Contrôle continu 3

Exercice 1

Soient $p > q > 2$ deux nombres premiers tels que q divise $p+1$ mais q^2 ne divise pas $p+1$. On veut montrer qu'il y a exactement trois groupes d'ordre p^2q à isomorphisme près. On rappelle que tout groupe d'ordre p^2 est abélien et isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

1. Soit G un groupe d'ordre p^2q. Montrer que G contient un sous-groupe distingué H d'ordre p^2 et un sous-groupe K d'ordre q. Montrer que $G = H \rtimes K$.
2. Dans cette question, on se donne un groupe abélien fini H. On s'intéresse aux produits semi-directs externes $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ où φ est un morphisme de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$. Pour tout $k \in \mathbb{Z}$, on note $\overline{k}$ la classe de k dans $\mathbb{Z}/q\mathbb{Z}$, et $\varphi_{\overline{k}} = \varphi(\overline{k})$. On dit que le morphisme φ est trivial lorsque $\varphi_{\overline{k}} = \mathrm{id}_H$ pour tout $\overline{k} \in \mathbb{Z}/q\mathbb{Z}$.
   (a) Pour $(h, \overline{k})$ et $(h', \overline{k'})$ dans $H \times \mathbb{Z}/q\mathbb{Z}$, comment est défini $(h, \overline{k}) \times_\varphi (h', \overline{k'})$?
   (b) Montrer que $\varphi(\overline{1})$ est d'ordre 1 ou q.
   (c) En déduire l'équivalence entre
      i. Il existe un produit semi-direct $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ qui n'est pas direct.
      ii. Le groupe $\mathrm{Aut}(H)$ contient un élément d'ordre q.
      iii. L'entier q divise $|\mathrm{Aut}(H)|$.
   (d) Montrer que $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ est abélien si et seulement si φ est trivial.
3. Dans cette question on suppose que H est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, montrer que tout produit semi-direct $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ est direct.
4. Dans cette question, on suppose que H est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$, donc $\mathrm{Aut}(H)$ est isomorphe à $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) = GL((\mathbb{Z}/p\mathbb{Z})^2)$, qui est d'ordre $(p^2-1)(p^2-p)$.
   (a) En déduire que la plus grande puissance de q divisant $|\mathrm{Aut}(H)|$ est q.
   (b) Montrer que si f_1 et f_2 sont deux éléments d'ordre q de $\mathrm{Aut}(H)$ alors il existe $g \in \mathrm{Aut}(H)$ et $a \in [\![1, q-1]\!]$ tels que $f_2^a = g \circ f_1 \circ g^{-1}$. Indication : que peut-on dire des sous-groupes $\langle f_1 \rangle$ et $\langle f_2 \rangle$ de $\mathrm{Aut}(H)$?
   (c) Soient φ et ψ les morphismes de groupes de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$ définis par $\varphi(\overline{1}) = f_1$ et $\psi(\overline{1}) = f_2$. Montrer qu'il existe $\alpha \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ tel que $\mathrm{Int}_g \circ \varphi = \psi \circ \alpha$.
   D'après un résultat vu en TD, l'application $\gamma : H \times_\varphi \mathbb{Z}/q\mathbb{Z} \to H \times_\psi \mathbb{Z}/q\mathbb{Z}$ définie par $\gamma((h, \overline{k})) = (g(h), \alpha(\overline{k}))$ est alors un isomorphisme de groupes.

Suite au dos.

5. On fixe un morphisme de groupe non trivial ψ de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2)$. Montrer que tout groupe d'ordre p^2q est isomorphe à $G_1 := (\mathbb{Z}/p^2\mathbb{Z}) \times \mathbb{Z}/q\mathbb{Z}$ ou à $G_2 := (\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/q\mathbb{Z}$ ou à $G_3 := (\mathbb{Z}/p\mathbb{Z})^2 \times_\psi \mathbb{Z}/q\mathbb{Z}$.
6. Montrer que G_1, G_2, G_3 ne sont pas isomorphes.

Un corrigé

1. Soit G un groupe d'ordre p^2q.

   D'après les théorèmes de Sylow, G contient un sous-groupe H d'ordre p^2 et un sous-groupe K d'ordre q. De plus, le nombre N_p de p-Sylow divise q, donc vaut 1 ou q, et il vérifie $N_p \equiv 1[p]$. Comme $q < p$, cela entraîne $N_q = 1$. Donc H est l'unique p-Sylow de G, donc distingué dans G. On peut aussi déduire le fait que $H \triangleleft G$ du fait que $[G : H] = q$ est le plus petit facteur premier de $|G|$ grâce au théorème de Frobénius.

   De plus $|H| \times |K| = p^2 \times q = |G|$ et $|H| \wedge |K| = p^2 \wedge q = 1$, ce qui entraîne que $H \cap K$ est réduit à $\{1_G\}$ (puisque l'ordre $H \cap K$ divise à la fois $|H| = p^2$ et $|K| = q$ donc vaut 1). Ainsi, $G = H \rtimes K$.

2. Soient H un groupe abélien fini H et φ un morphisme de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$.

   (a) Pour $(h, \overline{k})$ et $(h', \overline{k'})$ dans $H \times \mathbb{Z}/q\mathbb{Z}$,

   $$(h, \overline{k}) \times_\varphi (h', \overline{k'}) = (h\varphi_{\overline{k}}(h'), \overline{k} + \overline{k'}).$$

   (b) Comme $\varphi(\overline{1})^q = \varphi(q\overline{1}) = \varphi(\overline{q}) = \varphi(\overline{0}) = \mathrm{id}_H$, l'ordre de $\varphi(\overline{1})$ divise q donc vaut 1 ou q puisque q est premier.

   (c) De deux choses l'une :

   $*$ ou bien q divise $|\mathrm{Aut}(H)|$. Comme q est premier, $\mathrm{Aut}(H)$ contient au moins un élément f_1 d'ordre q d'après le théorème de Cauchy. Le morphisme de groupes $k \mapsto f_1^k$ de $\mathbb{Z}$ dans $\mathrm{Aut}(H)$ a un noyau qui contient $q\mathbb{Z}$. Par passage au quotient, il fournit un morphisme φ de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$, non trivial puisque $\varphi(\overline{1}) = f_1^1 \neq \mathrm{id}_H$.

   $*$ ou bien q ne divise pas $|\mathrm{Aut}(H)|$. D'après le théorème de Lagrange, $\mathrm{Aut}(H)$ ne contient pas d'élément d'ordre q. Pour tout morphisme φ de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$, $\varphi(\overline{1})$ est d'ordre 1 d'après la question 2b donc égal à id_H. Pour tout $k \in \mathbb{Z}$, $\varphi(\overline{k}) = \varphi(\overline{1})^k = \mathrm{id}_H$, donc φ est trivial.

   On en déduit les équivalences annoncées.

   (d) Si φ est trivial, alors $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ est abélien comme produit direct de groupes abéliens.

   Sinon, on peut trouver $k \in \mathbb{Z}$ tel que $\varphi_{\overline{k}} \neq \mathrm{id}_H$, puis $h \in H$ tel que $\varphi_{\overline{k}}(h) \neq h$. Donc $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ n'est pas abélien puisque

   $$(h, \overline{1}) \times_\varphi (1_H, \overline{k}) = (h\varphi_{\overline{1}}(1), k) = (h, k),$$

   $$(1_H, \overline{k}) \times_\varphi (h, \overline{1}) = (1_H\varphi_{\overline{k}}(h), k) = (\varphi_{\overline{k}}(h), k).$$

   On en déduit l'équivalence annoncée.

3. Si H est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, alors $\mathrm{Aut}(H)$ est isomorphe à $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ donc à $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Donc $|\mathrm{Aut}(H)| = p^2 - p = p(p-1)$. Or $q \geq 3$ et divise $p+1$, donc il ne divise ni $p-1$ ni p. Comme q est premier, il ne divise donc pas $|\mathrm{Aut}(H)|$. D'après la question 2c, tout morphisme de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$ est trivial, donc tout produit $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ est direct.

4. Dans cette question, on suppose que H est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

   (a) On a $|\mathrm{Aut}(H)| = (p^2-1)(p^2-p) = (p+1)(p-1)^2p$. Par hypothèse, la plus grande puissance de q divisant $p+1$ est q. Or q est premier et ne divise ni $p-1$ ni p. Ainsi, la plus grande puissance de q divisant $|\mathrm{Aut}(H)|$ est donc q.

   (b) Soient f_1 et f_2 deux éléments d'ordre q de $\mathrm{Aut}(H)$. D'après la question 4a, $\langle f_1\rangle$ et $\langle f_2\rangle$ de $\mathrm{Aut}(H)$ sont deux q-Sylow de $\mathrm{Aut}(H)$ donc sont conjugués. Il existe $g \in \mathrm{Aut}(H)$ tel que $\langle f_2\rangle = g \circ \langle f_1\rangle \circ g^{-1} = \langle g \circ f_1 \circ g^{-1}\rangle$. Comme $g \circ f_1 \circ g^{-1}$ est un générateur du groupe $\langle f_2\rangle$, qui est d'ordre q, il existe $a \in [\![1, q-1]\!]$ tel que $f_2^a = g \circ f_1 \circ g^{-1}$.

   (c) Soient φ et ψ les morphismes de groupes de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathrm{Aut}(H)$ définis par $\varphi(\overline{1}) = f_1$ et $\psi(\overline{1}) = f_2$. Pour tout $k \in \mathbb{Z}$,

$$\begin{aligned}(\mathrm{Int}_g \circ \varphi)(\overline{k}) &= g \circ \varphi(k) \circ g^{-1} \\ &= g \circ f_1^k \circ g^{-1} \\ &= (g \circ f_1 \circ g^{-1})^k \\ &= f_2^{ak} = \psi(\overline{ak}) = \psi(\overline{a}\overline{k}).\end{aligned}$$

   Donc $\mathrm{Int}_g \circ \varphi = \psi \circ \alpha$, où α est la multiplication par $\overline{a}$ dans $\mathbb{Z}/q\mathbb{Z}$. Comme q est premier et $a \in [\![1, q-1]\!]$, $\overline{a}$ est inversible dans $\mathbb{Z}/q\mathbb{Z}$, donc $\alpha \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Ainsi, les groupes $H \times_\varphi \mathbb{Z}/q\mathbb{Z}$ et $H \times_\psi \mathbb{Z}/q\mathbb{Z}$ sont isomorphes.

5. Soit G un groupe d'ordre p^2q. D'après la question 1 on peut l'écrire comme produit semi-direct interne $H \rtimes K$, avec H et K d'ordre p^2 et q. Donc G est isomorphe à un produit semi-direct externe de H par K. Mais H est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$, tandis que K est isomorphe à $\mathbb{Z}/q\mathbb{Z}$ puisqu'il est d'ordre q premier. Ainsi, G est donc isomorphe soit à un produit semi-direct (externe) de $\mathbb{Z}/p^2\mathbb{Z}$ par $\mathbb{Z}/q\mathbb{Z}$, soit à un produit semi-direct (externe) de $(\mathbb{Z}/p\mathbb{Z})^2$ par $\mathbb{Z}/q\mathbb{Z}$. Dans le premier cas, le seul produit possible est direct d'après la question 3, donc G est isomorphe à G_1. Dans le deuxième cas, G est isomorphe à G_2 ou à G_3 suivant que le produit est direct ou non, d'après la question 4c.

6. Les groupes G_1 et G_2 sont abéliens, mais pas G_3. Le groupe G_1 contient un élément d'ordre p^2, puisque le sous-groupe $\mathbb{Z}/p^2\mathbb{Z} \times \{\overline{0}\}$ est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Mais G_2 ne contient pas d'élément d'ordre p^2. En effet, l'ordre de tout élément $(h, \overline{k})$ de G_2 est $o(h) \vee o(\overline{k})$, qui divise pq.

   Ainsi, G_1, G_2, G_3 ne sont pas isomorphes.