TD4 : Produit semi-direct

Exercices $\star$: à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices $\star\star$: seront traités en classe en priorité.
Exercices $\star\star\star$: plus difficiles.

Exercice 1 : $\star$
Soient N et H des groupes et soit $\phi : H \to \mathrm{Aut}(N)$ un morphisme de groupes. Notons $N \underset{\phi}{\rtimes} H$ l'ensemble $N \times H$ muni de la loi de composition définie par $(n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2) = (n_1\phi(h_1)(n_2), h_1h_2)$.

a) Montrer que $N \underset{\phi}{\rtimes} H$ est un groupe, appelé *produit semi-direct* de H par N relativement à ϕ.

b) Montrer que $N \times \{e_H\} \lhd N \underset{\phi}{\rtimes} H$ et $\{e_N\} \times H < N \underset{\phi}{\rtimes} H$.

c) Identifier le quotient de $N \underset{\phi}{\rtimes} H$ par $N \times \{e_H\}$.

Solution de l'exercice 1.

a) Montrons d'abord que la loi est associative. Soient $n_1, n_2, n_3 \in N$ et $h_1, h_2, h_3 \in H$. Par définition du produit, on a

$$((n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2)) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1\phi(h_1)(n_2), h_1h_2) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1\phi(h_1)(n_2)\phi(h_1h_2)(n_3), h_1h_2h_3)\,.$$

De même, on a

$$(n_1, h_1) \underset{\phi}{\rtimes} ((n_2, h_2) \underset{\phi}{\rtimes} (n_3, h_3)) = (n_1, h_1) \underset{\phi}{\rtimes} (n_2\phi(h_2)(n_3), h_2h_3) = (n_1\phi(h_1)(n_2\phi(h_2)(n_3)), h_1h_2h_3)\,.$$

Or par définition de ϕ, $\phi(_1)$ est un morphisme de groupes, et ϕ est lui-même un morphisme, donc on a

$$\phi(h_1)(n_2\phi(h_2)(n_3)) = \phi(h_1)(n_2)(\phi(h_1) \circ \phi(h_2))(n_3) = \phi(h_1)(n_2)\phi(h_1h_2)(n_3)\,,$$

dont on déduit que

$$((n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2)) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1, h_1) \underset{\phi}{\rtimes} ((n_2, h_2) \underset{\phi}{\rtimes} (n_3, h_3))\,,$$

donc le produit $\underset{\phi}{\rtimes}$ est associatif.
On voit tout de suite que l'élément (e_N, e_H) est neutre pour la loi $\underset{\phi}{\rtimes}$.
Montrons que tout élément admet un inverse. Soit $n \in N$ et $h \in H$. Pour tous $n' \in N$, $h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (n', h') = (e_N, e_H)$$

si et seulement si

$$(n\phi(n')(h'), hh') = (e_N, e_H)\,,$$

si et seulement si $h' = h^{-1}$ et $n' = \phi(h^{-1})(n^{-1})$. Le calcul de $(n', h') \underset{\phi}{\rtimes} (n, h)$ est exactement similaire, ce qui assure que (n, h) est inversible et que son inverse est $(n, h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.
On a donc bien montré que $N \underset{\phi}{\rtimes} H$ est un groupe.

b) Les formules définissant le produit assurent que $N \times \{e_H\}$ et $\{e_N\} \times H$ sont bien des sous-groupes de $N \underset{\phi}{\rtimes} H$, car $\phi(h)(e_N) = e_N$ pour tout $h \in H$. Montrons que le premier est distingué : soit $n, n' \in N$ et $h' \in H$. On a alors

$$\begin{aligned}(n,h) \underset{\phi}{\rtimes} (n',e_H) \underset{\phi}{\rtimes} (n,h)^{-1} &= (n,h) \underset{\phi}{\rtimes} (n',e_H) \underset{\phi}{\rtimes} (\phi(h^{-1})(n^{-1}),h^{-1}) \\ &= (n\phi(h)(n'),h) \underset{\phi}{\rtimes} (\phi(h^{-1}(n^{-1}),h^{-1}) \\ &= (n\phi(h)(n')\phi(h)(\phi(h^{-1})(n^{-1})),e_H) \\ &= (n\phi(h)(n')n^{-1},e_H) \in N \times \{e_H\}\,.\end{aligned}$$

Cela montre bien que $N \times \{e_H\}$ est distingué.

On remarque en revanche qu'en général, $\{e_N\} \times H$ n'est pas distingué (faire le calcul).

c) On dispose d'une application naturelle $\pi : N \underset{\phi}{\rtimes} H \to H$ donné par la seconde projection, à savoir $\pi(n,h) := h$. Il est clair que π est surjective, et la définition de la loi de groupes assure que π est un morphisme de groupes. Calculons son noyau : soient $n \in N$ et $h \in H$. On a $\pi(n,h) = e_H$ si et seulement si $h = e_H$, donc $\mathrm{Ker}(\pi) = N \times \{e_H\}$. Finalement, l'application π passe au quotient par son noyau et induit un isomorphisme de groupes

$$\overline{\pi} : \left(N \underset{\phi}{\rtimes} H\right) / \left(N \underset{\phi}{\rtimes} \{e_H\}\right) \xrightarrow{\sim} H\,.$$

Exercice 2 : $\star$

Soit G un groupe et soient N et H des sous-groupes de G tels que $N \cap H = \{e\}$, $NH = G$ et $N \lhd G$. Montrer que :

a) l'application $i : H \to \mathrm{Aut}(N)$ définie par $h \mapsto i_h$, où $i_h(n) = hnh^{-1}$, est un morphisme de groupes.

b) l'application

$$\begin{aligned} f : N \underset{i}{\rtimes} H &\to G \\ (n,h) &\mapsto nh \end{aligned}$$

est un isomorphisme de groupes.

On dit alors que G est le *produit semi-direct* de H par N.

Solution de l'exercice 2.

a) C'est évident (i est bien définie car N est distingué dans G).

b) Montrons que f est un morphisme de groupes. Soient $n, n' \in N$ et $h, h' \in H$. On a

$$f(n,h)f(n',h') = nhn'h'$$

et

$$f((n,h) \underset{i}{\rtimes} (n',h')) = f(ni(h)(n'),hh') = f(nhn'h^{-1},hh') = nhn'h^{-1}hh' = nhn'h'\,,$$

ce qui assure que $f((n,h) \underset{i}{\rtimes} (n',h')) = f(n,h)f(n',h')$, donc f est bien un morphisme de groupes.

Montrons maintenant que f est un isomorphisme de groupes : l'hypothèse $NH = G$ assure que f est surjectif, et l'hypothèse $N \cap H = \{e\}$ assure que le noyau de f est trivial. Donc f est bien un isomorphisme.

Exercice 3 : $\star$

Montrer que le produit semi-direct $N \underset{\phi}{\rtimes} H$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_N\} \times H \lhd N \underset{\phi}{\rtimes} H$.

Solution de l'exercice 3. Le produit semi-direct $N \underset{\phi}{\rtimes} H$ est direct si et seulement si pour tous $n, n' \in N$ et $h, h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (n', h') = (n', hh')$$

si et seulement si pour tous $n, n' \in N$ et $h \in H$, $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in N$ et $h \in H$, $\phi(h)(n') = n'$ si et seulement si ϕ est le morphisme trivial.
Pour tout $n \in N$ et $h, h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (e_N, h') \underset{\phi}{\rtimes} (n, h)^{-1} = (n\phi(hh'h^{-1})(n^{-1}), hh'h^{-1}) .$$

On en déduit immédiatement que le morphisme ϕ est trivial si et seulement si $\{e_N\} \times H$ est distingué dans $N \underset{\phi}{\rtimes} H$.

Exercice 4 : $\star\star$
Une suite de morphismes $\ldots \to A \xrightarrow{u} B \xrightarrow{v} C \to \ldots$ est dit exacte en B si $\mathrm{Im}(u) = \mathrm{Ker}(v)$, et elle est dite *exacte* si elle est exacte en tous ses termes.
Soit

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

une suite exacte (courte). On dit alors que G est une *extension* de H par N.

a) Montrer que, si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.

b) Réciproquement soit une telle suite exacte. Si p possède une *section*, c'est-à-dire s'il existe un morphisme de groupes $s : H \to G$ tel que $p \circ s = \mathrm{id}_H$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.

c) Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Solution de l'exercice 4.

a) On suppose que $G = N \underset{\phi}{\rtimes} H$. On a vu dans l'exercice 1, question c), que l'on disposait d'un morphisme surjectif $\pi : G \to H$ dont le noyau est le sous-groupe $N \underset{\phi}{\rtimes} \{e_H\}$, qui est isomorphe à N. Donc on a bien une suite exacte

$$1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1 ,$$

où $i : N \to G$ est défini par $i(n) := (n, e_H)$.
On vérifie en outre que l'application $H \to G$ définie par $h \mapsto (e_N, h)$ est une section de π.

b) C'est une conséquence de l'exercice 2 appliqué aux sous-groupes $N' := i(N)$ et $H' := s(H)$ de G. Vérifons seulement que ces deux sous-groupes satisfont les hypothèses de l'exercice 2 : il est clair que N' est distingué dans G car $N' = \mathrm{Ker}(p)$. Soit $g \in G$, posons $h := s(\pi(g)) \in H'$. Alors on a

$$\pi(h) = \pi(s(\pi(g)) = \pi(g) ,$$

donc $n := gh^{-1} \in \mathrm{Ker}(\pi) = N'$, donc finalement on a bien $g = nh$, ce qui assure que $G = N'H'$.
Soit $g \in N' \cap H'$. Comme $g \in H'$, il existe $h \in H$ tel que $g = s(h)$. Comme $g \in N'$, $\pi(g) = e_H$. Donc $\pi(s(h)) = e_H$, i.e. $h = e_H$, donc $g = s(e_H) = e_G$. Donc $N' \cap H' = \{e_G\}$.
On peut donc bien appliquer l'exercice 2 pour conclure.

c) On peut par exemple considérer la suite exacte

$$1 \to \mathbb{Z}/2\mathbb{Z} \to Z/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \to 1$$

où p est la réduction modulo 2. C'est bien une suite exacte, en revanche p n'admet pas de section, puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2, alors que tous ses antécédents par p sont d'ordre 4. Donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Un autre exemple est donné par le groupe des quaternions $\mathbf{H}_8$ dont le centre Z est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $G/Z \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ce qui fournit une suite exacte

$$1 \to Z/2\mathbb{Z} \to \mathbf{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 1\,,$$

telle que p n'admet pas de section (on le voit en listant les éléments d'ordre 2 dans $\mathbf{H}_8$). Donc $\mathbf{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 5 : $\star\star$

a) Montrer que l'on peut écrire $\mathfrak{S}_n$ comme un produit semi-direct naturel.

b) Montrer que l'on peut écrire le groupe diédral D_n comme un produit semi-direct naturel.

c) Montrer que l'on peut écrire $\mathrm{GL}_n(k)$ comme un produit semi-direct naturel (k est un corps).

d) Ces produits semi-directs sont-ils directs ?

Solution de l'exercice 5.

a) On considère la suite exacte suivante

$$1 \to \mathfrak{A}_n \to \mathfrak{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1\,,$$

ce qui est une traduction du fait que la signature est un morphisme de groupes surjectif dans $\{\pm 1\}$ à noyau $\mathfrak{A}_n$.
La donnée d'une section du morphisme ε équivaut à la donnée d'une permutation $\sigma \in \mathfrak{S}_n$ d'ordre 2 et de signature -1. On peut prendre par exemple $\sigma = (12)$. L'exercice 4 assure alors que cette section induit un isomorphisme de groupes

$$\mathfrak{S}_n \cong \mathfrak{A}_n \underset{\phi}{\rtimes} \{\pm 1\}$$

où l'action de $\{\pm 1\}$ sur $\mathfrak{A}_n$ est donnée par la conjugaison par σ, i.e. $\phi(-1) : \tau \mapsto \sigma\tau\sigma^{-1}$.

b) On rappelle que le groupe diédral D_n est le groupe des isométries du plan préservant un polygone régulier à n côtés. Ce groupe est constitué de n isométries directes qui forment un sous-groupe, engendré par la rotation r de centre O et d'angle $\frac{2\pi}{n}$ (une fois qu'on a choisi pour origine O l'isobarycentre des sommets de polygone), et n isométries indirectes qui sont de la forme $r^k \circ s$, où $k \in \mathbb{Z}$ et s est une symétrie axiale (fixée) préservant le polygone. On dispose alors des sous-groupes $\langle r \rangle$ et $\langle s \rangle$ qui vérifient les hypothèses de l'exercice 2, ce qui assure que l'on a un isomorphisme $D_n \cong \langle r \rangle \underset{\phi}{\rtimes} \langle s \rangle$ où l'action ϕ est donnée par conjugaison dans D_n. Comme les groupes $\langle r \rangle$ et $\langle s \rangle$ sont cycliques d'ordre respectifs n et 2, on a donc un isomorphisme

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/2\mathbb{Z}\,,$$

où l'action ϕ est donnée par $\phi(-1) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $x \mapsto -x$.

c) On a une suite exacte naturelle

$$1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^* \to 1\,,$$

et on dispose d'une section $s : k^* \to \mathrm{GL}_n(k)$ du morphisme déterminant donnée par exemple par $s(\lambda) := \mathrm{diag}(\lambda, 1, \ldots, 1)$. Alors l'exercice 4 assure que cela fournit un isomorphisme

$$\mathrm{GL}_n(k) \cong \mathrm{SL}_n(k) \underset{\phi}{\rtimes} k^*\,.$$

d) On voit facilement que dans les cas a) et b), les produits ne sont pas directs (sauf pour $n = 2$), quelle que soit la section choisie. Et mieux, on vérifie facilement qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

En revanche, le cas c) est moins évident pour $n \geq 2$. Si $x \mapsto x^n$ est un automorphisme de k^*, notons $a : k^\times \to k^\times$ son inverse. Alors l'application

$$\begin{aligned} \alpha : \mathrm{SL}_n(k) \times k^* &\simeq \mathrm{GL}_n(k) \\ (A, t) &\mapsto A.\mathrm{diag}(a(t), \ldots, a(t)) \end{aligned}$$

est un isomorphisme.

Réciproquement, supposons qu'il existe un isomorphisme de groupes

$$\begin{aligned} \alpha : \mathrm{SL}_n(k) \times k^* &\simeq \mathrm{GL}_n(k) \\ (A, t) &\mapsto \phi(A)s(t)\,. \end{aligned}$$

Le sous-groupe dérivé de $\mathrm{SL}_n(k) \times k^*$ est $\mathrm{SL}_n(k) \times \{1\}$ et celui de $\mathrm{GL}_n(k)$ est aussi $\mathrm{SL}_n(k)$ [1]. On en déduit que ϕ est un automorphisme de $\mathrm{SL}_n(k)$.

En outre, $\alpha(k^*) = s(k^*)$ commute avec tout élément de $\mathrm{GL}_n(k)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}_n(k)$ est formé des homothéties). On a donc que l'application $t \mapsto s(t)$ est un morphisme injectif de la forme $t \mapsto \mathrm{diag}(a(t), \ldots, a(t))$ de k^* vers $\mathrm{GL}_n(k)$.

Puisque le noyau de det est $\mathrm{SL}_n(k)$, on en déduit que $a(t)^n = 1$ si, et seulement si, $a(t) = 1$. Puisque $t \mapsto a(t)$ est injectif, on déduit que $t \mapsto a(t)^n$ est injectif. Or det est surjectif sur k^*, donc $t \mapsto a(t)^n = a(t^n)$ est bijectif, et donc $x \mapsto x^n$ est bijectif et donc un automorphisme de k^*.

Finalement, $\mathrm{GL}_n(k)$ est isomorphe au produit direct de $\mathrm{SL}_n(k)$ par k^* si et seulement si le morphisme $(.)^n : k^* \to k^*$ est un automorphisme. C'est le cas par exemple si $k = \mathbb{R}$ et n est impair, ou si k est un corps fini (ou plus généralement un corps dit parfait) de caractéristique p avec n égal à une puissance de p.

Exercice 6 :
Soit $G = N \rtimes H$ et soit K un sous-groupe de G contenant N. Montrer que l'on a $K = N \rtimes (K \cap H)$.

Solution de l'exercice 6. C'est immédiat en applicant par exemple l'exercice 2 :

a) On a $N \lhd G$ et $N < K$, donc $N \lhd K$.

b) On a $H < G$ et $K < G$, donc $H \cap K < K$.

c) On a $N \cap H = \{e\}$, donc $N \cap (K \cap H) = \{e\}$.

d) On a $NH = G$, donc si $k \in K$, alors $k = nh$ avec $n \in N$ et $h \in H$. Puisque $N \subset K$, on en déduit que $h \in H \cap K$. D'où $N(H \cap K) = K$.

Exercice 7 :
Montrer que tout groupe d'ordre 255 est cyclique.

Solution de l'exercice 7. Soit G un groupe d'ordre $255 = 3 \cdot 5 \cdot 17$. D'après les théorèmes de Sylow, le nombre n_3 de 3-Sylow vaut 1 ou 85, le nombre n_5 de 5-Sylow vaut 1 ou 51 et on n'a qu'un seul 17-Sylow. On ne peut pas avoir $n_3 = 85$ et $n_5 = 51$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ (l'autre cas se résoud de la même façon). Notons S_3 le seul 3-Sylow, S_{17} le seul 17-Sylow et S_5 un 5-Sylow quelconque. On a :

a) $S_3 S_{17} \simeq S_3 \times S_{17} \lhd G$.

b) $S_3 S_{17} \cap S_5 = \{e\}$.

c) $S_3 S_{17} S_5 = G$

1. Sauf dans le cas $n = 2$ et $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On peut faire l'exercice à la main dans ces deux cas (si $k = \mathbb{Z}/2\mathbb{Z}$, on a un produit direct et si $k = \mathbb{Z}/3\mathbb{Z}$ ce n'est pas un produit direct).

On déduit de l'exercice 2 que $G = S_3S_{17} \rtimes S_5$. Soit $\phi : S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, donc ϕ est trivial et le produit semi-direct est direct. On conclut par le lemme chinois.

Exercice 8 : ⋆⋆
Soient H et N des groupes et soient ϕ et $\psi : H \to \mathrm{Aut}(N)$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $N \rtimes_\phi H$ et $N \rtimes_\psi H$ soient isomorphes.

a) S'il existe un automorphisme α de H tel que $\psi = \phi \circ \alpha$, montrer que l'on a la conclusion attendue.

b) S'il existe un automorphisme u de N tel que

$$\forall h \in H \qquad \phi(h) = u\psi(h)u^{-1},$$

montrer que la conclusion attendue vaut encore.

c) Si H est cyclique et que ϕ et $\psi : H \to \mathrm{Aut}(N)$ sont tels que $\phi(H) = \psi(H)$, montrer que $N \rtimes_\phi H$ et $N \rtimes_\psi H$ sont isomorphes.

Solution de l'exercice 8.

a) Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (n, \alpha(h)) \end{array}$ est un isomorphisme.

b) Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (u(n), h) \end{array}$ est l'isomorphisme recherché.

c) H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\mathrm{Im}\,(\phi) = \mathrm{Im}\,(\psi)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ est surjective, il existe $d' \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui s'envoie vers d.
La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait aux conditions de a), d'où le résultat.

Exercice 9 : ⋆⋆
Soient $p < q$ des nombres premiers.

a) Déterminer à isomorphisme près tous les groupes de cardinal pq.

b) Si $q \geq 3$, en déduire que tout groupe de cardinal $2q$ est isomorphe à $\mathbb{Z}/2q\mathbb{Z}$ ou au groupe diédral D_q.

Solution de l'exercice 9.

a) Soit G un groupe de cardinal pq. Le théorème de Sylow assure que G admet un unique q-Sylow N qui est donc distingué dans G. Par cardinalité, on a $N \cong \mathbb{Z}/q\mathbb{Z}$. On sait aussi que G admet un p-Sylow $H \cong \mathbb{Z}/p\mathbb{Z}$. Alors $N \cap H = \{e\}$, et $NH = G$ par cardinalité. Donc G est un produit semi-direct de G par H. Donc

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}\,.$$

Ce produit semi-direct est défini via un morphisme $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ (voir TD3, exercice 7). On a alors deux cas :
— Si p ne divise pas $q-1$, alors le morphisme ϕ est trivial, donc G est isomorphe au produit direct $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. Il y a donc une unique classe d'isomorphisme de groupes d'ordre pq, à savoir celle de $\mathbb{Z}/pq\mathbb{Z}$.
— Si p divise $q-1$, alors il existe un morphisme non trivial $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ et tout tel morphisme est injectif. Alors la question c) de l'exercice 8 assure que si ϕ et ϕ' sont deux tels morphismes non triviaux, alors les produits semi-directs $\mathbb{Z}/q\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \underset{\phi'}{\rtimes} \mathbb{Z}/p\mathbb{Z}$ sont isomorphes. Il existe donc exactement deux classes d'isomorphisme de groupes de cardinal pq, à savoir $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ (produit semi-direct non trivial).

b) C'est le cas particulier de la question précédente avec $p = 2$. Comme $q - 1$ est pair, on est dans le second cas : il existe exactement deux classes d'isomorphisme de groupes d'ordre $2q$, qui sont $\mathbb{Z}/2q\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Or on a vu à l'exercice 5, question b), que ce dernier groupe est isomorphe à D_q (c'est l'unique groupe non abélien d'ordre $2q$).

Exercice 10 : $\star\star\star$

a) Montrer qu'un groupe d'ordre 8 est isomorphe à l'un des groupes suivants :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ \mathbf{H}_8.$$

Justifier que $\mathbf{H}_8$ n'est pas un produit semi-direct et que les cinq groupes cités sont deux-à-deux non isomorphes.

b) Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ possède un unique 2-Sylow que l'on identifiera.

c) Donner la liste des classes d'isomorphisme de groupes finis de cardinal ≤ 15.

Solution de l'exercice 10.

a) Soit G un groupe d'ordre 8.

i) Si G possède un élément d'ordre 8, alors G est cyclique, isomorphe $\mathbb{Z}/8\mathbb{Z}$.

ii) Si G est d'exposant 2, alors G est abélien et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

iii) Si G est d'exposant 4 et est abélien, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

iv) On suppose maintenant G d'exposant 4 et non abélien. Il existe $r \in G$ d'ordre 4. Alors $R\langle r\rangle$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Soit $s \in G \setminus \langle r\rangle$ d'ordre minimal.

i. Si s est d'ordre 2, alors le sous-groupe engendré $S = \langle s\rangle$ intersecte R trivialement, et G est engendré par R et S (puisque ces derniers contiennent au moins 5 éléments). De plus, R est distingué car d'indice 2, et G est donc isomorphe au produit semi-direct $R \rtimes S \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_4$.

ii. Si s est d'ordre 4, renommons r et s respectivement par i et j. Reste à établir la table de G et voir qu'elle coïncide avec celle de $\mathbf{H}_8$: pour cela, on note $k := ij \in G$. Comme $j \notin R$ et j est d'ordre 4, on voit que $k \notin R \cup S$. Donc k est d'ordre 4 également. Si $R \cap S = \{1\}$, alors $k^3 \in R \cup S$, donc $k \in R \cup S$, ce qui est contradictoire. Donc $R \cap S$ est d'ordre 2, engendré par $i^2 = j^2$. Cela assure que $i^2 = j^2$ est central dans G. Comme G est de cardinal 8 et comme les éléments $1, i, j, i^2 = j^2, i^3, j^3, k, k^3$ sont deux-à-deux distincts, l'élément k^2 qui est d'ordre 2, est nécessairement égal à $i^2 = j^2$. On a donc i, j, k d'ordre 4, avec $k = ij$ et $i^2 = j^2 = k^2$ central. Calculons ji : comme $ji \notin R \cup S$, on a $ji = k$ ou $ji = k^3$. Or G n'est pas commutatif, donc $ji = k^3 = i^2(ij)$. Finalement, on a bien montré que la table de multiplication de G est celle du groupe des quaternions, donc $G \cong \mathbf{H}_8$.

On a donc bien montré qu'il y avait exactement cinq groupes d'ordre 8 à isomorphisme près.

Supposons maintenant que $\mathbf{H}_8 = N \rtimes H$ soit un produit semi-direct non trivial. Alors l'un des sous-groupes N ou H est d'ordre 2, donc est exactement $\{\pm 1\}$ (-1 est l'unique élément d'ordre 2 dans $\mathbf{H}_8$). Si c'était H, H serait distingué car -1 est central, et le produit semi-direct serait direct. Comme tout groupe d'ordre 4 est abélien, $\mathbf{H}_8$ serait abélien, ce qui n'est pas le cas. On peut donc supposer $N = \{\pm 1\}$. Mais alors $\mathrm{Aut}(N)$ est réduit à un élément et tout morphisme $H \to \mathrm{Aut}(N)$ est trivial. Le produit semi-direct serait encore direct et $\mathbf{H}_8$ à nouveau abélien. C'est donc que l'hypothèse initiale est fausse, donc $\mathbf{H}_8$ n'est pas un produit semi-direct non trivial.

b) En passant en revue les éléments de $\mathrm{SL}_2(\mathbb{F}_3)$, il y en a uniquement 8 d'ordre une puissance de 2. Ce sont :

— ordre 1 : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

— ordre 2 : $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$;
— ordre 4 : $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$.

Il y a donc un unique 2-Sylow dans $\mathrm{SL}_2(\mathbb{F}_3)$, et il est clairement isomorphe à $\mathbf{H}_8$.

c) On a déjà classifié les groupes d'ordre ≤ 7 dans l'exercice 8 de la feuille de TD1. Les groupes d'ordre 8 sont classifiés à la question a). Les groupes d'ordre 9, 11 et 13 sont abéliens. Les groupes d'ordre 10, 13, 14 et 15 sont classifiés à l'exercice 9. Il reste donc à traiter les groupes d'ordre $12 = 2^2.3$. Soit G un groupe d'ordre 12. Les théorèmes de Sylow assure que G admet un ou quatre 3-Sylow :
— Dans le premier cas, G admet donc un sous-groupe distingué N isomorphe à $\mathbb{Z}/3\mathbb{Z}$, tel que $H = G/N$ soit un groupe d'ordre 4. Alors par cardinalité, G est produit semi-direct de H par $N \cong \mathbb{Z}/3\mathbb{Z}$. Un tel produit est défini par un morphisme $\phi : H \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Si H est cyclique d'ordre 4, il existe un unique tel morphisme ϕ non trivial, qui définit le produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, en plus du produit direct $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Sinon, $H \cong (\mathbb{Z}/2\mathbb{Z})^2$, et il y a exactement trois morphismes ϕ non triviaux dont on constate qu'ils diffèrent deux-à-deux d'un automorphisme de H, et donc l'exercice 8, question a), assure que les produits semi-directs associés sont isomorphes ; par conséquent, dans ce cas, on a un unique produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$ en plus du produit direct $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
— Dans le second cas, G admet $4.2 = 8$ éléments d'ordre 3, ce qui assure que le complémentaire de l'ensemble de ces éléments est l'unique 2-Sylow N de G. Alors G est produit semi-direct de $\mathbb{Z}/3\mathbb{Z}$ par N. Un tel produit est donné par un un morphisme de groupes $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(N)$. Si N est cyclique, alors $\mathrm{Aut}(N)$ est d'ordre 2 et ϕ est trivial. Si $N \cong (\mathbb{Z}/2\mathbb{Z})^2$, alors $\mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$, donc il existe un morphisme non trivial $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(N)$, et deux tels morphismes définissent des produits semi-directs isomorphes par l'exercice 8, question c). Donc finalement, donc ce cas, G est soit $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, soit $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$, soit $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$.

On a donc la liste suivante des classes d'isomorphisme de groupes d'ordre 12 (il est facile de vérifier que ces groupes ne sont pas deux-à-deux isomorphes) :

$$\mathbb{Z}/12\mathbb{Z}\,,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\,,\ \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}\,,\ \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2 \cong D_6\,,\ (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \cong \mathfrak{A}_4\,.$$

Finalement, on a la classification complète des groupes d'ordre ≤ 15 :
— ordre 1 : le groupe trivial $\{1\}$.
— ordre 2 : le groupe cyclique d'ordre 2, à savoir $\mathbb{Z}/2\mathbb{Z}$.
— ordre 3 : le groupe cyclique d'ordre 3, à savoir $\mathbb{Z}/3\mathbb{Z}$.
— ordre 4 : les groupes abéliens d'ordre 4, à savoir $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.
— ordre 5 : le groupe cyclique d'ordre 5, à savoir $\mathbb{Z}/5\mathbb{Z}$.
— ordre 6 : le groupe cyclique d'ordre 6, i.e. $\mathbb{Z}/6\mathbb{Z}$, et le groupe symétrique $\mathfrak{S}_3$.
— ordre 7 : le groupe cyclique d'ordre 7, i.e. $\mathbb{Z}/7\mathbb{Z}$.
— ordre 8 : les groupes abéliens d'ordre 8, i.e $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$, le groupe diédral D_4 et le groupe des quaternions $\mathbf{H}_8$.
— ordre 9 : les groupes abéliens d'ordre 9, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$.
— ordre 10 : le groupe cyclique d'ordre 10, i.e. $\mathbb{Z}/10\mathbb{Z}$ et le groupe diédral D_5.
— ordre 11 : le groupe cyclique d'ordre 11, à savoir $\mathbb{Z}/11\mathbb{Z}$.
— ordre 12 : les groupes abéliens d'ordre 12, i.e. $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, le groupe alterné $\mathfrak{A}_4 \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$, le groupe diédral D_6 et le groupe $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.
— ordre 13 : le groupe cyclique d'ordre 13, à savoir $\mathbb{Z}/13\mathbb{Z}$.
— ordre 14 : le groupe cyclique d'ordre 14, i.e $\mathbb{Z}/14\mathbb{Z}$, et le groupe diédral D_7.
— ordre 15 : le groupe cyclique d'ordre 15, à savoir $\mathbb{Z}/15\mathbb{Z}$.

Exercice 11 : $\star\star\star$

Soit p un nombre premier impair.

a) Déterminer les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

b) Soient ϕ et ψ des morphismes non triviaux de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. En notant pour tout entier k, ϕ_k le morphisme défini par $\phi_k(x) = \phi(kx)$, montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ tels que $\psi = P\phi_k P^{-1}$.

c) En déduire qu'il existe, à isomorphisme près, un unique produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

d) Montrer que le centre de ce dernier groupe est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

e) Soit G un groupe d'ordre p^3 non cyclique, contenant un élément x d'ordre p^2. Monter que $\langle x\rangle$ est distingué dans G et que G est un produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\langle x\rangle \cong \mathbb{Z}/p^2\mathbb{Z}$.

f) Décrire les classes d'isomorphisme de groupes de cardinal p^3 : on raisonnera par exemple suivant l'ordre maximal d'un élément du groupe.

Solution de l'exercice 11.

a) Les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Soit $\mathcal{S}$ l'ensemble des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$. Comme le sous-groupe $U := \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} : * \in \mathbb{F}_p \right\}$ des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, en faisant agir $\mathrm{GL}_2(\mathbb{F}_p)$ sur $\mathcal{S}$ par conjugaison, on voit que $\mathcal{S}$ est isomorphe à $\mathrm{GL}_2(\mathbb{F}_p)/\mathrm{Stab}(U) = \mathrm{GL}_2(\mathbb{F}_p)/B$, où $B := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\}$ désigne le sous-groupe de Borel standard de $\mathrm{GL}_2(\mathbb{F}_p)$. Cela donne directement la liste qui suit dans a') :

a') Une variante : les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe U des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ et que tous sont conjugués, on voit qu'une matrice de $\mathrm{GL}_2(\mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre (à la main) p^2 telles matrices et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). On remarque que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

b) Comme les images de ψ et φ sont des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, elles sont conjuguées par une matrice $P \in \mathrm{GL}_2(\mathbb{F}_p)$. Notons $\begin{array}{rccc} \varphi^{(P)} : & \mathbb{Z}/p\mathbb{Z} & \to & \psi(\mathbb{Z}/p\mathbb{Z}) \\ & x & \mapsto & P\varphi(x)P^{-1} \end{array}$; c'est un isomorphisme. Dès lors, $(\varphi^{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, donc de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

c) Comme on a $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{F}_p)$, la question a) nous donne l'existence d'un tel produit semi-direct non trivial. L'unicité résulte de b) et de l'exercice 8.

d) Comme le centre d'un p-groupe est non trivial, le centre de $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$, ne peut être que d'ordre p, p^2 ou p^3. Mais s'il était d'ordre p^2 ou p^3, l'exercice 9 du TD1 nous dirait que $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$ est abélien. Ce n'est pas le cas puisque le produit semi-direct est non trivial, et donc le centre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

e) Le sous-groupe $\langle x\rangle$ est d'indice p dans un groupe d'ordre p^3, donc on a vu à l'exercice 5, question a), du TD2, que $\langle x\rangle$ est distingué dans G. En outre, le quotient $G/\langle x\rangle$ est d'ordre p, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Soit alors $y \in G \setminus \langle x\rangle$. Alors $y^p \in \langle x\rangle$ et $y^{p^2} = e$, donc il existe $k \in \mathbb{Z}$ tel que $y^p = x^{pk}$. Comme $\langle x\rangle$ est distingué, il existe un entier $r \geq 0$ tel que $y^{-1}xy = x^r$. On voit alors facilement que pour tous $\alpha \in \mathbb{N}$, on a $x^\alpha y = yx^{\alpha r}$. On cherche à trouver $z \in G \setminus \langle x\rangle$ d'ordre p. On cherche z sous la forme $z = yx^n$. Alors $z^p = (yx^n)^p = yx^nyx^n \dots yx^n$, et une récurrence simple assure que

$$z^p = y^p x^{n(r^{p-1}+\cdots+r+1)} = x^{pk+n(r^{p-1}+\cdots+r+1)}\,.$$

Donc z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + \cdots + r + 1) \equiv 0\ [p^2]\,. \tag{1}$$

On cherche donc à résoudre l'équation (1) d'inconnue $n \in \mathbb{Z}$. Notons $S := r^{p-1} + \cdots + r + 1$. Alors on a $(r-1)S \equiv r - 1\ [p]$, donc soit $r \not\equiv 1\ [p]$ et $S \equiv 1\ [p]$, soit $r \equiv 1\ [p]$ et on vérifie

que dans ce cas $S \equiv p\ [p^2]$ (remarquons que l'hypothèse p impair est utilisée ici). Donc dans les deux cas, cela assure que l'équation (1) admet toujours une solution $n_0 \in \mathbb{Z}$. Au vu de la discussion précédente, on sait donc que $z_0 := yx^{n_0} \in G \setminus \langle x \rangle$ est d'ordre p. Par conséquent, les deux sous-groupe $N := \langle x \rangle$ et $H := \langle z \rangle$ vérifient les hypothèses de l'exercice 2, ce qui asssure que G est produit semi-direct de $H \cong \mathbb{Z}/p\mathbb{Z}$ par $N \cong \mathbb{Z}/p^2\mathbb{Z}$.

f) Soit G un groupe d'ordre p^3. On note p^r l'ordre maximal d'un élément de G.
   — Si $r = 3$, G est cyclique et $G \cong \mathbb{Z}/p^3\mathbb{Z}$.
   — Si $r = 2$, alors la question e) assure que $G \cong \mathbb{Z}/p^2\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$. Ce produit semi-direct est défini par un morphisme $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/p(p-1)\mathbb{Z}$. Comme le groupe $\mathbb{Z}/p(p-1)\mathbb{Z}$ admet un unique sous-groupe d'ordre p, l'exercice 8, question c), assure qu'il existe un unique produit semi-direct non trivial $\mathbb{Z}/p^2\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$.
   — Si $r = 1$, alors tout sous-groupe de G d'ordre p^2 est distingué et isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ (on rappelle qu'un tel sous-groupe existe effectivement), et tout élément du complémentaire de ce sous-groupe est d'ordre p, ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $(\mathbb{Z}/p\mathbb{Z})^2$. Par conséquent, la question c) assure que $G \cong (\mathbb{Z}/p\mathbb{Z})^3$ ou G est isomorphe à l'unique produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

   Finalement, on aboutit à la conclusion qu'il y a exactement cinq classes d'isomorphisme de groupes d'ordre p^3, à savoir

$$\mathbb{Z}/p^3\mathbb{Z}\,,\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}\,,\ (\mathbb{Z}/p\mathbb{Z})^3\,,\ (\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}\,,\ (\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}\,.$$

   On remarquera que contrairement au cas $p = 2$ (voir exercice 10, question c)), tous les groupes d'ordre p^3 sont des produits semi-directs de groupes abéliens.

   Le lecteur curieux pourra essayer de réaliser les deux classes d'isomorphisme non abéliennes comme des groupes de matrices sur $\mathbb{F}_p$.

Exercice 12 : $\star\star\star$

Soient $p \neq q$ deux nombres premiers. Classifier les groupes d'ordre p^2q.

Solution de l'exercice 12. Soit G un groupe d'ordre p^2q. On note n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G. Les théorèmes de Sylow assurent que $n_p = 1$ ou q et $n_q = 1, p$ ou p^2.
Supposons que $n_q = p^2$. Cela implique que $q|p^2 - 1$. Alors G possède exactement $p^2(q-1) = p^2q - p^2$ éléments d'ordre r. Donc le complémentaire de l'ensemble de ces éléments est l'unique p-Sylow de G. Donc on a $n_p = 1$.
Supposons $n_q = p$. Il est clair qu'alors $n_p = q$ est impossible. Donc $n_p = 1$.
Finalement, on donc dans l'un des cas suivants :
— $q|p^2 - 1$, $n_p = 1$ et $n_q = p^2$. Dans ce cas, G est produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par son p-Sylow, lequel est soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$.
— $q|p - 1$, $n_p = 1$ et $n_q = p$. Dans ce cas, G est produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par son p-Sylow, lequel est soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$.
— $p|q - 1$, $n_p = q$ et $n_q = 1$. Dans ce cas, G est produit semi-direct non trivial de soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$, par son q-Sylow $\mathbb{Z}/q\mathbb{Z}$.
— $n_p = n_q = 1$. Dans ce cas, G est abélien, isomorphe à $\mathbb{Z}/p^2q\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$.

On est donc amené à classifier les produits semi-directs d'un groupe d'ordre p^2 par un groupe d'ordre q, et d'un groupe d'ordre q par un groupe d'ordre p^2. On obtient que :

a) Il existe un produit semi-direct non trivial $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ si et seulement si $q|p - 1$ (car $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ est cyclique d'ordre $p(p-1)$), et dans ce cas, il existe une unique classe d'isomorphisme de tels groupes, grâce à l'exercice 8, question c).

b) Il existe un produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ si et seulement si $q|p^2-1$ (on rappelle que $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{F}_p)$). Dénombrons maintenant, sous cette hypothèse, le nombre de classes d'isomorphisme de tels groupes. On voit facilement que deux produits semi-directs de cette forme, définis par deux morphismes non triviaux $\phi, \psi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{GL}_2(\mathbb{F}_p)$, sont isomorphes si et seulement si $\phi(\mathbb{Z}/q\mathbb{Z})$ et $\psi(\mathbb{Z}/q\mathbb{Z})$ sont des sous-groupes conjugués de $\mathrm{GL}_2(\mathbb{F}_p)$. On voit

facilement que deux matrices non scalaires de $\mathrm{GL}_2(\mathbb{F}_p)$ sont conjuguées si et seulement si elles ont les mêmes valeurs propres (c'est valable sur un corps quelconque). Or deux matrices d'ordre q dans $\mathrm{GL}_2(\mathbb{F}_p)$ ont pour valeurs propres des racines q-ièmes de l'unité. Si les deux valeurs propres sont 1, la matrice est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ qui est d'ordre p, ce qui est contradictoire. On est alors amené à distinguer les cas suivants :

i) $q = 2$. La discussion précédente assure qu'il y a exactement deux classes de conjugaison de matrices d'ordre 2, à savoir $-I_2$ et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On en déduit donc deux classes d'isomorphisme de produits semi-directs non triviaux $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

ii) $q|p-1$ et $q \not| p+1$. Comme $q|p-1$, $\mathbb{F}_p^*$ contient exactement q racines q-ièmes de l'unité. Soit $\zeta \in \mathbb{F}_p^*$ une telle racine primitive. Alors on voit que tout sous-groupe d'ordre q de $\mathrm{GL}_2(\mathbb{F}_p)$ est engendré par une matrice dont les valeurs propres sont ζ et ζ^r avec $0 \leq r < q$. Deux tels sous-groupes (caractérisé par des entiers r et r' comme précédemment) sont conjugués si et seulement s'il existe $1 \leq s < q$ tel que $(1, r) = (s, r's)$ ou $(1, r) = (r's, s)$, si et seulement si $r = r'$ ou ($r \neq 0$ et $r' = r^{-1}$ mod. q). Donc dans ce cas, le nombre de produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ non triviaux non isomorphes est de $\frac{q+3}{2}$.

iii) $q \not| p-1$ et $q|p+1$. Alors $\mathbb{F}_p^*$ ne contient aucun élément d'ordre q. Donc toute matrice d'ordre q est de déterminant 1, donc les valeurs propres d'une telle matrice sont des racines primitives q-ièmes de l'unité $\neq 1$ inverses l'une de l'autre. Par conséquent, si A et B sont deux matrices quelconques d'ordre q, B est conjuguée à une puissance de A première à q (et vice-versa). Cela assure que le produit semi-direct non-trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ est unique (à isomorphisme près) dans ce cas.

c) Il existe un produit semi-direct non trivial $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ si et seulement si $p|q-1$ (car $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $q-1$), et dans ce cas, l'exercice 8, question c), assure qu'il existe une unique classe d'isomorphisme de tels groupes si p divise exactement $q-1$, et deux telles classes si $p^2|q-1$.

d) Il existe un produit semi-direct non trivial $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$ si et seulement si $p|q-1$ (car $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $q-1$). Or dans ce cas, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet un unique sous-groupe d'ordre p, et deux morphismes non triviaux de $(\mathbb{Z}/p\mathbb{Z})^2$ vers ce sous-groupe diffèrent par un automorphisme de $(\mathbb{Z}/p\mathbb{Z})^2$, ce qui assure que tous les produits semi-directs non triviaux $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$ sont isomorphes.

Finalement, on obtient la classification suivante :

a) Si $p \not| q-1$ et $q \not| p^2-1$. Deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$.

b) Si $p|q-1$, $p^2 \not| q-1$ et $q \not| p^2-1$. Quatre groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

c) Si $p^2|q-1$ et $q \not| p^2-1$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; deux produits semi-directs $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

d) Si $q|p-1$ et $q \neq 2$. $\frac{q+9}{2}$ groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$; $\frac{q+3}{2}$ produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

e) Si $q|p+1$ et $q \neq 2$ et $p \neq 2$. Trois groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

f) $q = 2$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$; deux produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

g) $p = 2$ et $q = 3$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$; un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$.