Contrôle continu 3

Soit $p > 2$ un nombre premier. On veut montrer qu'il y a exactement cinq groupes d'ordre $2p^2$ à isomorphisme près. On rappelle que tout groupe d'ordre p^2 est abélien et isomorphe à l'un des deux groupes $H_1 := \mathbb{Z}/p^2\mathbb{Z}$ ou $H_2 := \mathbb{F}^2$, en notant $\mathbb{F} := \mathbb{Z}/p\mathbb{Z}$.

1. Pourquoi les groupes $G_1 := H_1 \times \{-1, 1\}$ et $G_2 := H_2 \times \{-1, 1\}$ sont-ils abéliens et non isomorphes ?
2. Soit $(H, +)$ un groupe abélien fini d'ordre impair ≥ 3.
   (a) Pour tout $k \in \{-1, 1\}$, on pose $\rho_k = k\ \mathrm{id}_H$. Montrer qu'on définit ainsi un morphisme de groupes non trivial ρ de $\{-1, 1\}$ dans $\mathrm{Aut}(H)$. Indication : montrer que pour tout $h \in H \setminus \{0_H\}$, $-h \neq h$.
   (b) Dans le groupe $H \rtimes_\rho \{-1, 1\}$, expliciter ce que vaut $(h, k) *_\rho (h', k')$, puis calculer $(h, k)^2$ et $(h, k)^{2p}$.
   (c) En déduire les éléments d'ordre 2 dans le groupe $H \rtimes_\rho \{-1, 1\}$.
3. On construit ainsi les groupes $G_3 := H_1 \rtimes_\rho \{-1, 1\}$, $G_4 := H_2 \rtimes_\rho \{-1, 1\}$ et $G_5 := \mathbb{F} \times (\mathbb{F} \rtimes_\rho \{-1, 1\})$. Pourquoi ces groupes sont-ils non abéliens et non isomorphes ? Indication : utiliser les questions 2b et 2c.
4. Soit G un groupe d'ordre $2p^2$. Montrer que
   (a) G contient un sous-groupe H d'ordre p^2 et un sous-groupe K d'ordre 2 ;
   (b) $G = H \rtimes K$;
   (c) G est isomorphe à un produit semi-direct de H_1 ou H_2 par $\{-1, 1\}$.
5. Soit $\varphi : k \mapsto \varphi_k$ un morphisme de groupes de $\{-1, 1\}$ dans $\mathrm{Aut}(H_1)$.
   (a) On note $\varphi_{-1}^{\circ 2} = \varphi_{-1} \circ \varphi_{-1}$. Montrer que $\varphi_{-1}^{\circ 2} = \mathrm{id}_{H_1}$.
   (b) Montrer que pour tout $r \in \mathbb{Z}$, $r^2 \equiv 1 \quad [p^2] \iff r \equiv \pm 1 \quad [p^2]$.
   (c) En utilisant le fait que $\mathrm{Aut}(H_1)$ est isomorphe à $(\mathbb{Z}/p^2\mathbb{Z})^\times$, en déduire que $\varphi_{-1} = \pm \mathrm{id}_{H_1}$ puis que $H_1 \rtimes_\varphi \{-1, 1\}$ est isomorphe à G_1 ou G_3.
6. Soit $\psi : k \mapsto \psi_k$ un morphisme de groupes de $\{-1, 1\}$ dans $\mathrm{Aut}(H_2)$. On rappelle que $\mathrm{Aut}(H_2) = GL(\mathbb{F}^2)$, où $\mathbb{F}^2$ est muni de sa structure de $\mathbb{F}$-espace vectoriel. Soient $E_1 = \mathrm{Ker}(\psi_{-1} - \mathrm{id}_{H_2})$ et $E_{-1} = \mathrm{Ker}(\psi_{-1} + \mathrm{id}_{H_2})$.
   (a) Montrer que $\mathbb{F}^2 = E_1 \oplus E_{-1}$. Qu'en déduit-on sur $\dim E_1$ et $\dim E_{-1}$?
   (b) Montrer que si $\dim E_{-1} \neq 1$, alors $\mathbb{F}^2 \rtimes_\psi \{-1, 1\}$ est isomorphe à G_2 ou G_4.
   (c) On suppose maintenant que $\dim E_{-1} = 1$. On fixe deux vecteurs non nuls $v_1 \in E_1$ et $v_{-1} \in E_{-1}$. Montrer qu'on obtient un isomorphisme de groupes de $G_5 = \mathbb{F} \times (\mathbb{F} \rtimes_\rho \{-1, 1\})$ dans $H_2 \rtimes_\psi \{-1, 1\}$ en posant $f\big((x, (y, k))\big) = (xv_1 + yv_{-1}, k)$. On rappelle que $\rho_k = k\ \mathrm{id}_{\mathbb{F}}$ pour tout $k \in \{-1, 1\}$.
7. Conclure.

Un corrigé

1. Les groupes $G_1 := H_1 \times \{-1,1\}$ et $G_2 := H_2 \times \{-1,1\}$ sont abéliens comme produit direct de groupes abéliens. Si h_1 est un générateur de H_1, alors $(h_1,-1)$ est d'ordre $o(h_1) \vee o(-1) = 2p^2$ dans G_1. En revanche, l'ordre dans G_2 de tout élément $(h_2,-1)$ divise $2p$ car $(h_2,-1)^{2p} = ((2p)h_2, (-1)^{2p}) = (0_{H_2}, 1)$. Donc G_1 et G_2 ne sont pas isomorphes.
2. Soit $(H,+)$ un groupe abélien d'ordre impair.
   (a) Pour tout k et k' dans $\{-1,1\}$, $\rho_k = k\,\mathrm{id}_H \in \mathrm{Aut}(H)$ et $\rho_k \circ \rho_{k'} = \rho_{kk'}$ car pour tout $x \in H$, $k(k'x) = (kk')x$. Donc l'application $k \mapsto \rho_k$ est un morphisme de groupes de $\{-1,1\}$ dans $\mathrm{Aut}(H)$. Montrons qu'il est non trivial. Pour tout $h \in H \setminus \{0_H\}$, h est d'ordre impair (car $o(h)$ divise $|H|$ impair) différent de 1, donc $2h \neq 0_H$, d'où $\rho_{-1}(h) = -h \neq h$. Donc $\rho_{-1} \neq \mathrm{id}_{H_1}$.
   (b) Pour tous (h,k) et (h',k') dans $H \times \{-1,1\}$,
   $$(h,k) *_\rho (h',k') = (h + \rho_k(h'), kk') = (h + kh', kk').$$
   Dans le groupe $H \rtimes_\rho \{-1,1\}$, on a donc $(h,k)^2 = ((1+k)h, 1)$ d'où $(h,k)^{2p} = (p(1+k)h, 1)$ puisque l'application $h \mapsto (h,1)$ est un morphisme de groupes de H dans $H \rtimes_\rho \{-1,1\}$.
   (c) Soit $(h,k) \in H \rtimes_\rho K$, différent du neutre $(0_H,1)$. Dans le groupe $H \rtimes_\rho \{-1,1\}$,
   $$(h,k)^2 = (0_H,1) \iff (1+k)h = 0_H \iff k = -1,$$
   puisque si $k = 1$, alors $h \neq 0_H$ d'où $2h \neq 0_H$ d'après la question 1. Ainsi, les éléments d'ordre 2 dans $H \rtimes_\rho \{-1,1\}$ sont les $(h,-1)$ pour $h \in H$.
3. Pour qu'un produit semi-direct externe $H \rtimes_\rho K$ soit abélien, il faut (et il suffit) que H, K soient abéliens et que le produit soit direct (c'est-à-dire que le morphisme ρ soit trivial). Ici, le morphisme ρ n'est pas trivial d'après la question 1. Donc les groupes G_3, G_4, G_5 ne sont pas abéliens.
   D'après la question 2c, les éléments d'ordre 2 dans G_3, G_4, G_5 sont respectivement ceux de $H_1 \times \{-1\}$, de $H_2 \times \{-1\}$ et de $\{0_{\mathbb{F}}\} \times \mathbb{F} \times \{-1\}$, dont les cardinaux sont p^2, p^2, p. Donc G_5 n'est isomorphe ni à G_3, ni à G_4.
   D'après la question 2b,
   (a) Dans le groupe G_3, $(\overline{1},1)^{2p} = (\overline{2p},1) \neq (\overline{0},1)$.
   (b) Pour tout $(h_2,k) \in G_4$, $(h_2,k)^{*2p} = (0_{H_2},1)$.
   L'ordre de tout élément divise $2p$ dans G_4, mais pas dans G_3.
   Ainsi, les groupes G_3, G_4 et G_5 sont deux-à-deux non isomorphes.
4. (a) D'après les théorèmes de Sylow, G contient un sous-groupe H d'ordre p^2 et un sous-groupe K d'ordre 2.

(b) Le sous-groupe H est d'indice 2 donc distingué dans G. Or $|G| = |H| \times |K|$ et $H \cap K = \{1_G\}$ car $|H|$ et $|K|$ sont premiers entre eux. Ainsi, $G = H \rtimes K$.

(c) Donc G est isomorphe à un produit semi-direct de H par K. Or H est isomorphe à H_1 ou H_2, tandis que K est d'ordre 2 donc isomorphe à $\{-1, 1\}$. Ainsi, G est isomorphe à un produit semi-direct de H_1 ou H_2 par $\{-1, 1\}$.

5. (a) On a $\varphi_{-1}^{\circ 2} = \varphi_{(-1)^2} = \varphi_1 = \mathrm{id}_{H_1}$.

(b) Soit $r \in \mathbb{Z}$. Pour que p^2 divise $r^2 - 1 = (r-1)(r+1)$, le nombre premier p doit diviser $r-1$ ou $r+1$, mais il ne peut pas diviser les deux car ces nombres diffèrent de 2 et $p \geq 3$. Si p divise l'un des facteurs, p^2 est premier avec l'autre, ce qui permet d'appliquer le lemme de Gauss. Ainsi,

$$r^2 \equiv \quad [p^2] \iff \big(p^2 | (r-1) \text{ ou } p^2 | (r+1)\big) \iff r \equiv \pm 1 \quad [p^2].$$

(c) Dans le groupe $(\mathbb{Z}/p^2\mathbb{Z})^\times$, les seuls éléments dont le carré est $\overline{1}$ sont $\pm\overline{1}$. Par isomorphisme, $\pm\mathrm{id}_{H_1}$ sont les deux seuls éléments de $\mathrm{Aut}(H_1)$ dont le carré est id_{H_1}. D'après la question 5a, on a donc $\varphi_{-1} = \pm\mathrm{id}_{H_1}$. Or $\varphi_1 = \mathrm{id}_{H_1}$. Donc φ est soit le morphisme trivial, soit le morphisme ρ défini comme à la question 2. Ainsi, $H_1 \rtimes_\varphi \{-1, 1\}$ est isomorphe à G_1 ou G_3.

6. (a) Comme à la question 5a, on voit que $\psi_{-1}^2 = \mathrm{id}_{H_2}$. L'application linéaire ψ_{-1} est donc une symétrie par rapport à $E_1 = \mathrm{Ker}(\psi_{-1} - \mathrm{id}_{H_2})$ et parallèlement à $E_{-1} = \mathrm{Ker}(\psi_{-1} + \mathrm{id}_{H_2})$. En particulier, les espaces E_1 et E_{-1} sont supplémentaires dans $\mathbb{F}^2$, donc $\dim E_1 + \dim E_{-1} = 2$.

(b) Si $\dim E_{-1} \neq 1$, alors $E = E_1$ ou $E = E_{-1}$ donc $\psi_{-1} = \mathrm{id}_{H_2}$ ou $\psi_{-1} = \mathrm{id}_{H_2}$. Le morphisme ψ est soit le morphisme trivial soit le morphisme ρ défini comme à la question 2, donc $\mathbb{F}^2 \rtimes_\psi \{-1, 1\}$ est isomorphe à G_2 ou G_4.

(c) Par construction, (v_1, v_{-1}) est une base de $\mathbb{F}^2$. La bijectivité de f en découle. Pour tout $(x, (y, k))$ et $(x', (y', k'))$ dans G_5,

$$\begin{aligned} f\big((x,(y,k)) * (x',(y',k'))\big) &= f\big((x+x', y+ky', kk')\big) \\ &= \big((x+x')v_1 + (y+ky')v_{-1}, kk'\big)\big) \\ &= \big((xv_1 + yv_{-1}) + (x'v_1 + ky'v_{-1}), kk'\big)\big) \\ &= \big((xv_1 + yv_{-1}) + \rho_k(x'v_1 + y'v_{-1}), kk'\big)\big) \\ &= (xv_1 + yv_{-1}, k) *_\rho (x'v_1 + y'v_{-1}, k') \\ &= f\big((x,(y,k))\big) *_\rho f\big((x',(y',k'))\big). \end{aligned}$$

Ainsi, f est un isomorphisme de groupes de G_5 dans $H_2 \rtimes_\psi \{-1, 1\}$.

7. Dans les questions 1 et 3, on a construit cinq groupes d'ordre $2p^2$ deux-à-deux non isomorphes. Les questions 4c, 5 et 6 montrent que tout groupe d'ordre $2p^2$ est isomorphe à l'un de ces cinq groupes. Donc on a exactement cinq groupes d'ordre $2p^2$ à isomorphisme près.