TD n°6 : Produits semi-directs

27/10/2023

Exercice 1. Engendrer $\mathfrak{A}_n$

1. Soit $n \geq 5$ impair. Démontrer que le grand cycle $(1\,2\,\ldots\,n)$ et le 3-cycle $(1\,2\,3)$ engendrent $\mathfrak{A}_n$.
2. Soit $n \geq 6$ pair. Démontrer que le cycle $(2\,3\,\ldots\,n)$ et le 3-cycle $(1\,2\,3)$ engendrent $\mathfrak{A}_n$.

Correction de l'exercice 1 :

1. Appelons c le grand cycle. Les conjugués de $(1\,2\,3)$ par le grand cycle donnent tous les $(i\,(i+1)\,(i+2))$. En conjuguant $(1\,2\,3)$ par $(3\,4\,5)$ et ses puissances, nous obtenons les 3-cycles $(1\,2\,4)$ et $(1\,2\,5)$. En répétant l'opération avec les $(i\,(i+1)\,(i+2))$, nous obtenons tous les 3-cycles de la forme $(1\,2\,j)$ et leurs inverses $(2\,1\,j)$. Prenons ensuite un cycle $(2\,i\,j)$ avec $i \neq j$. Si i ou j vaut 1, nous avons déjà obtenu ce cycle ; sinon, la conjugaison de $(1\,2\,j)$ par $(1\,2\,i)$ fournit effectivement $(2\,i\,j)$. En conjuguant de nouveau par c, nous obtenons tous les 3-cycles, qui engendrent $\mathfrak{A}_n$.
2. Appelons d le grand cycle. En conjuguant $(1\,2\,3)$ par d, nous obtenons $(1\,3\,4)$. En conjuguant $(1\,2\,3)$ par $(1\,3\,4)$ puis en inversant, nous obtenons $(2\,3\,4)$. La question précédente appliquée à l'ensemble $\{2,\ldots,n\}$ affirme alors que tous les 3-cycles à support dans $\{2,\ldots,n\}$ sont dans le groupe engendré. Il reste à traiter le cas des 3-cycles de la forme $(1\,i\,j)$. Puisque $n \geq 6$, il existe dans les permutations paires de $\{2,\ldots,n\}$ une permutation σ envoyant 2 sur i et 3 sur j. À ce moment,
$$(1\,i\,j) = \sigma(1\,2\,3)\sigma^{-1}.$$

Exercice 3. Sous-groupes d'indice n de $\mathfrak{S}_n$

Soit $n \geq 3$.

1. Rappeler pourquoi les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$ sauf dans le cas $n = 4$ où il faut ajouter K_4.
2. Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$. Démontrer que l'action de $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}/_H$ par translation est fidèle.
3. Démontrer que H est isomorphe à $\mathfrak{S}_{n-1}$.

Correction de l'exercice 3 :

1. Voir votre cours.
2. Considérons le noyau de l'action par translation de $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}/_H$. Il s'agit d'un sous-groupe distingué contenu dans le stabilisateur de $\{H\}$ qui est H. Son indice est donc divisible par n. Ce n'est le cas d'aucun des sous-groupes de la question précédente. Nous avons montré que l'action de $\mathfrak{S}_n$ était fidèle ; a fortiori celle de H.
3. Puisque l'action est fidèle, nous déduisons un morphisme injectif
$$H \hookrightarrow \mathfrak{S}_{{}^{\mathfrak{S}_n}/_H}.$$
L'image étant contenue dans les permutations qui fixent $\{H\}$, un argument de cardinalité montre que cela établit un isomorphisme entre H et le sous-groupes des permutations qui fixent $\{H\}$. Ce dernier sous-groupe est isomorphe à $\mathfrak{S}_{n-1}$ puisque $|{}^{\mathfrak{S}_n}/_H| = n$.

Exercice 5. Centre d'un produit semi-direct

Soit N un groupe abélien et K un groupe muni d'un morphisme $\varphi : K \to \mathrm{Aut}(N)$.

1. Démontrer que le centre de $N \rtimes_\varphi K$ est égal ensemblistement à $N^{\varphi(K)} \times [\mathrm{Ker}(\varphi) \cap \mathrm{Z}(K)]$ dénote les éléments fixés par tous les automorphismes de $\varphi(K)$. Vérifier que la structure de groupe produit est effectivement la structure de groupe induite par l'inclusion dans $N \rtimes_\varphi K$.
2. Décrire à présent le centre ensemblistement en ôtant l'hypothèse d'abélianité sur N.

Correction de l'exercice 5 :

Nous choisirons de noter nk l'élément (n, k) du produit semi-direct et la mulitplication du produit semi-direct vérifie donc que $nkn'k' = n\varphi(k)(n')kk'$.

1. Supposons que n_0k_0 appartienne au centre. Cela signifie que pour tout $k \in K$, on a

$$\varphi(k)(n_0)kk_0 = kn_0k_0 = n_0k_0k$$

d'où en identifiant $n_0 = \varphi(k)(n_0)$ (resp. $kk_0 = k_0k$) ce qui se reformule en $n_0 \in N^{\varphi(K)}$ (resp. $k \in \mathrm{Z}(K)$). D'un autre côté, pour tout $n \in N$, on a

$$nn_0k_0 = n_0k_0n = n_0\varphi(k_0)(n)k_0$$

ce qui implique puisque N est abélien que $n = \varphi(k_0)(n)$. Nous obtenons que $k_0 \in \mathrm{Ker}(\varphi)$. L'élément n_0k_0 appartient bien au produit annoncé. Réciproquement si l'élément appartient à $N^{\varphi(K)} \times [\mathrm{Ker}(\varphi) \cap \mathrm{Z}(K)]$, il commute à N et à K par les mêmes calculs que précédemment, donc appartient au centre.

2. Dans le cas général, le deuxième calcul n'implique plus la même chose. Cela se reformule par

$$nn_0 = n_0\varphi(k_0)(n),$$

ce qui se reformule en $\mathrm{Int}(n_0^{-1}) = \varphi(k_0)$. Le centre est donc précisément

$$\left\{ n_0k_0 \in N^{\varphi(K)} \times \mathrm{Z}(K) \,|\, \mathrm{Int}(n_0^{-1}) = \varphi(k_0) \right\}.$$

En termes catégoriques nous pouvons l'exprimer comme le produit fibré

$$N^{\varphi(K)} \times_{\mathrm{Int}(-^{-1}),\mathrm{Aut}(N),\varphi} \mathrm{Z}(K).$$

Mais avec une structure de groupe bien étrange qui le rend abélien. Remarquons que dans de nombreux cas, le centre sera bien plus simple, par exemple si $N^{\varphi(K)} \subseteq \mathrm{Z}(N)$ où on obtient le même résultat qu'à la question précédente, ou si $\mathrm{Z}(K) \cap \varphi^{-1}(\mathrm{Int}(N))$ se contrôle.

Exercice 8. Groupes d'ordre pq

Soient $p > q$ deux nombres premiers. Nous souhaitons classer puis déplier la structure des groupes d'ordre pq. Soit G un tel groupe.

1. Démontrer qu'il existe un élément g_p d'ordre p dans G puis que $\langle g_p \rangle$ est distingué dans G.
2. Démontrer que G est isomorphe à un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ par μ_p.
3. On suppose de plus que $q \nmid p - 1$. Démontrer que G est cyclique.
4. On suppose à présent, que $q \mid p - 1$. Démontrer qu'il existe un élément z d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On fixe un tel z pour la suite de la question. En déduire que G est cyclique ou isomorphe au produit semi-direct

$$\mu_p \rtimes_{\alpha_z} \mathbb{Z}/q\mathbb{Z}, \text{ où } \alpha_z(x) = [\zeta \mapsto \zeta^{(z^x)}].$$

Expliquer pourquoi ces deux groupes ne sont pas isomorphes.

5. Dans le cas d'un groupe non cyclique, démontrer qu'il existe un unique p-Sylow et qu'il est caractéristique [1]. Démontrer aussi que le centre est trivial.
6. Toujours dans le cas d'un groupe non abélien, calculer le groupe dérivé. Conclure que tout groupe d'ordre pq est résoluble.

Correction de l'exercice 8 :

1. Le lemme de Cauchy démontre qu'il existe un élément d'ordre p. Pour conclure que le sous-groupe engendré est distingué, nous proposons deux solutions. Puisque $p > q$, un tel sous-groupe est d'indice le premier minimal divisant le cardinal de G : le lemme de Ore (cf. exercice 2 du TD n°5) permet de conclure.

   De manière moins théorique, soit g_p un élément d'ordre p et $g \in G$. L'intersection $\langle g_p\rangle \cap g\langle g_p\rangle g^{-1}$ est de cardinal divisant p. Si elle était triviale, l'application

   $$\langle g_p\rangle \times g\langle g_p\rangle g^{-1} \to G, \ \ (h_1, h_2) \mapsto h_1 h_2$$

   serait injective (cf. exercice 5 du TD n°1). Cela entraînerait que $|G| \geq p^2$. Par l'absurde, l'intersection est donc de cardinal p, autrement dit

   $$\langle g_p\rangle = g\langle g_p\rangle g^{-1}.$$

   Nous venons de démontrer que $\langle g_p\rangle$ est distingué.
2. Le sous-groupe $\langle g_p\rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et le quotient de G par $\langle g_p\rangle$ à $\mathbb{Z}/q\mathbb{Z}$. Il nous suffit de trouver un complément de $\langle g_p\rangle$ dans G : alors G sera produit semi-direct interne d'un groupe isomorphe à $\mathbb{Z}/q\mathbb{Z}$ par un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$, ce qui conclut. Trouver un complément revient à trouver un élément d'ordre q qui n'est pas dans $\langle g_p\rangle$. Les premiers sont différents ; ainsi, il nous suffit de trouver un élément d'ordre q dans G, ce que le lemme de Cauchy nous fournit avec mansuétude.
3. Il existe une identification de $\langle g_p\rangle$ à μ_p. Le groupe d'automorphismes de $\langle g_p\rangle$ est donc isomorphe à $\mathrm{Aut}(\mu_p)$, i.e. $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclique d'ordre $p-1$. Pour un complément K de $\langle g_p\rangle$ comme à la question précédente, la conjugaison fournit un morphisme de groupes

   $$\varphi \ : \ K \to \mathrm{Aut}\left(\langle g_p\rangle\right).$$

   Les groupes à la source et au but ont des cardinaux premiers entre eux puisque $q \nmid p-1$: le morphisme est trivial. Cela signifie que les éléments de K et de $\langle g_p\rangle$ commutent entre eux. Dans ce cas G est isomorphe à $\langle g_p\rangle \times K$ (voir l'exercice 5 du TD n°1), cyclique grâce à l'isomorphisme des restes chinois.
4. Comme $q \mid p-1$ et que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, il existe des éléments d'ordre q et que les éléments d'ordre divisant q sont exactement $\langle z\rangle$. Soit h un élément d'ordre q dans G. La conjugaison par h induit un automorphisme de $\langle g_p\rangle$ qui s'écrit $g \mapsto g^t$ pour un certain élément t de $(\mathbb{Z}/p\mathbb{Z})^\times$. Puisque h est d'ordre q, la conjugaison par h est d'ordre divisant q ce qui implique que t est d'ordre divisant q. Si $t = 1$, la conjugaison par h est triviale et les mêmes arguments qu'à la question précédente nous font retomber sur le cas d'un groupe cyclique. Sinon, t est d'ordre q. Quitte à remplacer h par l'une de ses puissances, nous pouvons supposons que la conjugaison par h s'identifie à la puissance z-ième. En prenant une identification de $\langle g_p\rangle$ à μ_p et l'identification de son complément $\langle h\rangle$ à $\mathbb{Z}/q\mathbb{Z}$ qui envoie h sur 1, la proposition 7.8 sur le suivi des isomorphismes fournit un isomorphisme entre le groupe G et

   $$\mu_p \rtimes_{\alpha_z} \mathbb{Z}/q\mathbb{Z}.$$

   Pour démontrer que ces groupes ne sont pas isomorphes, nous remarquons que l'élément d'ordre q choisi agit par conjugaison sur $\langle g_p\rangle$ de manière non triviale. A fortiori, notre produit semi-direct n'est pas abélien.
5. Gardons les notations de la preuve précédente : le groupe d'ordre pq sera G, l'élément d'ordre p choisi sera encore g_p et l'élement d'ordre q convenable sera noté h. Notons également $G_p = \langle g_p\rangle$. Nous allons

1. Sans utiliser le théorème de Sylow.

démontrer que les seuls éléments d'ordre p de G sont $G_p \backslash \{e\}$. Prenons un élément g d'ordre p. Son image par la projection

$$G \to {}^{G}/_{G_p} \cong \mathbb{Z}/q\mathbb{Z}$$

est un élément d'ordre divisant p (parce qu'il divise l'ordre de g) et divisant q (parce qu'il appartient à un groupe d'ordre q). Son image est donc triviale, i.e. $g \in \langle g_p \rangle$. Nous avons démontré que les seuls éléments d'ordre divisant p sont G_p. C'est donc l'unique p-Sylow, et il est même caractéristique puisque tout automorphisme stabilise les éléments d'ordre divisant p.

Pour qu'un élément soit dans le centre, il faut et suffit que son action par conjugaison soit triviale. Puisque G_p est abélien, l'action par conjugaison de $g_p^k h^l$ sur G_p est la même que celle de h^l ; elle correspond à $\alpha_z(l)$, i.e. la puissance z^l-ième. Ils n'appartient donc au centre que si h^l est le neutre. Le centre est par conséquent contenu dans G_p. Mais pour des raison similaires aucun élément non trivial de G_p ne commute à h. Le centre de G est réduit au neutre.

6. Calculons un commutateur avec des notations additives. Nous rappelons que $(k,l)^{-1} = (-z^{-l}k, -l)$

$$\begin{aligned}
[(k,l);(k',l')] &= (k,l)(k',l')(-z^{-l}k,-l)(-z^{-l'}k',-l') \\
&= (k+z^l k', l+l')(-z^{-l}k,-l)(-z^{-l'}k',-l') \\
&= (k+z^l k' - z^{l'}k, l')(-z^{-l'}k',-l') \\
&= ((1-z^{l'})k - (1-z^l)k', 0)
\end{aligned}$$

Et on démontre que les commutateurs donnent exactement G_p.

Nous proposons une autre méthode plus conceptuelle. L'image par la projection du groupe dérivé de G est contenue dans le groupe dérivé de ${}^{G}/_{G_p}$ qui est abélien. Ceci implique que son image est triviale, autrement dit que $\mathrm{D}(G) \subseteq G_p$. Les seuls sous-groupes possibles sont $\{e\}$ et G_p. Si le groupe dérivé était trivial, le groupe G serait abélien, ce que nous avons contredit. Cela prouve de manière plus conceptuelle que $\mathrm{D}(G) = G_p$.

Le groupe dérivé étant abélien, le groupe est résoluble d'indice 2.

Exercice 9. Groupes d'ordre p^2q

Soient p, q deux nombres premiers. Classer les groupes d'ordre p^2q à isomorphisme près.

Correction de l'exercice 9 :

Soit G un groupe d'ordre p^2q. Puisqu'il est impossible d'avoir simultanément $q \equiv 1\,[p]$ et $p \equiv 1\,[q]$. Les théorèmes de Sylow nous affirme alors que l'un des Sylow est distingué.

Cas d'un unique q-Sylow

Commençons par traiter le cas où il existe un unique q-Sylow G_q. Un p-Sylow fournissant un complément dans G, le groupe G s'écrit systématiquement comme produit semi-direct interne

$$G_q \rtimes_\varphi G_p$$

correspondant à un morphisme

$$\varphi : G_p \to \mathrm{Aut}(G_q) \cong \left(\mathbb{Z}/q\mathbb{Z}\right)^\times.$$

Dans le cas où $p \nmid q-1$, ce produit semi-direct est nécessairement trivial ce qui affirme que G est abélien. Nous obtenons les deux classes d'isomorphismes de groupes suivant, que nous écrivons avec les diviseurs élémentaires :

$$\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \text{ et } \mathbb{Z}/q\mathbb{Z} \times \left(\mathbb{Z}/p\mathbb{Z}\right)^2.$$

Nous distinguons à présent selon la tête du p-Sylow, qui ne dépend que de la classe d'isomorphisme de G.

Supposons à présent que G_p est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ et que $p \mid q-1$ sans quoi nous avons déjà examiné les possibilités. Posons α un élément d'ordre p de $(\mathbb{Z}/q\mathbb{Z})^\times$. Pour que le produit semi-direct ne soit pas direct, il faut et suffit qu'un élément de G_p soit envoyé sur α (après identification de G_q à $\mathbb{Z}/q\mathbb{Z}$). Il est alors possible de décomposer $G_p = \langle g_p \rangle \times \mathrm{Ker}(\varphi)$ où g_p est envoyé sur α. À isomorphisme près, le groupe G est donc isomorphe à

$$(\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\alpha} \mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/p\mathbb{Z}$$

où $\varphi_\alpha(k)$ est la multiplication par α^k.

Supposons à présent que G_p est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ et que $p \nmid q-1$ sans quoi nous avons déjà examiné les possibilités. Si $p^2 \nmid q-1$, en gardant les notations du paragraphe précédent, pour que le produit semi-direct ne soit pas direct, il faut et suffit que φ ne soit pas trivial. En particulier, l'image d'un élément d'ordre p^2 de G_p est non triviale. Par hypothèse, elle est nécessairement d'ordre p et quitte à bien choisir notre élément d'ordre p^2, on peut suppose que son image est α. Le groupe G est alors isomorphe à

$$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\alpha} \mathbb{Z}/p^2\mathbb{Z}$$

où $\varphi_\alpha(k)$ est la multiplication par α^k. Si $p^2 \mid q-1$, prenons β un élément d'ordre p^2 de $(\mathbb{Z}/q\mathbb{Z})^\times$. Pour que le produit semi-direct ne soit pas direct, il faut et suffit que φ ne soit pas trivial. En particulier, l'image d'un élément d'ordre p^2 de G_p est non triviale. Si elle est d'ordre p, nous retombons sur le paragraphe précédent. Sinon, cette image est d'ordre p^2 et quitte à bien choisir notre élément d'ordre p^2, il est envoyé sur β. Le groupe G est alors isomorphe à

$$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\beta} \mathbb{Z}/p^2\mathbb{Z}$$

où $\varphi_\beta(k)$ est la multiplication par β^k.

Pour distinguer tous ces groupes des groupes abéliens, il suffit de remarquer qu'ils sont non abéliens. Pour les distinguer entre eux, deux critères suffisent : la tête du p-Sylow et le centre. Nous résumerons tout ceci dans un tableau à la fin.

Cas d'un unique p-Sylow isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.

Avec les mêmes notations, n'importe quel q-Sylow G_q fournit un complément de G_p ce qui prouve que G est un produit semi-direct interne

$$G_p \rtimes_\varphi G_q.$$

Les automorphismes de $\mathbb{Z}/p^2\mathbb{Z}$ forment systématiquement un groupe cyclique d'ordre $p(p-1)$. Les mêmes arguments que précédemment montrent que pour que le produit ne soit pas direct (ce qui fournirait un des groupes abéliens du cas d'un unique q-Sylow), il faut que $q \mid p-1$ auquel cas

$$G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes_{\varphi_\gamma} \mathbb{Z}/q\mathbb{Z}$$

où γ est un élément fixé une fois pour toutes d'ordre q dans $(\mathbb{Z}/p^2\mathbb{Z})^\times$ et où $\varphi_\gamma(k)$ est la multiplication par γ^k.

On se rappelle de plus que le complément dans un produit semi-direct est distingué si et seulement si le produit est direct. Ainsi G_q n'est pas distingué dans G pour ce nouveau groupe, ce qui le distingue des cas précédemment traités.

Cas d'un unique p-Sylow isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

Avec les mêmes notations, n'importe quel q-Sylow G_q fournit un complément de G_p ce qui prouve que G est un produit semi-direct interne

$$G_p \rtimes_\varphi G_q.$$

Les automorphismes de $(\mathbb{Z}/p\mathbb{Z})^2$ s'identifient à $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ qui est d'ordre $p(p-1)^2(p+1)$. Pour que le produit semi-direct soit non trivial, il faut qu'il existe une matrice d'ordre q, donc par Gauss que $q|p-1$ ou $q|p+1$.

Si $q|p-1$ le polynôme X^q-1 divise $X^{p-1}-1$ donc est scindé sur $\mathbb{Z}/p\mathbb{Z}$. Soit ζ un élément d'ordre q. La matrice d'ordre q définissant le produit-semi-direct est par conséquent diagonalisable et ses valeurs propres

sont des puissances de ζ, non toutes égales à 1. Puisque la conjugaison de φ par un élément de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ ne change pas la classe d'isomorphisme du produit semi-direct, nous pouvons supposer la matrice diagonale avec action non triviale sur le premier facteur. Quitte à choisir correctement son générateur de G_q, nous pouvons supposer que cette matrice est $\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)$ pour un certain $k \in [\![0, q-1]\!]$. Globalement, nous avons utilisé que pour deux matrices M et N qui déterminait deux produits semi-directs, si une puissance non triviale de M est sembable à N, les deux produits semi-directs sont isomorphes. En particulier les matrices pour k et k^{-1} fournissent le même produit-semi-direct. Nous obtenons donc

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes_{\left(\begin{smallmatrix}\zeta & 0\\ 0 & 1\end{smallmatrix}\right)^\bullet} \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \left(\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_\zeta} \mathbb{Z}/q\mathbb{Z}\right)$$

et

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes_{\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)^\bullet} \mathbb{Z}/q\mathbb{Z} \text{ pour } k \text{ variant dans un système de représentants de } {}^{(\mathbb{Z}/q\mathbb{Z})^\times}/_{k \sim k^{-1}}.$$

Le centre du premier groupe est non trivial ce qui le distingue des autres. Pour démontrer que les autres ne sont pas isomorphes, supposons que deux tels groupes associés à k et l sont isomorphes et on se donne ι un isomorphisme de celui associé à k vers celui associé à l. Le p-Sylow étant distingué, il est unique donc un isomorphisme envoie le p-Sylow du premier groupe sur celui du second et induit un automorphisme du p-Sylow que l'on note u. Les automorphismes intérieurs des deux groupes agissent sur le p-Sylow par les puissances de la matrice associée. Ainsi, via l'isomorphisme, nous identifions que $\langle\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)\rangle = u\langle\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^l\end{smallmatrix}\right)\rangle u^{-1}$. Les seules puissances de $\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)$ qui ont ζ comme valeur propre sont $\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)$ et $\left(\begin{smallmatrix}\zeta^{k^{-1}} & 0\\ 0 & \zeta\end{smallmatrix}\right)$ ce qui conclut que $l \in \{k, k^{-1}\}$.

Supposons à présent que $q \nmid p-1$ mais $q \mid p+1$. Le polynôme $X^q - 1$ divise $X^{p^2} - X$ qui est scindé dans $\mathbb{F}_{p^2}$. Prenons ζ une racine primitive q-ième de l'unité dans $\mathbb{F}_{p^2}$, qui engendre fatalement toutes lesdites racines. Au-dessus de l'unique extension de degré 2 de $\mathbb{F}_p$, la matrice est donc sembable à une matrice de la forme $\left(\begin{smallmatrix}\zeta^k & 0\\ 0 & \zeta^l\end{smallmatrix}\right)$ avec $l = -k$ puisque le polynôme caractéristique est à coefficients dans $\mathbb{F}_p$. Pour toutes ces matrices, l'un de ses puissances est sembable à $\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^{-1}\end{smallmatrix}\right)$ au-dessus de $\mathbb{F}_{p^2}$, donc au-dessus [2] de $\mathbb{F}_p$. Tous les produits semi-directs obtenus sont donc isomorphes à

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes_{M_\zeta^\bullet} \mathbb{Z}/q\mathbb{Z}$$

où M_ζ est la matrice compagnon dans la base canonique du polynôme minimal de ζ (qui est de degré 2). Aucun sous-groupe d'ordre p n'est distingué puisque la matrice n'est pas diagonalisable sur $\mathbb{F}_p$, ce qui distingue ce produit semi-direct des précédents.

On se rappelle de plus que le complément dans un produit semi-direct est distingué si et seulement si le produit est direct. Ainsi G_q n'est pas distingué dans G pour ces nouveaux groupes, ce qui les distingue du cas d'un unique q-Sylow.

2. L'un des meilleurs moyens de s'en convaincre reste le suivant. Pour tout corps K et tout K-espace vectoriel V, la décomposition de Frobenius, autrement dit les facteurs invariants de V comme $K[X]$-module où la multiplication par X est l'action de u, fournit un invariant de similitude parfait pour les endomorphismes u de V. A fortiori, puisque ces invariants ne dépendent pas de l'extension considérée, deux matrice sont sembables sur une extension L de K si et seulement si elles le sont sur K.

Groupe	Existe si p divise $q-1$	Existe si q divise $p-1$	Est-il abélien ?	Description d'un p-Sylow	A-t-il un q-Sylow distingué ?	Centre
$\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$	✓	✓	✓	$\mathbb{Z}/p^2\mathbb{Z}$	✓	Lui-même
$\mathbb{Z}/q\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^2$	✓	✓	✓	$(\mathbb{Z}/p\mathbb{Z})^2$	✓	Lui-même
$(\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\alpha} \mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/p\mathbb{Z}$	✓	×	×	$(\mathbb{Z}/p\mathbb{Z})^2$	✓	$\mathbb{Z}/p\mathbb{Z}$
$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\alpha} \mathbb{Z}/p^2\mathbb{Z}$	✓	×	×	$\mathbb{Z}/p^2\mathbb{Z}$	✓	$\mathbb{Z}/p\mathbb{Z}$
$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_\beta} \mathbb{Z}/p^2\mathbb{Z}$	✓	×	×	$\mathbb{Z}/p^2\mathbb{Z}$	✓	$\{0\}$
$\mathbb{Z}/p^2\mathbb{Z} \rtimes_{\varphi_\gamma} \mathbb{Z}/q\mathbb{Z}$	×	✓	×	$\mathbb{Z}/p^2\mathbb{Z}$	×	$\{0\}$
$\mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_\zeta} \mathbb{Z}/q\mathbb{Z})$	×	✓	×	$(\mathbb{Z}/p\mathbb{Z})^2$	×	$Z/p\mathbb{Z}$
$(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\left(\begin{smallmatrix}\zeta & 0\\ 0 & \zeta^k\end{smallmatrix}\right)^\bullet} \mathbb{Z}/q\mathbb{Z}$ pour k variant	×	✓	×	$(\mathbb{Z}/p\mathbb{Z})^2$	×	$\{0\}$
$(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{M_\xi^\bullet} \mathbb{Z}/q\mathbb{Z}$	?	×	×	$(\mathbb{Z}/p\mathbb{Z})^2$	×	$\{0\}$