Université Claude Bernard Lyon 1

MASTER M1-G

Algèbre

CORRECTION DU PARTIEL 2013

Problème.

A. Préliminaires.

1. Si a et b commutent à y, alors ab commute à y et a^{-1} commute également à y. Donc, $Z_G(y)$ est un sous-groupe de G. Par hypothèses, $H \subset Z_G(y) \subset G$. Donc, par Lagrange, l'ordre du p-groupe H est un diviseur de l'ordre de $Z_G(y)$, maximal, puisque maximal pour l'ordre de G. Conclusion, H est un p-Sylow de $Z_G(y)$.
2. Comme $g?g^{-1}$ est un automorphisme (intérieur) de G, il envoie un sous-groupe de G en un sous-groupe de même ordre. Il suffit donc de voir que $gHg^{-1} \subset Z_G(y)$.

   Soit h dans H, alors h commute à x par hypothèses. Donc $xhx^{-1} = h$. Appliquons l'automorphisme intérieur $g?g^{-1}$ pour obtenir $y(ghg^{-1})y^{-1} = ghg^{-1}$, ce qui implique $ghg^{-1} \in Z_G(y)$.
3. Comme H et gHg^{-1} sont deux p-Sylow de $Z_G(y)$, le théorème de Sylow dit qu'il existe un élément a de $Z_G(y)$ qui envoie l'un sur l'autre par conjugaison.
4. On vérifie que $n = a^{-1}g$ normalise bien H.

B. Un contre-exemple.

1. En calculant le cardinal de l'ensemble des bases de l'espace $\mathbb{F}_p^2$, on trouve que le groupe G a pour ordre $(p^3 - 1)(p^3 - p^2)(p^3 - p^2) = p^3(p-1)(p^2-1)(p^3-1)$. Comme p ne divise pas les trois derniers facteurs (sinon il diviserait 1), la p-valuation de l'ordre de G est 3. Le sous-groupe H est bien d'ordre p^3. C'est donc un p-Sylow de G.
2. Soit n triangulaire supérieure inversible et h dans H. Alors, $nhn^{-1} \in H$. Effectivement, le produit et l'inverse de matrices triangulaires supérieures est encore triangulaire supérieure. Et comme, dans ces produits, les diagonales se multiplients terme à terme, on obtient bien que nhn^{-1} n'a que des 1 sur la diagonales.

   Réciproquement. On suppose que $h = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Posons $P_k = (X-1)^k$ et $nhn^{-1} = h'$, avec $n \in N_G(H)$. Alors, n envoie bijectivement $\ker(P_k(h))$ sur $\ker(P_k(h'))$. Comme $\ker(P_1(h)) = \langle e_1 \rangle$ et $\ker(P_2(h)) = \langle e_1, e_2 \rangle$, on a $\dim \ker(P_1(h')) = 1$ et $\dim \ker(P_2(h')) = 2$. Or, comme $h' \in H$, on a déjà l'inclusion $\langle e_1 \rangle \subset \ker(P_1(h'))$ et $\langle e_1, e_2 \rangle \subset \ker(P_2(h'))$, d'où l'égalité. Résultat des courses, n respecte les sous-espaces $\langle e_1 \rangle$ et $\langle e_1, e_2 \rangle$, et donc n est triangulaire supérieure.
3. Il suffit de remplacer la base canonique (e_1, e_2, e_3) de $\mathbb{F}_p^3$ par (e_3, e_1, e_2). La matrice de permutation associée au 3-cycle (123) fait l'affaire.
4. Il suffit de regarder comme un système l'équation $nx = yn$, avec n triangulaire supérieure inversible pour voir que c'est impossible.
5. Les éléments x et y ne sont pas centraux dans H puisque x et y ne commutent pas.

C. Morphisme de transfert de Burnside.

1. $s \mapsto \sigma_s$ n'est rien d'autre que le morphisme $G \to \mathfrak{S}(G/H) \simeq \mathfrak{S}_n$ associé à l'action de G sur G/H par translation à gauche sur les classes.
2. On a $s.x_iH = x_{\sigma_s(i)}H$, ce qui donne directement $x_{\sigma_s(i)}^{-1} s x_i \in H$.
3. Avec ce nouveau choix, on a, comme H est abélien :

$$\mathrm{Ver}(s)' = \prod_{i=1}^{n} h'_{s,i} = \prod_{i=1}^{n} {x'_{\sigma_s(i)}}^{-1} s x'_i = \prod_{i=1}^{n} {h_{\sigma_s(i)}}^{-1} ({x_{\sigma_s(i)}}^{-1} s x_i) h_i =$$

$$= \prod_{i=1}^{n} ({x_{\sigma_s(i)}}^{-1} s x_i) \prod_{i=1}^{n} {h_{\sigma_s(i)}}^{-1} \prod_{i=1}^{n} h_i = \mathrm{Ver}(s).$$

4. On a, comme H est abélien :
$\mathrm{Ver}(ss') = \prod_{i=1}^n h_{ss',i} = \prod_{i=1}^n x_{\sigma_{ss'}(i)}^{-1} s x_{\sigma_{s'}(i)} x_{\sigma_{s'}(i)}^{-1} s' x_i = \prod_{i=1}^n x_{\sigma_{ss'}(i)}^{-1} s x_{\sigma_{s'}(i)} \prod_{i=1}^n x_{\sigma_{s'}(i)}^{-1} s' x_i =$ $\mathrm{Ver}(s)\,\mathrm{Ver}(s')$, après changement de variable $j = \sigma_{s'}(i)$ dans le premier produit.

D. Action d'un sous-groupe cyclique de G.

1. On fixe x dans X. Comme l'action est transitive et que $C_s/\mathrm{Stab}_x \simeq C_s.x = X$, on a bien $|X|$ divise l'ordre de C_s. Ainsi, Stab_x est un sous-groupe d'ordre $\frac{|C_s|}{|X|}$. On sait qu'un tel sous-groupe, dans le cas cyclique est unique et engendré par $s^{|X|}$. Il est clair que le noyau de l'action est contenu dans le stabilisateur de x. Réciproquement, comme C_s est abélien, et agit transitivement sur X, on a pour tout g de Stab_x et tout $y = h.x$ de X : $g.y = (gh).x = (hg).x = h.x = y$. Donc g est bien dans le noyau de l'action.
2. Pour tout k, $(g_k, sg_k, \cdots, s^{d_k-1}g_k)$ représente bien des classes distinctes, sinon, cela contredirait la question précédente, en prenant $X = O_k$, de cardinal d_k et $x = g_k$. De plus, pour des k distincts, on obtient bien des classes distinctes puisque les O_k sont disjointes. Donc, toutes ces classes sont bien distinctes. Il y en a $\sum_k d_k = n$. On a donc bien toutes les classes.
3. Avec les notations de **C**, on a, pour $1 \leq k \leq l$, que $s.(s^j g_k)H = s^{j+1} g_k H$ et donc, $h_{s,i} = (s^{j+1}g_k)^{-1} s (s^j g_k) = 1$.
4. On a, par **D**1), que s^{d_k} est dans le stabilisateur de g_k. Donc, $s^{d_k} g_k \in g_k H$, ce qui implique $g_k^{-1} s^{d_k} g_k \in H$.
5. C'est exactement la définition de $\mathrm{Ver}(s)$ pour le choix de représentants
$(g_1, sg_1, \cdots, s^{d_1-1}g_1, \cdots, g_k, sg_k, \cdots, s^{d_k-1}g_k \cdots, g_l, sg_l, \cdots, s^{d_l-1}g_l)$. Tous les $h_{s,i}$ sont égaux à 1 sauf éventuellement l d'entre eux égaux à $g_k^{-1} s^{d_k} g_k$.

E. Applications.

1. (a) En utilisant **A**, avec $x = s^{d_k}$ et $y = g_k^{-1} s^{d_k} g_k$, il vient que $g_k^{-1} s^{d_k} g_k = n_k^{-1} s^{d_k} n_k$ pour un élément du normalisateur du p-Sylow H. Mais comme celui-ci centralise le p-Sylow, on a $n_k^{-1} s^{d_k} n_k = s^{d_k}$.
   (b) On a donc $\mathrm{Ver}(s) = \prod_{k=1}^l g_k^{-1} s^{d_k} g_k = \prod_{k=1}^l s^{d_k} = s^{\sum_k d_k} = s^n$.
   (c) Comme H est un p-Sylow de G, p est premier avec $|G/H| = n$. On a donc une relation de Bezout $up^m + vn = 1$, où p^m est l'ordre de H et donc, par Lagrange, $s \mapsto s^v$ est l'automorphisme inverse de $s \mapsto s^n$ de H.

(d) On a un morphisme Ver : $G \to H$ qui induit par restriction un automorphisme de G sur H. Il existe donc une section à Ver (la réciproque de cet automorphisme) et donc, G est un produit semi-direct $Q \rtimes H$, où Q est le noyau de Ver.

2. (a) On sait que le groupe des automorphismes de $\mathbb{Z}/p^m\mathbb{Z}$ est d'ordre $\varphi(p^m) = p^{m-1}(p-1)$.

   (b) Le sous-groupe $N_G(H)$ est le plus grand sous-groupe dans lequel H est distingué. En particulier, il agit par conjugaison sur H. Cette action est une action par automorphisme et donc induit un morphisme de $N_G(H)$ dans $\mathrm{Aut}(H)$. Le noyau de cette action est le sous-groupe des z de $N_G(H)$ tels que $zhz^{-1} = h$ pour tout h dans H. C'est donc par définition $Z_G(H)$.

   On a donc un morphisme de $N_G(H)/Z_G(H)$ qui arrive sur $\mathrm{Aut}(H)$.

   (c) Comme H est abélien, on a $H \subset Z_G(H)$ et donc $N_G(H)/Z_G(H)$ est premier avec p. Comme le morphisme s'envoie sur $\mathrm{Aut}(H)$, l'ordre de $N_G(H)/Z_G(H)$ divise $p^{m-1}(p-1)$ et donc divise $p-1$ par le lemme de Gauss.

   (d) Comme p est le plus petit nombre premier qui divise l'ordre de G, aucun premier plus petit que p ne peut diviser $N_G(H)/Z_G(H)$, et donc $N_G(H) = Z_G(H)$. Ce qui prouve que H est centralisé par son normalisateur. On a montré que dans ces conditions, on avait bien que G est un produit semi-direct $Q \rtimes H$.

Exercice.

1. Par propriété universelle, le groupe libre L_{n-1}, engendré par $\hat{x}_i$ s'envoie sur $\mathfrak{S}_n$ par $\hat{x}_i \mapsto (1 i{+}1)$. On sait que les $(1\, i{+}1)$ forment une partie génératrice de $\mathfrak{S}_n$ et donc ce morphisme est surjectif. De plus, on voit par un calcul simple qu'ils vérifient les relations imposées par G_n. On peut donc quotienter par Noether et obtenir par passage au quotient un morphisme surjectif de G_n vers $\mathfrak{S}_n$.

2. On montre péniblement avec un cas par cas, et en utilisant les relations, que $H \cup x_{n-1}H \cup x_1x_{n-1}H \cup \cdots \cup x_{n-2}x_{n-1}H$ est une partie de G_n contenant e (en fait on n'en a pas vraiment besoin, mais c'est plus clair) et stable par multiplication à gauche par tous les x_i.

   Pour donner un exemple, lorsque l'on multiplie à gauche x_j, $1 \leq j \leq n-2$, par un élément de $x_ix_{n-1}H$, $1 \leq i \leq n-2$, on obtient un élément de $x_jx_ix_{n-1}H$, qui par la dernière relation et le fait que les x sont d'ordre 2, se voit être égale à $x_ix_{n-1}x_ix_jx_iH = x_ix_{n-1}H$. Tout le reste est à l'avenant.

3. Par récurrence, on a que H est isomorphe à $\mathfrak{S}_{n-1}$. Donc, G_n est de cardinal inférieur à $n \times |H| = n!$. Vu la surjection de G_n sur $\mathfrak{S}_n$, il vient l'inégalité inverse et donc l'égalité $|G_n| = n!$. D'où l'isomorphisme voulu, provenant de la surjectivité et de l'égalité des ordres.