Devoir Confiné (4h)

Problème 1 – (Groupes résolubles et théorème de Sylow généralisé)

Tous les groupes de ce problème sont notés multiplicativement. Le neutre d'un groupe G sera noté e_G, ou simplement e s'il n'y a pas d'ambiguïté. On rappelle les définitions et résultats suivants, vus soit en cours, soit en TD, soit en DM. Ces résultats pourront être utilisés sans être redémontrés. En revanche, on fera une référence précise au résultat utilisé, en indiquant son nom rappelé dans l'énoncé.

Soit G un groupe.

- ***Groupes isomorphes.*** *On dit que le groupe H est isomorphe au groupe G s'il existe $\varphi : G \to H$ un isomophisme entre G et H. La notation $G \simeq H$ signifie que G et H sont isomorphes.*
- ***Sous-groupe distingué.*** *Un sous-groupe distingué H de G est un sous-groupe tel que pour tout $g \in G$ et tout $h \in H$, $ghg^{-1} \in H$; en d'autres termes, pour tout $g \in G$, $gHg^{-1} = H$ (l'égalité provenant de la symétrie de l'hypothèse).*
  Lorsque H est un sous-groupe distingué de G, on écrira $H \lhd G$. On dira que H est un sous-groupe distingué propre si de plus $H \neq G$.
- ***Groupe distingué propre.*** *On dit qu'un sous-groupe distingué propre $H \lhd G$ est maximal (dans G), s'il n'existe aucun sous-groupe distingué K de G tel que $H \subsetneq K \subsetneq G$.*
- ***Groupe simple.*** *Un groupe G est dit simple s'il n'admet pas d'autre sous-groupe distingué que $\{e\}$ et lui-même.*
- ***Groupe quotient.*** *On rappelle que si $H \lhd G$, l'ensemble $G/H = \{aH = Ha, a \in G\}$ peut être muni d'un produit, obtenu par passage au quotient de la loi de G, munissant ainsi G/H d'une structure de groupe. On rappelle que $|G/H| = |G|/|H|$. On note $\pi_{G,H} : G \longrightarrow G/H$ la projection canonique, qui à g associe sa classe $\overline{g} = gH$.*
- ***Quotient d'un morphisme****. On rappelle qu'un morphisme $f : G \to K$ passe au quotient $G/H \to K$ si et seulement si $H \subset \mathrm{Ker}(f)$.*
- ***Premier théorème d'isomophisme.*** *Soit $f : G \to H$ un morphisme de groupes surjectif. Alors $\mathrm{Ker}(f) \lhd G$ et l'application quotient $\tilde{f} : G/\mathrm{Ker}(f) \to H$ est un isomorphisme*
- ***Produits de groupes.*** *Soit H et K deux sous-groupes de G. Alors si $HK = KH$, HK est un groupe.*
- ***Centre d'un groupe.*** *Le centre d'un groupe G est le sous-groupe $Z(G) = \{z \in G \mid \forall g \in G,\ zg = gz\}$ des éléments commutant avec tous les autres. $Z(G)$ est un sous-groupe distingué de G.*
- ***Centre d'un p-groupe.*** *Soit p un nombre premier et G un p-groupe, c'est-à-dire un groupe d'ordre égal à une puissance de p. Si $|G| > 1$, alors $|Z(G)| > 1$ (le centre d'un p-groupe non trivial est non trivial).*
- ***Lemme de Cauchy.*** *Soit G un groupe d'ordre n. Si p est un nombre premier divisant n, il existe $x \in G$ d'ordre p.*
- ***Sous-groupes conjugués.*** *On dit que deux sous-groupes H et K de G sont conjugués s'il existe $g \in G$ tel que $gHg^{-1} = K$.*
- ***Premier théorème de Sylow.*** *Soit G un groupe d'ordre $p^a m$, avec p premier et $m \wedge p = 1$. Alors G admet un sous-groupe d'ordre p^a. Un tel sous-groupe est appelé p-Sylow de G.*
- ***Deuxième théorème de Sylow.*** *Les p-Sylow d'un groupe G sont deux-à-deux conjugués.*

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) Montrer que $HK = KH =< H \cup K >$
   (b) Montrer que $H \cap K \lhd H$
2. Soit G un groupe, $H \lhd G$ et $K \lhd G/H$. Montrer que $\pi_{G,H}^{-1}(K) \lhd G$.
3. Soit H et K deux sous-groupes de G tels que $H \cap K = \{e\}$, $H \lhd G$ et $K \lhd G$
   (a) Montrer que pour tout $h \in H$ et tout $k \in K$, $hk = kh$
   (b) Montrer que $\varphi : H \times K \longrightarrow HK$ définie par $\varphi((h,k)) = hk$ est un isomorphisme.

Partie I – Théorèmes d'isomorphisme

Nous donnons dans cette partie deux conséquences du premier théorème d'isomophisme, sous forme de deux résultats appelés respectivement deuxième et troisième théorèmes d'isomorphisme.

1. **Deuxième théorème d'isomophisme**
   Soit G un groupe, et H et K deux sous-groupes tels que $K \subset H$, $K \lhd G$ et $H \lhd G$
   (a) Montrer que $K \lhd H$.
   (b) Montrer que $H/K \lhd G/K$
   (c) Montrer que la projection $\pi_{G,H} : G \mapsto G/H$ passe au quotient, définissant $\overline{\pi}_{G,H} : G/K \mapsto G/H$, telle $\pi_{G,H} = \overline{\pi}_{G,H} \circ \pi_{G,K}$.
   (d) Déterminer le noyau de $\overline{\pi}_{G,H}$, et en déduire que les groupes $(G/K)/(H/K)$ et G/H sont isomorphes (deuxième théorème d'isomorphisme).
2. **Normalisateur**
   Soit G un groupe, et H un sous-groupe de G. Le normalisateur $N_G(H)$ est défini par :
   $$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$
   Montrer que $N_G(H)$ est un sous-groupe de G et que $H \subset N_G(H)$.
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) Montrer que HK est un sous-groupe de G et que $H \cap K \lhd H$.
   (b) En définissant un morphisme $H \longrightarrow HK/K$ et en considérant son noyau, montrer qu'il existe un isomorphisme
   $$H/(H \cap K) \xrightarrow{\simeq} HK/K \text{ (troisième théorème d'isomophisme)}$$
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) Montrer que $H(U \cap K) \lhd H(U \cap V)$ et $(H \cap V)K \lhd (U \cap V)K$.
   (b) À l'aide du troisième théorème d'isomorphisme, montrer que
   $$(U \cap V) \ / \ (H \cap V)(U \cap K) \simeq H(U \cap V) \ / \ H(U \cap K).$$
   (c) En déduire que $H(U \cap V) \ / \ H(U \cap K) \simeq (U \cap V)K \ / \ (H \cap V)K$ (lemme du papillon).

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

Soit G un groupe fini. Une suite de composition de G est une famille $(G_i)_{i \in [\![1,r]\!]}$ de sous-groupes de G tels que :

$$\{e\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 = G.$$

Ainsi, les groupes G_i forment une chaîne de sous-groupes distingués les uns dans les autres. Attention, cela ne signifie pas qu'ils sont tous distingués dans G.
Un raffinement de la suite de composition $(G_1, \dots, G_r)$ est une suite de composition

$$\{0\} \lhd G_{r-1,j_{r-1}} \lhd \cdots \lhd G_{r-1,1} \lhd \cdots\cdots \lhd G_{2,j_2} \lhd \cdots \lhd G_{2,1} \lhd G_{1,j_1} \lhd \cdots \lhd G_{1,1} = G,$$

où pour tout $i \in [\![1, r-1]\!]$, $G_{i,1} = G_i$. Ainsi, c'est une suite de composition obtenue de la première en insérant un certain nombre de termes.
On dit que deux suites de composition $(G_i)_{i \in [\![1,r]\!]}$ et $(H_j)_{j \in [\![1,s]\!]}$ sont équivalentes si la suite des quotients G_i/G_{i+1} et la suite des quotients H_j/H_{j+1} sont égales, à l'ordre près des facteurs.

1. **Théorème de Schreier**
   Soit
   $$\{0\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 \lhd G_0 = G \qquad \text{et} \qquad \{0\} = H_s \lhd H_{s-1} \lhd H_{s-2} \lhd \cdots \lhd H_1 \lhd H_0 = G.$$
   deux séries de composition. On définit pour $(i,j) \in [\![0, r-1]\!] \times [\![0, s-1]\!]$,
   $$G_{i,j} = G_{i+1}(H_j \cap G_i).$$
   (a) Montrer que $(G_{i,j})$ est un raffinement de (G_i).
   (b) En se servant d'un résultat de la partie I, construire de même un raffinement $(H_{j,i})$ de (H_j) équivalent à $(G_{i,j})$.
2. **Suite de Jordan-Hölder.**
   Soit $\{0\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 = G$ une suite de composition. On dit qu'il s'agit d'une suite de Jordan Hölder si elle est maximale, i.e. si elle n'est raffinée par aucune suite de composition autre qu'elle-même.
   (a) Montrer l'existence d'une suite de Jordan-Hölder $(G_i)_{i\in[\![1,r]\!]}$ de G.
   (b) Montrer que deux suites de Jordan-Hölder de G sont équivalentes.
   (c) Justifier que toute suite de composition peut être raffinée en une suite de Jordan-Hölder.
   (d) Montrer que les quotients G_i/G_{i+1} d'une suite de Jordan-Hölder sont simples.

Partie III – Groupes résolubles

Soit G un groupe fini. On dit qu'il est résoluble s'il admet une suite de composition (G_i) telle que tous les quotients G_i/G_{i+1} soient des groupes abéliens.

1. **Sous-groupes et quotients d'un groupe résoluble.**
   (a) Soit G un groupe résoluble et H un sous-groupe de G. Montrer que H est résoluble.
   (b) Soit G un groupe résoluble et $H \lhd G$. Montrer que G/H est résoluble.
   (c) Soit $H \lhd G$. Montrer réciproquement que si H et G/H sont tous deux résolubles, alors G est résoluble.
2. **Caractérisation de la résolubilité par les quotients d'une suite de Jordan-Hölder**
   (a) Soit A un groupe abélien. Montrer que A est simple si et seulement si A est cyclique d'ordre p premier.
   (b) Montrer que G est résoluble si et seulement si les quotients d'une suite de Jordan-Hölder sont des groupes cycliques d'ordre p premier.

Partie IV – Suites principales

Soit G un groupe fini et $\{e\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 = G$ une suite de composition de G. On dit que $(G_1, \ldots, G_r)$ est une suite distinguée de G si de plus pour tout $i \in [\![1, r]\!]$, $G_i \lhd G$. On dit que $(G_1, \ldots, G_r)$ est une suite principale si elle est distinguée et maximale (dans le sens où elle ne peut être raffiné par aucune suite distinguée autre qu'elle-même). Le but de cette partie est de montrer que les quotients d'une suite principale sont isomorphes à des puissances de groupes simples.
Soit $\{e\} = G_r \lhd G_{r-1} \lhd G_{r-2} \lhd \cdots \lhd G_1 = G$ une suite principale, et soit, pour $k \in [\![2, r]\!]$, $H \lhd G_{k-1}/G_k$ un sous groupe distingué de G_{k-1}/G_k, minimal parmi les sous-groupes distingués non triviaux.

1. Justifier que si $H = G_{k-1}/G_k$, G_{k-1}/G_k est simple.
2. On suppose que $H \neq G_{k-1}/G_k$.
   (a) Soit $K = \pi^{-1}_{G_{k-1},G_k}(H)$. Justifier que $G_k \lhd K \lhd G_{k-1}$.
   (b) Soit $\mathrm{Conj}_G(K)$ l'ensemble des conjugués de K par un élément g de G. Ainsi, $L \in \mathrm{Conj}_G(K)$ si et seulement s'il existe $g \in G$ tel que $L = gKg^{-1}$.
   Montrer que pour tout $L \in \mathrm{Conj}_G(K)$, $G_k \lhd L \lhd G_{k-1}$.
   (c) Montrer que $\left\langle \bigcup_{L\in\mathrm{Conj}_G(K)} L \right\rangle \lhd K$
   (d) En déduire que $\bigcup_{L\in\mathrm{Conj}_G(K)} L = G_{k-1}$.
   (e) Montrer qu'il existe une famille $(L_1, \ldots, L_j)$ d'éléments de $\mathrm{Conj}_G(K)$ tels que

(i) $G_{k-1} = \left\langle \bigcup_{i \in [\![1,j]\!]} L_i \right\rangle$;

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

(f) Montrer que pour tout $L \in \mathrm{Conj}_G(K)$, L est un sous-groupe distingué de G_{k-1} minimal parmi ceux contenant strictement G_k.

(g) En déduire que pour tout $j_0 \in [\![1,j]\!]$,

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

(h) À l'aide d'une des questions préliminaires, en déduire que

$$G_{k-1}/G_k \simeq L_1/G_k \times \cdots \times L_j/G_k.$$

(i) Soit $S = L_1/G_k$. Montrer que S est simple et que $G_{k-1}/G_k \simeq S^j = S \times \cdots \times S$.

Partie V – Théorèmes de Sylow généralisés

Le but de cette ultime partie est de montrer une généralisation du premier théorème de Sylow dans le cas de groupes résolubles. Plus précisément, étant donné un groupe fini résoluble G d'ordre mn avec $m \wedge n = 1$, il existe H un sous-groupe de G d'ordre m (H est appelé sous-groupe de Hall). On peut obtenir une description plus précise de la structure de G en fonction de sous-groupes de Sylow, mais les techniques nécessaires sont plus fines.

Le principe de la preuve repose sur une récurrence forte sur $|G|$. L'initialisation est faite sur les p-groupes : le théorème est trivial dans ce cas puisque $m = 1$ ou $m = p^a = |G|$. On considère donc G un groupe d'ordre mn, $m \wedge n = 1$ et $n \geqslant 2$. On suppose que pour tout groupe H d'ordre $k < mn$ si $k = m'n'$ avec $m' \wedge n' = 1$, alors H admet un sous-groupe H' d'ordre m'.

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

(a) En appliquant l'hypothèse de récurrence à G/K, montrer que G admet un sous-groupe d'ordre mn'.

(b) Montrer que G admet un sous-groupe 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) En considérant une suite principale, montrer que G admet un sous-groupe distingué K dont l'ordre est p^a, où p est un nombre premier et a un entier strictement positif.

Indication : G est résoluble. Qu'est-ce que ça implique sur les quotients d'une suite de composition ?

(b) Montrer qu'en raison de l'hypothèse $\mathcal{H}$, $n = p^a$ et K est un p-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. Montrer qu'il existe un nombre premier q et un entier strictement positif b tel que $|L/K| = q^b$. Quel est l'ordre de L ?

(d) Soit Q un q-Sylow de L, et $T = K \cap N_G(Q)$. Montrer que T est un sous-groupe distingué de $N_G(Q)$ et est abélien.

(e) Montrer que $T \subset Z(L)$.

(f) En remarquant que $Z(L) \lhd G$, montrer que $Z(L) = \mathrm{e}$.

Indication : On pourra montrer que sinon, $L = KQ$ puis que $Q \lhd G$, pour contredire l'hypothèse $\mathcal{H}$.

(g) En déduire que $|\mathrm{Conj}_L(Q)| = p^a$.

*(h) En déduire que $|\mathrm{Conj}_G(Q)| = p^a = n$.

(i) Déterminer alors l'ordre de $N_G(Q)$ et conclure.