Groupes d'ordre pq

Salim Rostam

Soient $p < q$ deux nombres premiers et soit G un groupe d'ordre pq. En regardant les q-sous-groupes de Sylow de G on obtient que G s'écrit comme un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. Si $p \nmid q-1$, en regardant cette fois les p-sous-groupes de Sylow de G on obtient que ce produit est nécessairement direct et donc $G \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique par le théorème chinois. On suppose donc maintenant $p \mid q-1$. On veut montrer qu'il n'y a que deux produits semi-directs $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ à isomorphisme près.

Un tel produit semi-direct est donné par un morphisme $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Commençons par donner une description de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Lemme 1. *Soit $n \in \mathbb{N}^*$. L'application*

$$\mu : \left| \begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ \alpha & \longmapsto & (\mu_\alpha : n \mapsto \alpha n) \end{array} \right. ,$$

est un isomorphisme de groupes. En particulier, si $n = q$ est premier on a

$$\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}.$$

Démonstration. Un morphisme $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est déterminé par l'image de 1, puisque l'on a $f(k) = f(1 + \cdots + 1) = f(1) + \cdots + f(1) = kf(1)$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$. Réciproquement, tout application de cette forme est bien un morphisme de $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Puisque les ensembles de départ et d'arrivée ont le même cardinal, un tel morphisme f est bijectif (et donc un automorphisme) si et seulement si f est surjectif, c'est-à-dire si $f(k) = 1$ pour un certain k, puisqu'alors $f(ak) = a$ pour tout $a \in \mathbb{Z}/n\mathbb{Z}$ (l'élément 1 est un générateur de $\mathbb{Z}/n\mathbb{Z}$). Ainsi, le morphisme f est bijectif si et seulement si il existe k tel que $kf(1) = 1$ donc si et seulement si $f(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$.

On a donc montré que μ est bien définie et surjective. Pour tout $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^\times$ on a $\mu_{\alpha\beta}(k) = \alpha\beta k = \alpha\mu_\beta(k) = \mu_\alpha(\mu_\beta(k)) = \mu_\alpha \circ \mu_\beta(k)$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$ donc μ est bien un morphisme. De plus, le morphisme μ est injectif car si $\mu_\alpha = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$ alors $\mu_\alpha(k) = k$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$ donc $\alpha k = k$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$ donc $\alpha = 1$. Finalement, le morphisme μ est un isomorphisme.

Finalement, si $n = q$ est premier alors on conclut puisque l'on sait que $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique (voir l'exercice sur le groupe multiplicatif d'un corps fini) de cardinal $q-1$. (Rappelons que le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est de cardinal le nombre d'entiers de $\{1, \ldots, n\}$ premiers à n, mais non cyclique en général.) □

On donne maintenant le lemme qui va permettre de distinguer à isomorphisme près les différents produits semi-directs.

Lemme 2. *Soient N et H deux groupes. Soient $\phi : H \to \mathrm{Aut}(N)$ et $\alpha \in \mathrm{Aut}(H)$ deux morphismes. On a l'isomorphisme de groupes suivant :*

$$N \rtimes_{\phi\circ\alpha} H \simeq N \rtimes_\phi H,$$

un isomorphisme étant donné par l'application

$$f : \left| \begin{array}{rcl} N \rtimes_{\phi\circ\alpha} H & \longrightarrow & N \rtimes_\phi H \\ (n,h) & \longmapsto & (n, \alpha(h)). \end{array} \right.$$

Démonstration. Tout d'abord, on a deux morphismes $\alpha : H \to H$ et $\phi : H \to \mathrm{Aut}(N)$ donc la composition $\phi \circ \alpha$ est un morphisme $H \to \mathrm{Aut}(N)$ et on peut donc bien former le produit semi-direct $N \rtimes_{\phi\circ\alpha} H$. L'application $f : N \rtimes_{\phi\circ\alpha} H \to N \rtimes_\phi H$ de l'énoncé donnée par $(n,h) \mapsto (n,\alpha(h))$ est clairement bijective, d'inverse l'application $N \rtimes_{\phi\circ\alpha} H \leftarrow N \rtimes_\phi H$ donnée par $(n, \alpha^{-1}(h)) \leftarrow\!\shortmid (n,h)$. Ainsi, il suffit de montrer que f est un morphisme.

On note $\cdot_\phi$ (resp. $\cdot_{\phi\circ\alpha}$) la loi de groupe sur $N \rtimes_\phi H$ (resp. $N \rtimes_{\phi\circ\alpha} H$). Il suffit de vérifier que

$$f\big((n,h) \cdot_{\phi\circ\alpha} (n',h')\big) = f(n,h) \cdot_\phi f(n',h'),$$

pour tout $(n,h),(n',h') \in N \times H$. On a d'une part

$$(n,h) \cdot_{\phi\circ\alpha} (n',h') = (n\phi\circ\alpha(h)(n'), hh'),$$

donc

$$f\big((n,h) \cdot_{\phi\circ\alpha} (n',h')\big) = (n\phi\circ\alpha(h)(n'), \alpha(hh')),$$

et d'autre part

$$\begin{aligned} f(n,h) \cdot_\phi f(n',h') &= (n,\alpha(h)) \cdot_\phi (n', \alpha(h')) \\ &= (n\phi(\alpha(h))(n'), \alpha(h)\alpha(h')) \\ &= (n\phi\circ\alpha(h)(n'), \alpha(h)\alpha(h')), \end{aligned}$$

donc on conclut que f est bien un morphisme puisque $\alpha(h)\alpha(h') = \alpha(hh')$ car α est un morphisme. $\square$

À titre indicatif, on donne également le résultat suivant. À noter qu'il n'a pas d'intérêt dans notre cadre puisque $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ est commutatif.

Lemme 3. *Soient N et H deux groupes. Soient $\phi : H \to \mathrm{Aut}(N)$ et $u \in \mathrm{Aut}(N)$ deux morphismes. On considère le morphisme $\phi_u : H \to \mathrm{Aut}(N)$ donné par $\phi_u(h) \coloneqq u \circ \phi(h) \circ u^{-1}$ pour tout $h \in H$. On a l'isomorphisme de groupes suivant :*

$$N \rtimes_{\phi_u} H \simeq N \rtimes_\phi H,$$

un isomorphisme étant donné par l'application

$$f : \left| \begin{array}{rcl} N \rtimes_{\phi_u} H & \longrightarrow & N \rtimes_\phi H \\ (n,h) & \longmapsto & (u^{-1}(n), h). \end{array} \right.$$

Démonstration. Tout d'abord, l'application

$$\gamma_u : \left| \begin{array}{rcl} \mathrm{Aut}(N) & \longrightarrow & \mathrm{Aut}(N) \\ \psi & \longmapsto & u \circ \psi \circ u^{-1} \end{array} \right.$$

étant un morphisme (c'est même un *automorphisme intérieur*[1] de $\mathrm{Aut}(N)$), la composée $\gamma_u \circ \phi$ est bien un morphisme $H \to \mathrm{Aut}(N)$. Ainsi, cette composée n'étant rien d'autre que ϕ_u, on en déduit que $\phi_u : H \to \mathrm{Aut}(N)$ est bien un morphisme donc on peut former le produit semi-direct

1. Si G est un groupe, un automorphisme intérieur de G est un (auto)morphisme $\gamma_g : G \to G$ donné par $G \ni h \mapsto \gamma_g(h) \coloneqq ghg^{-1}$, pour $g \in G$.

$N \rtimes_{\phi_u} H$. L'application $f : N \rtimes_{\phi_u} H \to N \rtimes_\phi H$ de l'énoncé donnée par $(n,h) \mapsto \big(u^{-1}(n), h\big)$ est clairement bijective, d'inverse l'application $N \rtimes_{\phi_u} H \leftarrow N \rtimes_\phi H$ donnée par $\big(u(n), h\big) \leftarrow\!\shortmid (n,h)$. Ainsi, il suffit de montrer que f est un morphisme.

On note $\cdot_\phi$ (resp. $\cdot_{\phi_u}$) la loi de groupe sur $N \rtimes_\phi H$ (resp. $N \rtimes_{\phi_u} H$). Il suffit de vérifier que

$$f\big((n,h) \cdot_{\phi_u} (n',h')\big) = f(n,h) \cdot_\phi f(n',h'),$$

pour tout $(n,h),(n',h') \in N \times H$. On a d'une part

$$\begin{aligned}(n,h) \cdot_{\phi_u} (n',h') &= (n\phi_u(h)(n'), hh') \\ &= (n\, u \circ \phi(h) \circ u^{-1}(n'), hh')\end{aligned}$$

donc, en utilisant le fait que u^{-1} est un morphisme,

$$\begin{aligned}f\big((n,h) \cdot_{\phi_u} (n',h')\big) &= \Big(u^{-1}(n) u^{-1}\big(u \circ \phi(h) \circ u^{-1}(n')\big), hh'\Big) \\ &= \big(u^{-1}(n)\, \phi(h) \circ u^{-1}(n'), hh'\big),\end{aligned}$$

et d'autre part

$$\begin{aligned}f(n,h) \cdot_\phi f(n',h') &= (u^{-1}(n), h) \cdot_\phi (u^{-1}(n'), h') \\ &= \Big(u^{-1}(n)\phi(h)\big(u^{-1}(n')\big), hh'\Big),\end{aligned}$$

donc on conclut que f est bien un morphisme. $\square$

Finalement, énonçons un dernier résultat de standard de cours.

Lemme 4. *Soient $m, n \in \mathbb{N}^*$ avec $m \mid n$ et notons $k := \frac{n}{m}$. Alors $n\mathbb{Z}$ est un sous-groupe de $k\mathbb{Z}$ et l'application*

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & k\mathbb{Z}/n\mathbb{Z} \\ a & \longmapsto & ka \end{array},$$

est un isomorphisme.

Démonstration. Le groupe $n\mathbb{Z}$ est bien un sous-ensemble de $k\mathbb{Z}$ puisque $k \mid n$ donc c'est un sous-groupe. L'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & k\mathbb{Z}/n\mathbb{Z} \\ a & \longmapsto & ka \end{array},$$

est bien définie et

$$\begin{aligned} a \in \mathbb{Z} \text{ appartient au noyau } &\iff n \mid ka \\ &\iff km \mid ka \\ &\iff m \mid a,\end{aligned}$$

donc le noyau est $m\mathbb{Z}$. On conclut en appliquant le premier théorème d'isomorphisme. $\square$

On revient maintenant à notre exercice. Puisque $p \mid q-1$, on peut écrire $q - 1 = kp$ pour $k \in \mathbb{N}^*$. Ainsi, si $\psi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ est un morphisme alors $0 = \psi(0) = \psi(p) = p\psi(1)$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$ donc $q - 1 \mid p\psi(1)$ donc $k \mid \psi(1)$. Ainsi, on a $\psi(1) \in k\mathbb{Z}/(q-1)\mathbb{Z}$, ce groupe étant isomorphe par le Lemme 4 à $\mathbb{Z}/p\mathbb{Z}$ via le morphisme $\mathbb{Z}/p\mathbb{Z} \to k\mathbb{Z}/(q-1)\mathbb{Z}$ donné par $n \mapsto kn$. Ainsi, si pour tout $i \in \mathbb{Z}/p\mathbb{Z}$ on note $\psi_i : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ le morphisme donné par $\psi_i(1) = ik$, on a

$$\psi_i(n) = ikn = ink = \psi_1(in),$$

pour tout $n \in \mathbb{Z}/p\mathbb{Z}$ donc
$$\psi_i = \psi_1 \circ \mu_i, \tag{5}$$
où $\mu_i : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est le morphisme donné par la multiplication par $i \in \mathbb{Z}/p\mathbb{Z}$. On choisit maintenant un isomorphisme $\theta : \mathbb{Z}/(q-1)\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times$ (note[2]) et pour tout $i \in \mathbb{Z}/p\mathbb{Z}$ on note $\phi_i \coloneqq \mu \circ \theta \circ \psi_i$, où $\mu : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est l'isomorphisme du Lemme 1. En composant à gauche par $\mu \circ \theta$ la relation (5) devient
$$\phi_i = \phi_1 \circ \mu_i. \tag{6}$$
Si $i = 0$ alors $\phi_0 = \mathrm{id}_{\mathbb{Z}/q\mathbb{Z}}$ et le produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_0} \mathbb{Z}/p\mathbb{Z}$ est direct. Sinon, on a $i \neq 0$ et donc $i \in (\mathbb{Z}/p\mathbb{Z})^\times$ donc $\mu_i \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ par le Lemme 1. En particulier, par le Lemme 2 et (6) on a
$$\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_i} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}.$$

Ainsi, on sait que notre groupe G est soit isomorphe à $\mathbb{Z}/pq\mathbb{Z}$ soit à $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$. Pour conclure, il suffit donc de voir que $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$ n'est pas abélien. Pour tout $n \in \mathbb{Z}/p\mathbb{Z}$ on a
$$\phi_1(n) = \mu \circ \theta \circ \psi_1(n) = \mu \circ \theta(nk) = \mu_{\theta(nk)} \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}),$$
donc pour tout $(a, b), (a', b') \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ on a, dans $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$,
$$\begin{aligned}(a, b) \cdot (a', b') &= (a\phi_1(b)(a'), bb') \\ &= (a\mu_{\theta(bk)}(a'), bb') \\ &= (a\theta(bk)a', bb') \\ &= (aa'\theta(bk), bb'),\end{aligned}$$
en utilisant la commutativité de $\mathbb{Z}/q\mathbb{Z}$ pour la dernière égalité. On a donc
$$(a', b') \cdot (a, b) = (aa'\theta(b'k), bb')$$
dans $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$. Ainsi, en prenant par exemple $a = a' = 1$ on a
$$\begin{aligned}&(1, b) \cdot (1, b') \neq (1, b') \cdot (1, b) \text{ dans } \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z} \\ &\qquad \iff \theta(bk) \neq \theta(b'k) \text{ dans } \mathbb{Z}/q\mathbb{Z} \\ &\qquad \iff \theta(bk) \neq \theta(b'k) \text{ dans } (\mathbb{Z}/q\mathbb{Z})^\times \\ &\qquad \iff bk \neq b'k \text{ dans } \mathbb{Z}/(q-1)\mathbb{Z} \text{ (par injectivité de } \theta) \\ &\qquad \iff bk \neq b'k \text{ dans } k\mathbb{Z}/(q-1)\mathbb{Z} \\ &\qquad \iff b \neq b' \text{ dans } \mathbb{Z}/p\mathbb{Z} \text{ (par le Lemme 4).}\end{aligned}$$
Ainsi, le groupe $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/p\mathbb{Z}$ n'est jamais abélien et on conclut.

2. Un tel isomorphisme θ est donné par $\theta(i) = \alpha^i$ où α est un générateur de $(\mathbb{Z}/q\mathbb{Z})^\times$.