.
- Encore un autre lemme, à rapprocher du lemme de la question précédente :
  Lemme : Soit $f : A \to B$ un morphisme de groupes surjectif. Si A est abélien, alors B l'est aussi.
  Démonstration : Soit x, y dans B. Il existe a, b dans A tels que $f(a) = x$ et $f(b) = y$, car f est surjective. Ainsi,

$$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx.$$

  Donc B est abélien.

- Pour montrer que $\pi(G_i)/\pi(G_{i+1})$ est abélien, il suffit donc de construire un morphisme surjectif $G_i/G_{i+1} \to \pi(G_i)/\pi(G_{i+1})$. Pour cela, on commence par construire la composée f suivante, composée de deux morphismes surjectifs, donc f est aussi un morphisme surjectif :

$$f \ : \ G_i \xrightarrow{\pi} \pi(G_i) \overset{\pi_{\pi G_i, \pi(G_{i+1})}}{\longrightarrow} \pi(G_i)/\pi(G_{i+1}).$$

  Soit $g \in G_{i+1}$. Alors $\pi(g) = gH$ (classe de g modulo H. Comme $g \in G_{i+1}$, $\pi(g) \in \pi(G_{i+1})$, donc $\pi_{\pi G_i, \pi(G_{i+1})}(\pi(g)) = e_{\pi(G_i)/\pi(G_{i+1})}$. On en déduit que $G_{i+1} \subset \mathrm{Ker}(f)$. On peut donc passer f au quotient et définir :

$$\overline{f} \ : \ G_i/G_{i+1} \longrightarrow \pi(G_i)/\pi(G_{i+1}),$$

  qui reste un morphisme surjectif. Ainsi, d'après le lemme, puisque G_i/G_{i+1} est abélien, $\pi(G_i)/\pi(G_{i+1})$ aussi.
- On en déduit que quitte à enlever les doublons pour avoir une chaîne d'inclusions strictes, $(\pi(G_i))$ est une suite de composition de G/H à quotients abéliens, donc $\boxed{G/H \text{ est résoluble}}$.

(c) Soit $\{0\} = K_r \lhd \cdots \lhd K_0 = G/H$ une suite de composition à quotients abéliens, et pour tout $i \in [\![0, r]\!]$, $G_i = \pi_{G,H}^{-1}(K)_i$. Alors :
- Pour $i \in [\![0, r-1]\!]$, $G_{i+1} \lhd G_i$. En effet, soit $h \in G_{i+1}$ et $g \in G_i$. On passe modulo H, en utilisant le fait que $K_{i+1} = G_{i+1}/H$, $K_i = G_i/H$ et $K_{i+1} \lhd K_i$. Ainsi,

$$\overline{ghg^{-1}} \in G_{i+1}/H,$$

  donc $ghg^{-1} \in G_{i+1}$. On en déduit que $G_{i+1} \lhd G_i$.
- Les quotients vérifient :

$$G_i/G_{i+1} \simeq (G_i/H)/(G_{i+1}/H) = K_i/K_{i+1},$$

  d'après le troisième théorème d'isomorphisme. Ainsi, les G_i/G_{i+1} sont abéliens, pour $i \in [\![0, r-1]\!]$.
- On considère ensuite une suite de composition de H à quotients abéliens :

$$\{0\} = G_s \lhd \cdots \lhd G_r = H.$$

  Avec les vérifications précédentes, il vient assez facilement que

$$\{0\} = G_s \lhd \cdots \lhd G_r = H \lhd G_{r-1} \lhd \cdots \lhd G_0 = G$$

  est une suite de compositions à quotients abéliens de G

Ainsi, $\boxed{G \text{ est résoluble.}}$

2. **Caractérisation de la résolubilité par les quotients d'une suite de Jordan-Hölder**

(a)
- Supposons que A est abélien et n'est pas d'ordre premier. Soit p un diviseur premier de $|A|$. D'après le lemme de Cauchy, il existe $x \in A$ d'ordre $p \neq |A|$. Ainsi, $< x >$ est un sous-groupe propre et non trivial de A. Il est nécessairement distingué puisque A est abélien. Ainsi, A n'est pas simple.
- Réciproquement, si A est d'ordre premier p, tout élément différent du neutre est d'ordre divisant p et différent de 1, donc d'ordre p. Soit donc $x \in A$, $x \neq e$. On a alors $| < x > | = p = |A|$, donc $< x >= A$. Par conséquent, si H est un sous-groupe de A non réduit à e et $x \in H \setminus \{e\}$, alors $A =< x > \subset H$, donc $H = A$. Par conséquent, les seuls sous-groupes de A sont $\{e\}$ et A. On peut en conclure que A est simple.

Ainsi, $\boxed{\text{un groupe abélien } A \text{ est simple si et seulement si } A \text{ est d'ordre } p \text{ premier}}$ (et nécessairement cyclique dans ce cas)

(b)
- Soit G un groupe résoluble, et (G_i) une suite de composition de G_i à quotients abéliens. En raffinant (G_i), on obtient encore une suite à quotients abéliens. En effet, en insérant H tel que $G_{i+1} \lhd H \lhd G_i$, on a :
  * d'une part $H/G_{i+1} \subset G_i/G_{i+1}$, donc H/G_{i+1} est abélien
  * d'autre part on peut connstruire un morphisme surjectif $\varphi : G_i \to G_i/H$, qui passe au quotient par G_{i+1}, puisque $G_{i+1} \subset \mathrm{Ker}(\varphi)$. Ainsi, il existe un morphisme surjectif de G_i/G_{i+1} sur G_i/H. Comme avant, cela implique le transfert à G_i/H du caractère abélien de G_i/G_{i+1}. Ainsi, G_i/H est abélien.

Ainsi, en considérant un raffinement de longueur maximale de (G_i), on obtient encore une suite de compositions à quotients abéliens, et c'est une suite de Jordan-Hölder. D'après la question précédente, les quotients de cette suite de Jordan-Hölder sont donc simples et abéliens, donc cycliques d'ordre premier p.

Ainsi, $\boxed{\text{si } G \text{ est résoluble, } G \text{ admet une suite de Jordan-Hölder à quotients cycliques d'ordre premier } p.}$

- Réciproquement, si G admet une suite de Jordan-Hölder à quotients cycliques d'ordre premier p, en particulier ces quotients sont abéliens, donc G admet une suite de composition à coefficients abéliens. Ainsi, $\boxed{G \text{ est résoluble}}$.

Partie IV – Suites principales

1. Puisque H est minimal parmi les sous-groupes distingués non triviaux de G_{k-1}/G_k, si $H = G_{k-1}/G_k$, il n'y a pas de sous groupe distingué non trivial plus petit, donc il n'y a pas d'autre sous-groupe distingué non trivial. Ainnsi, $\boxed{G_{k-1}/G_k \text{ est simple.}}$
2. On suppose que $H \neq G_{k-1}/G_k$.
   (a) On a déjà fait cette preuve en 1(c).
   (b) Soit $L \in \mathrm{C}_G(K)$, et $g \in G$ tel que $L = gKg^{-1}$.
   - Tout d'abord, $gG_kg^{-1} = G_k$, car $G_k \lhd G$. Ainsi, puisque $G_k \subset K$, on a aussi $G_k \subset L$
   - De même, puisque $K \subset G_{k-1}$ et $gG_{k-1}g^{-1} = G_{k-1}$, onn a aussi $L \subset G_{k-1}$.
   - Puisque $G_k \lhd G$, on a trivialement aussi $G_k \lhd L$.
   - Soit $h \in G_{k-1}$. On a alors
   $$hLh^{-1} = hgKg^{-1}h^{-1} = g(g^{-1}hg)K(g^{-1}hg)^{-1}g^{-1}.$$
   Puisque $G_{k-1} \lhd G$, $g^{-1}hg \in G_{k-1}$, et puisque $K \lhd G_{k-1}$, $(g^{-1}hg)K(g^{-1}hg)^{-1} = K$. Ainsi :
   $$hLh^{-1} = gKg^{-1} = L.$$
   Par conséquent $L \lhd G_{k-1}$.

   On a bien montré que $\boxed{G_k \lhd L \lhd G_{k-1}}$.

   (c) Soit $g \in G$ et $x \in \left\langle \bigcup_{L \in \mathrm{C}_G(K)} L \right\rangle$. On peut écrire
   $$x = \ell_1 \cdots \ell_n,$$
   où chaque ℓ_i est dans un $L \in \mathrm{C}_G(K)$. Ainsi,
   $$gxg^{-1} = \prod_{i=1}^{n} g\ell_i g^{-1}.$$
   Si $\ell_i \in L = hKh^{-1}$, alors
   $$g\ell_i g^{-1} \in ghK(gh)^{-1} \in \mathrm{C}_G(K).$$
   Ainsi, $gxg^{-1} \in \left\langle \bigcup_{L \in \mathrm{C}_G(K)} L \right\rangle$.

   Par conséquent, $\left\langle \bigcup_{L \in \mathrm{C}_G(K)} L \right\rangle \lhd G$.

   (d) On a donc trouvé un sous-groupe distingué de G tel que
   $$G_{k-1} \lhd \left\langle \bigcup_{L \in \mathrm{C}_G(K)} L \right\rangle \lhd G_k,$$
   la première inclusion étant stricte (car $K \neq G_{k-1}$, puisque H est non trivial). Ainsi, puisque la suite est principale (et ne peut donc être raffinée par aucune autre suite distinguée), onn a nécessairement
   $$\boxed{\left\langle \bigcup_{L \in \mathrm{C}_G(K)} L \right\rangle = G_k}.$$

(e) Puisque G est fini, $\mathrm{C}_G(K)$ est fini. En considérant l'ensemble de toutes sous-familles de sous-groupes L de $\mathrm{C}_G(K)$ vérifiant (i), cet ensemble est non vide (il contient la famille totale d'après la question précédente), et les cardinaux de ces familles forment un sous-ensemble nnon vide de $\mathbb{N}$. Ainsi, il existe une famille de cardinal minimal j, qu'on note $(L_1, \dots, L_j)$, vérifiant la **propriété (i)**.
La minimalité de cette famille implique que dès lors qu'on retire l'un des groupes L_{j_0} de cette famille, la propriété (i) n'est plus vérifiée. D'où la **propriété (ii)**.

(f) Soit $L \in \mathrm{C}_G(K)$. On a déjà montré que $L \lhd G_{k-1}$, et $G_k \subsetneq L$.
Supposons qu'il existe $L' \lhd G_{k-1}$ tel que $G_k \subsetneq L' \subset L \lhd G_k$. Soit g tel que $L = gKg^{-1}$, et soit $K' = g^{-1}L'g$. Puisque la conjugaison est bijective,

$$|G_k| = |g^{-1}G_k g| < |g^{-1}L'g| = |L'| < |L| = |K|,$$

donc $G_k \subsetneq L' \subsetneq K$.
Par ailleurs, $L' \lhd G_{k-1}$, par le même argument qu'en question 2(b). Cela contredit donc la minimalité de K.
Ainsi, **L est minimal tel que $G_k \subsetneq L' \subset L \lhd G_k$**.

(g) Le groupe $\left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle = G_k$ est distingué dans G_{k-1}. En effet, si $x = \ell_1 \dots \ell_n$, $\ell_i \in L_{j_i}$, et $g \in G_{k-1}$ on a :

$$gxg^{-1} = (g\ell_1 g^{-1})(g\ell_2 g^{-1}) \cdots (g\ell_n g^{-1}).$$

Comme chaque L_i est distingué dans G_{k-1}, on enn déduit que pour tout $i \in [\![1, n]\!]$, $g\ell_i g^{-1} \in L_{j_i}$. Par conséquent,

$$gxg^{-1} \in \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle,$$

et donc $\left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle \lhd G_{k-1}$.
On a aussi $L_{j_0} \lhd G_{k-1}$. De façon évidente, l'intersection de deux sous-groupes distingués est encore un sous-groupe distingué, donc

$$L_{j_0} \cap \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle \lhd G_{k-1}.$$

Par ailleurs, $L_{j_0} \not\subset \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle$, sinon, on aurait

$$G_{k-1} \neq \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle = \left\langle \bigcup_{i \in [\![1,j]\!]} L_i \right\rangle = G_{k-1}.$$

Ainsi, $L_{j_0} \cap \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle$ est un sous-groupe distingué de G_{k-1} strictement inclus dans L_{j_0}. Par minimalité de L_{j_0} (question 2(f)), on en déduit que

$$\boxed{L_{j_0} \cap \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{j_0\}} L_i \right\rangle = G_k.}$$

(h) On montre par récurrence sur $m \in [\![1, j]\!]$ que

$$\langle L_1/G_k, \dots, L_m/G_k \rangle \simeq L_1/G_k \times \cdots \times L_m/G_k.$$

L'initialisation pour $m = 1$ est évidente. Supposons la propriété acquise pour une valeur de $m \in [\![1, j-1]\!]$. On a alors

$$G_k \subset L_{m+1} \cap \left\langle \bigcup_{i \in [\![1,m]\!]} L_i \right\rangle \subset L_{m+1} \cap \left\langle \bigcup_{i \in [\![1,j]\!] \setminus \{m+1\}} L_i \right\rangle = G_k,$$

d'après la question précédente. Donc

$$L_{m+1} \cap \left\langle \bigcup_{i\in[\![1,m]\!]} L_i \right\rangle = G_k,$$

puis

$$L_{m+1}/G_k \cap \left\langle \bigcup_{i\in[\![1,m]\!]} L_i/G_k \right\rangle = \{\overline{e}\}.$$

Par ailleurs, $L_{m+1} \lhd G_{k-1}$, d'où on déduit que $L_{m+1}/G_k \lhd G_{k-1}/G_k$, et de même,

$$\left\langle \bigcup_{i\in[\![1,m]\!]} L_i/G_k \right\rangle \lhd G_k.$$

On peut donc utiliser la question préliminaire 3, qui amène :

$$\left\langle \bigcup_{i\in[\![1,m+1]\!]} L_i/G_k \right\rangle = L_{m+1}/G_k \cdot \left\langle \bigcup_{i\in[\![1,m]\!]} L_i/G_k \right\rangle \simeq L_{m+1}/G_k \times \left\langle \bigcup_{i\in[\![1,m]\!]} L_i/G_k \right\rangle.$$

Ainsi, l'hypothèse de récurrence amène enfin :

$$\left\langle \bigcup_{i\in[\![1,m+1]\!]} L_i/G_k \right\rangle \simeq L_1/G_k \times \cdots L_m/G_k \times L_{m+1}/G_k.$$

Par principe de récurrence, cette propriété est donc vraie pour tout $m \in [\![1,j]\!]$.
En particulier, pour $m = j$, en passant la propriété (i) de 2(e) au quotient, on obtient :

$$\boxed{G_{k-1}/G_k = \left\langle \bigcup_{i\in[\![1,j]\!]} L_i/G_k \right\rangle \simeq L_1/G_k \times \cdots \times L_j/G_k}.$$

(i) Soit $S = L_1/G_k$, et $g \in G$ tel que $gKg^{-1} = L_1$. On a alors $gHg^{-1} = S$. Soit T un sous-groupe distingué de S, et $H' = \overline{g}^{-1}T\overline{g}$, sous groupe de H.

- Dans un premier temps $T \lhd G_{k-1}/G_k$. En effet, on utilise la description de G_k en terme de produit direct, obtenu dans la question précédente, les éléments de $T \subset L_1/G_k$ étant dans la première coordonnée. Ainsi, soit $(t,0,\ldots,0) \in T$, et $h = (g_1,\ldots,g_j) \in G_k/G_{k_1}$, $g_i \in L_i/G_k$. On a alors

  $$hth^{-1} = (g_1 t g_1^{-1}, 0, \ldots, 0) \in T,$$

  puisque $T \lhd L_1/G_k$. Ainsi, $\boxed{T \lhd G_{k-1}/G_k}$
- On a alors $H' \lhd G_{k-1}/G_k$. En effet, soit $h \in G_{k-1}/G_k$, on a alors :

  $$hH'h^{-1} = h\overline{g}^{-1}T\overline{g}h^{-1} = \overline{g}^{-1}(\overline{g}h\overline{g}^{-1})T(\overline{g}h\overline{g}^{-1})^{-1}\overline{g}.$$

  Or, puisque $G_{k_1}/G_k \lhd G/G_k$, $\overline{g}h\overline{g}^{-1} \in G_{k-1}/G_k$, et comme $T \lhd G_{k-1}/G_k$,

  $$(\overline{g}h\overline{g}^{-1})T(\overline{g}h\overline{g}^{-1})^{-1} = T.$$

  On en conclut que

  $$hH'h^{-1} = \overline{g}^{-1}T\overline{g} = H'.$$

  Ainsi, H' est un sous-groupe de H, distingué dans G_{k-1}/G_k.
- La minimalité de H amène alors $H' = H$ ou $H' = \{0\}$, puis $T = \{0\}$ ou $T = S$. Ainsi, $\boxed{S \text{ est simple}}$.
- Les L_i sont tous isomorphes entre eux car conjugués à un même groupe K. En effet, le morphisme de conjugaison $K \to gKg^{-1}$ qui à x associe gxg^{-1} est un isomorphisme de K dans gKg^{-1}. Ainsi, pour i_1 et i_2 dans $[\![1,j]\!]$, $L_{i_1} \simeq K \simeq L_{i_2}$
  Ainsi, pour tout $i \in [\![1,j]\!]$, $L_i/G_k \simeq L_1/G_k \simeq S$.. La question 2(h) amène alors :

  $$\boxed{G_{k-1}/G_k \simeq S^j}.$$

Partie V – Théorèmes de Sylow généralisés

1. On suppose dans cette question qu'il existe un sous-groupe distingué non trivial K de G d'ordre $m'n'$, avec $m' \mid m$ et $n' \mid n$, $n' < n$.

   (a) Puisque K est non trivial, $|G/K| < |G|$. On peut donc appliquer l'hypothèse de récurrence à G/K. En notant $m'' = \frac{m}{m'}$ et $n'' = \frac{n}{n'}$, $|G/K| = m''n''$, et $m'' \wedge n'' = 1$. Ainsi, par hypothèse de récurrence G/K admet un sous-groupe A d'ordre m'. Soit $B = \pi_{G,K}^{-1}(A)$. Puisque pour tout $x \in A$,

   $$|\pi_{G,K}^{-1}(\{x\})| = |\operatorname{Ker}(\pi_{G,K})| = |K|,$$

   on obtient :

   $$|B| = m''(m'n') = mn'.$$

   (b) Par l'hypothèse faite sur n', $mn' < mn$, et on a toujours $m \wedge n' = 1$, puisque $n' \mid n$. On peut donc utiliser encore une fois l'hypothèse de récurrence : B admet un sous-groupe H d'ordre m.
   Alors $\boxed{H \text{ est un sous-groupe de } G \text{ d'ordre } m}$.

2. On suppose qu'il n'existe pas de sous-groupe distingué K de G d'ordre $m'n'$, avec $m' \mid m$ et $n' \mid n$, $n' < n$ (hypothèse $\mathcal{H}$)

   (a)
   - G admet une suite principale $(G_i)_{i\in[\![0,r]\!]}$, avec $G_s = \{0\}$ (même démonstration par recherche d'un élément minimal que pour les suites de Jordan-Hölder). Soit $K = G_{s-1}$, le plus petit groupe non trivial de cette suite principale. Alors, par définition d'une suite principale, $\boxed{K \lhd G}$. De plus, d'après IV-2(i), il existe un entier a est un groupe simple S tels que

     $$K = G_{r-1} \simeq G_{r-1}/G_r \simeq S^a.$$

   - De plus, G est résoluble, donc G admet une suite de compositionn à quotients abéliens. En raffinant cette suite de composition, on obtient une suite de Jordan-Hölder donc les quotients sont abéliens aussi. D'après II-2(b), toute suite de Jordan-Hölder a donc des quotients abéliens.
   - On peut raffiner (G_i) en innsérant des groupes entre e et $G_{r-1} \simeq S^a$, en définissant

     $$G_{r-1,1} = G_{r-1} = S^j, \qquad G_{r-1,2} = S^{j-1} \times \{\mathrm{e}\}, \qquad \cdots \qquad G_{r-1,j} = S \times \{e\}^{j-1},$$

     et $G_{r-1,j+1} = G_r = \{e\}$. On vérifie facilement que pour $i \in [\![1, j]\!]$, $G_{r-1,i+1} \lhd G_{r-1,i}$. Ainsi, ce raffinement est une suite de composition, qu'on peut encore raffiner en une suite de Jordan-Hölder. Le premier terme non trivial de ce raffinement est $G_{r-1,j}$, car ce groupe est isomorphe à S, donc simple : on ne peut pas insérer d'autre groupe entre $\{0\}$ et S de sorte à obtenir encore une suite de composition. D'après le point précédent, les quotients de cette suite sont cycliques d'ordre p premier. En particulier,

     $$S \simeq G_{r-1,j} \simeq G_{r-1,j}/G_r$$

     est cyclique d'ordre p premier.
   - Ainsi, $\boxed{K \simeq S^a \text{ est d'ordre } p^a}$. Remarquez qu'au passage on a montré même que K est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^a$, donc est lui-même abélien.

   (b) D'après l'hypothèse $\mathcal{H}$, $n \div |K| = p^a$.. Comme $n \geqslant 2$, $m \wedge n = 1$, $p^a \wedge m = 1$. D'après le théorème de Lagrange, $p^a \mid mn$. Ainsi, d'après le théorème de Gauss, $p^a \mid n$. On en déduit que $\boxed{p^a = n}$
   Comme $p \wedge m = 1$, $\boxed{K \text{ est bien un } p\text{-Sylow de } G.}$

   (c) Soit L un sous-groupe distingué de G, vérifiant $K \lhd L$, $K \neq L$, et étant minimal pour cette propriété.
   La suite distinguée $\{e\} \lhd K \lhd L \lhd G$ peut être raffinée en une suite principale. Par minimalité de L, aucun groupe ne peut s'insérer entre K et L dans ce raffinement. Ainsi, d'après IV-2(i), il existe un entier b et un groupe simple T tel que $L/K \simeq T^q$. En quotientant par K, on obtient une suite principale de G/K de premier terme non trivial L/K. Le même raisonnement qu'en 2(a) montre qu'il existe un nombre premier q tel que T soit cyclique d'ordre q, donc $\boxed{|L/K| = q^b}$.
   En relevant par $\pi_{L,K}^{-1}$ (chaque élément étant relevé en une classe modulo K de cardinal $|K|$), on obtient

   $$\boxed{|L| = |K|q^b = p^a q^b}.$$

(d) Soit $t \in T = K \cap N_G(Q)$ et $g \in N_G(Q)$. On a
- $gtg^{-1} \in K$, puisque $K \lhd G$
- $gtg^{-1}Q(gtg^{-1})^{-1} = Q$, car g, t et g^{-1} sont dans $N_G(Q)$.

Ainsi, $gtg^{-1} \in T$, donc $\boxed{T \lhd N_G(Q)}$.

Par ailleurs, T est un sous-groupe de K, qui est abélien, d'après la remarque faite en question 2(a). Ainsi, $\boxed{T \text{ est abélien}}$.

(e)
- Soit $t \in T$ et $h \in Q$. Alors
  - $tht^{-1}h^{-1} \in Q$, car $tht^{-1} \in Q$, puisque $t \in N_G(Q)$.
  - $tht^{-1}h^{-1} \in T$, car $T \lhd N_G(Q)$, et $Q \subset N_G(Q)$.

  Ainsi, $tht^{-1}h^{-1} \in T \cap Q$. Or, d'après le théorème de Lagrange,
  - $|T \cap Q|$ divise $|T|$ qui lui-même divise $|K| = p^a$
  - $|T \cap Q|$ divise $|Q| = q^b$
  - $p^a \wedge q^b = 1$,

  Donc $|T \cap Q| = 1$ et ainsi, $T \cap Q = \{e\}$. On en déduit donc enfin que $tht^{-1}h^{-1} = e$, donc que $\boxed{th = ht}$. Ainsi, les éléments de T commutent avec tous les éléments de Q, ainsi qu'avec les éléments de K, puisque $T \subset K$ et K abélien.
- On a $Q \subset L$ et $K \subset L$, donc $\langle Q \cup K \rangle \subset L$. D'autre part, d'après Lagrange, $p^a = |K|$ et $q^b = |Q|$ divisent l'ordre de $\langle Q \cup K \rangle$, donc, puisque $p^a \wedge q^b = 1$, $p^a q^b$ divise $\langle Q \cup K \rangle$.
  On en déduit que $\boxed{\langle Q \cup K \rangle = L}$.
- Tout élément de L peut donc s'écrire comme un produit $x_1 \dots x_k$, où les x_i sont dans Q ou dans K (pas besoin de rajouter les inverses puisqu'ils sont déjà dans Q et K, le système de générateur considéré). Soit alors $t \in T$. Comme t commute avec chaque x_i, il commute avec leur produit, donc avec tout élément de L. On en déduit que $\boxed{T \subset Z(L)}$.

(f)
- Commençons par montrer que $Z(L) \lhd G$. Soit $z \in Z(L)$ et $g \in G$. On a alors :
  - $gzg^{-1} \in L$, car $L \lhd G$,
  - Pour tout $\ell \in L$, en posant $\ell' = g^{-1}\ell g \in L$ (puisque $L \lhd G$)

$$gzg^{-1}\ell = gzg^{-1}g\ell' g^{-1} = gz\ell' g^{-1} = g\ell' zg^{-1} = g\ell' g^{-1}gzg^{-1} = \ell gzg^{-1}.$$

  Ainsi, $gzg^{-1} \in Z(L)$.

  Cela prouve bien que $Z(L) \lhd G$.
- Si $Z(L) \neq \{e\}$, alors $p^a = n \mid Z(L)$, d'après la propriété $\mathcal{H}$. Soit K' un p-Sylow de $Z(L)$, c'est aussi un p-Sylow de L. D'après le deuxième théorème de Sylow, les p-Sylow de L sont deux-à-deux conjugués, donc sont tous conjugués à K. Mais puisque K est distingué, ses conjugués sont tous égaux à lui-même. Ainsi, K est le seul p-Sylow de L, et $K' = K$.
  On en déduit que $K \subset Z(L)$. Ainsi, K commute avec tout élément de L. Or, d'après la question préliminaire 1 ($K \lhd L$), on en déduit que

$$L = \langle K \cup Q \rangle = KQ.$$

- Soit alors $g \in G$ et $x \in Q$. On a $x \in L$ et $L \lhd G$, donnc $gxg^{-1} \in L$. Écrivons donc $gxg^{-1} = ky$, avec $k \in K$ et $y \in Q$. On a alors, par le thorème de Lagrange :

$$(gxg^{-1})^{q^b} = gx^{q^b}g^{-1} = geg^{-1} = e, \qquad \text{donc:} \qquad (ky)^{q^b} = e.$$

  Puisque $K \subset Z(L)$, il vient

$$e = (ky)^{q^b} = k^{q^b}y^{q^b} = k^{q^b},$$

  toujours du fait du théorème de Lagrange. Ainsi, l'ordre de k divise q^b. Mais comme $k \in K$, il divise aussi p^a. Puisque $p^a \wedge q^b = 1$, on en déduit que l'ordre de k est 1, donc $k = e$. Ainsi,

$$gxg^{-1} = y \in Q.$$

  Ainsi, $\boxed{Q \lhd G}$.

- Cela fournit donc un sous-groupe distingué de G d'ordre $m'n'$, avec $m' = q^b \mid m$ et $n' = 1 \mid n$, et $n' < n$. Ainsi, cela contredit l'hypothèse $\mathcal{H}$. On en déduit donc que l'hypothèse initiale est fausse, donc $\boxed{Z(L) = \mathrm{e}}$.

(g) On a donc $T = \{\mathrm{e}\}$.

- Cela implique dans un premier temps que $N_L(Q) = N_G(Q) \cap L = Q$. En effet, d'une part $Q \subset N_L(Q) \subset L$. D'autre part, on a déjà montré que $L = KQ$, donc aussi $L = KN_L(Q)$. Ainsi, l'application $(k, g) \mapsto kg$ est une surjection de $K \times N_G(Q)$ dans L. C'est aussi une injection. En effet, supposons que

$$kg = k'g', \qquad k, k' \in K, \qquad g, g' \in N_G(Q),$$

alors :

$$k'^{-1}k = g'g^{-1} \in K \cap N_G(Q) = \{e\},$$

donc $k = k'$ et $g = g'$. Ainsi, cette application est bijective. On déduit donc l'égalité des cardinaux :

$$|K||N_L(Q)| = |L|, \qquad \text{donc:} \qquad |N_L(Q)| = q^b.$$

On déduit alors du cardinal de Q et de l'inclusion $Q \subset N_L(Q)$ que $Q = N_L(Q)$.

- Considérons alors l'ensemble $\mathrm{C}_L(Q)$ des conjugués de Q dans L. Deux conjugués sont égaux ssi

$$gQg^{-1} = hQh^{-1} \qquad \text{soit:} \qquad (h^{-1}g)Q(h^{-1}g)^{-1} = Q,$$

donc si et seulement si $h^{-1}g \in N_L(Q)$ (avec h et g dans L), donc si et seulement si h et g sont dans la même classe à gauche modulo $N_L(Q) = Q$. Or, Q admet $|L|/|Q| = p^a$ classes à gauche.
Ainsi, $\boxed{Q \text{ admet exactement } p^a \text{ conjugués dans } L}$.

(h) Tous les conjugués (dans G) de Q sont inclus dans L, car $L \lhd G$. De plus, ils ont tous même cardinal q^b. Ce sont donc tous des q-Sylow de L. D'après le deuxième théorème de Sylow, les q-Sylow de L sont deux à deux conjugués (dans L), donc sont tous conjugués (dans L) à Q. Ainsi, tous les conjugués dans G de Q sont aussi des conjugués dans L de Q. On en déduit que

$$\boxed{|\mathrm{C}_G(Q)| = |\mathrm{C}_L(G)| = p^a}.$$

(i) L'argument précédent sur le nombre de conjugués de Q dans L vaut aussi pour le nombre de ses conjugués dans Q. Ainsi, le nombre de conjugués distincts de Q dans G est égal au nombre de classes modulo $N_G(Q)$ dans G. Ainsi :

$$p^a = \frac{|G|}{|N_G(Q)|}.$$

D'après la question 2(b), $n = p^a$, donc

$$|N_G(Q)| = m.$$

On a bien trouvé un $\boxed{\text{sous-groupe de } G \text{ d'ordre } m}$.

NB : Ce théorème est d'autant plus fort que le nombre de groupes résolubles est grand. Or, un théorème important de théorie des groupes dit que tout groupe d'ordre impair est résoluble (théorème de Feit-Thompson, 1963). Sa démontration, qui tient en quelques centaines de pages, fera l'objet d'un prochain DM ou DS.

Sources :

- *The Theory of Groups*, Marshall Hall Jr., AMS Chelsea Publishing.
- *Algebra*, Serge Lang, Addision-Wesley Publishing Company
- *Groupes finis*, Jean-Pierre Serre (cours donné à l'ENS de Jeunes Filles, 1978-1979)