MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

Fiche 5: Produits semi-directs

1. (*a*) Soient K un corps et E un K-espace vectoriel. Soient F un sous-espace vectoriel de E et $p : E \to E/F$ la projection canonique. Montrer que pour tout supplémentaire S de F, la restriction $p|_S : S \to E/F$ est un isomorphisme.

(*b*) Soit G un groupe et H un sous-groupe distingué de G. Soit $p : G \to G/H$ la projection canonique. Peut-on toujours trouver un sous-groupe K de G tel que la restriction $p|_K : K \to G/H$ soit un isomorphisme ?

(*c*) Soit G un groupe, H et K deux sous-groupes de G avec H distingué dans G. Soit $p : G \to G/H$ la projection canonique. Montrer que la restriction $p|_K : K \to G/H$ est un isomorphisme si et seulement si $G = H \rtimes K$.

Solution.

(*a*) Soit S un sous-espace vectoriel de E tel que $F \oplus S = E$, *i.e.* $E \cap S = \{\mathbf{0}_E\}$ et $F + S = E$. On considère l'application $q : E \to S$ qui associe s à $f + s \in E$, où $f \in F$ et $s \in S$. C'est clair que q est une application linéaire surjective. Soit aussi $\iota : E/F \to E$ une application linéaire telle que $p \circ \iota = \mathrm{id}_{E/F}$. L'existe de ι est immédiate, car il suffit de choisir une base $\bar{\mathscr{B}}$ de E/F et pour chaque $\bar{v} \in \bar{\mathscr{B}}$ on choisit $v \in \bar{v} \subseteq E$. L'application $\iota : E/F \to E$ est la seule application linéaire telle que $\iota(\bar{v}) = v$ pour tout $\bar{v} \in \bar{\mathscr{B}}$. C'est clair que $q \circ \iota : S \to E/F$ est l'application réciproque de $p|_S : S \to E/F$. En conséquence, $p|_S : S \to E/F$ est un isomorphisme.

(*b*) Ce n'est pas toujours possible de trouver un sous-groupe K de G tel que la restriction $p|_K : K \to G/H$ soit un isomorphisme. Par exemple, soit $G = \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions. On sait que tout sous-groupe de G est distingué (voir exercice **5**). En plus, si $H \subseteq G$ est un sous-groupe non trivial, $\{\pm 1\} \subseteq H$. Cela nous dit que, étant donné H et K deux sous-groupes (distingués) non triviaux de G, alors -1 appartient au noyau de la restriction $p|_K : K \to G/H$ et en particulier le morphisme précédent n'est pas un isomorphisme.

(*c*) On rappelle que, étant donné deux sous-groupes H et K d'un groupe G, on dit que G est le **produit semi-direct (interne)** de H et K si H est une sous-groupe distingué de G et l'application $m : H \times K \to G$ qui associe hk à $(h, k) \in H \times K$ est bijective. On écrit dans ce cas $G = H \rtimes K$. Noter que le fait que H soit une sous-groupe distingué de G nous dit que l'image de m est un sous-groupe de G, car $hkh'k' = h(kh'k^{-1})kk' = m(h(kh'k^{-1}), kk')$ et $(hk)^{-1} = m(k^{-1}h^{-1}k, k^{-1})$, vu que $kh'k^{-1}, k^{-1}h^{-1}k \in H$ pour $h, h' \in H$ et $k, k' \in K$. En outre, l'injectivité de m est équivalente à $K \cap H = \{1_G\}$. On note en plus que si G est fini et $|G| = |H|.|K|$, alors l'application m est injective si et seulement si elle est surjective.

On note que, si $G = H \rtimes K$, alors H et K commutent si et seulement si K est un sous-groupe distingué. On dit dans ce cas que G est un **produit direct (interne)** de H et K et on écrit $G = H \times K$. En effet, si H et K commutent, on voit immédiatement que K est distingué. Réciproquement, si K est distingué, alors $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{1_G\}$ pour tous $h \in H$ et $k \in K$, car $hkh^{-1} \in K$ et $kh^{-1}k^{-1} \in H$, ce qui nous dit que H et K commutent.

Comme le noyau du morphisme de groupes $p|_K : K \to G/H$ est $K \cap H$, il est injectif si et seulement si $K \cap H = \{1_G\}$, *i.e.* l'application $m : H \times K \to G$ est injective. En

outre, comme l'image de $p|_K : K \to G/H$ est $\mathsf{Img}(m)/H$, il est surjectif si et seulement si $\mathsf{Img}(m) = G$, *i.e.* l'application $m : H \times K \to G$ est surjective En conséquence, la restriction $p|_K : K \to G/H$ est un isomorphisme si et seulement si $G = H \rtimes K$

2. Soit $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Pour tout $k \in \mathbb{Z}$, on note $\bar{k}$ et $\hat{k}$ les classes de k dans $\mathbb{Z}/4\mathbb{Z}$ et dans $\mathbb{Z}/2\mathbb{Z}$, respectivement.

(*a*) Soit $H_1 = \langle(\bar{2}, \hat{1})\rangle$. Existe-t-il un sous-groupe K de G tel que $G = H_1 \rtimes K$?

(*b*) Soit $H_2 = \langle(\bar{2}, \hat{0})\rangle$. Existe-t-il un sous-groupe K de G tel que $G = H_2 \rtimes K$?

Solution. L'existence de K tel que $G = H_i \rtimes K$ pour $i \in \{1, 2\}$ est équivalente à l'existence d'un sous-groupe K de G d'ordre 4 tel que $H_i \cap K = \{(\bar{0}, \hat{0})\}$. En effet, dans ce cas $m : H_i \times K \to G$ est aussi surjective, vu qu'elle est injective et les ensembles de départe et d'arrivé ont la même cardinalité finie.

(*a*) C'est clair que le sous-groupe $K = \mathbb{Z}/4\mathbb{Z} \times \{\hat{0}\}$ a cardinalité 4 et que $H_1 \cap K = \{(\bar{0}, \hat{0})\}$, vu que $H_1 = \{(\bar{0}, \hat{0}), (\bar{2}, \hat{1})\}$.

(*b*) Noter que $H_2 = \{(\bar{0}, \hat{0}), (\bar{2}, \hat{0})\}$. Soit K un sous-groupe de G tel que $G \cap H_2 = \{(\bar{0}, \hat{0})\}$. On remarque d'abord que, si $(\bar{x}, \hat{1}) \in K$, alors $\bar{x} \in \{\bar{0}, \bar{2}\}$. En effet, si $\bar{x} = 1$ ou $\bar{x} = 3$, alors $(\bar{2}, \hat{0}) = (\bar{x}, \hat{1}) + (\bar{x}, \hat{1}) \in K$, ce qui es absurde. En outre, si $(\bar{x}, \hat{1}) \in K + H_2$, alors alors $\bar{x} \in \{\bar{0}, \bar{2}\}$, car dans ce cas $(\bar{x}, \hat{1}) = (\bar{y}, \hat{1}) + (\bar{z}, \hat{0})$ avec $(\bar{y}, \hat{1}) \in K$ et $(\bar{z}, \hat{0}) \in H_2$, ce qui implique $\bar{y}, \bar{z} \in \{\bar{0}, \bar{2}\}$. En conséquence, $\bar{x} \in \{\bar{0}, \bar{2}\}$ et en particulier $(\bar{1}, \hat{1}) \in G \setminus (K + H_2)$, ce qui est absurde.

3. (*a*) Montrer que les groupes $\mathbb{A}_4$ et $\mathbb{S}_4$ sont des produits semi-directs non triviaux.

(*b*) Qu'en est-il pour le groupe $\mathbb{S}_n$ avec $n \geq 5$?

(*c*) Qu'en est-il pour le groupe $\mathbb{A}_n$ avec $n \geq 5$?

Solution.

(*a*) On rappelle que $K = \{\mathsf{id}_{[\![1,4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq \mathbb{A}_4$ est un sous-groupe distingué. On considère le sous-groupe $H = \{\mathsf{id}_{[\![1,4]\!]}, (1\ 2\ 3), (1\ 3\ 2)\} \subseteq \mathbb{A}_4$. Alors, c'est clair que $H \cap K = \{\mathsf{id}_{[\![1,4]\!]}\}$, ce qui implique que $\mathbb{A}_4 = K \rtimes H$ vu que $|\mathbb{A}_4| = |K||H|$. On fera le cas du groupe $\mathbb{S}_n$ pour $n \geq 4$ dans l'item suivant.

(*b*) On considère les sous-groupes $\mathbb{A}_n$ et $H = \{\mathsf{id}_{[\![1,n]\!]}, (1\ 2)\}$. Alors, c'est clair que $\mathbb{A}_n$ est distingué, $\mathbb{A}_n \cap H = \{\mathsf{id}_{[\![1,n]\!]}\}$ et que $|\mathbb{S}_n| = |\mathbb{A}_n||H|$, ce qui nous dit que $\mathbb{S}_n = \mathbb{A}_n \rtimes H$.

(*c*) Le groupe $\mathbb{A}_n$ est simple pour $n \geq 5$, donc il ne possède pas des sous-groupes distingués non triviaux. Cela nous dit que $\mathbb{A}_n$ ne peut pas être exprimé comme une produit semi-directs non trivial.

4. (*a*) Donner un exemple de produit semi-direct $\mathbb{R} \rtimes_\rho \mathbb{R}$ avec $\rho : \mathbb{R} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{R})$ non trivial.

(*b*) Pour $n, p \in \mathbb{N}^*$ avec p premier, à quelle condition peut-on définir un produit semi-direct $(\mathbb{Z}/p\mathbb{Z}) \rtimes_\rho (\mathbb{Z}/n\mathbb{Z})$ avec $\rho : \mathbb{Z}/n\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p\mathbb{Z})$ non trivial ?

Solution.

(*a*) On rappelle que, étant donné deux groupes Het K et un morphisme de groupes $\rho : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$, **produit semi-direct (externe)** de H et K est l'ensemble $H \times K$ muni du produit $(h,k)\cdot(h',k') = (h\rho(k)(h'), kk')$ pour $h,h' \in H$ et $k,k' \in K$. C'est clair qu'il s'agit d'un groupe, que sera noté $H \rtimes_\rho K$. Le produit semi-direct est trivial (ou, simplement, direct) si et seulement ρ est le morphisme trivial, *i.e.* $\rho(k)(h) = h$ pour tous $h \in H$ et $k \in K$. C'est facile à voir que le sous-groupe $\{1_H\} \times K \subseteq H \rtimes_\rho K$ est distingué si et seulement si ρ est trivial, *i.e.* $H \rtimes_\rho K$ est trivial si et seulement si $\{1_H\} \times K$ est distingué.

Soit $\rho : \mathbb{R} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{R})$ l'application donnée par $\rho(x)(y) = \alpha^x y$ pour $x, y \in \mathbb{R}$, où $\alpha \in \mathbb{R}_{>0}$ est fixe. On voit bien que

$$\rho(x)(0) = 0, \qquad \rho(x)(y+y') = \alpha^x(y+y') = \alpha^x y + \alpha^x y' = \rho(x)(y) + \rho(x)(y')$$

et $\rho(x) : \mathbb{R} \to \mathbb{R}$ est bijectif (car $\rho(-x) = \rho(x)^{-1}$) pour tous $x, y, y' \in \mathbb{R}$, ce qui implique l'application précédente est bien définie. En plus, comme $\rho(x+x')(y) = \alpha^{x+x'}y = \alpha^x\alpha^{x'}y = (\rho(x)\circ\rho(x'))(y)$ pour tous $x, x', y \in \mathbb{R}$, ρ est un morphisme de groupes. C'est clair que $\mathbb{R} \rtimes_\rho \mathbb{R}$ est un produit semi-direct non direct.

(*b*) On rappelle que, d'après l'exercice **19** de la fiche 2, pour $n \in \mathbb{N}^*$, l'application d'évaluation $\mathsf{ev}_{\bar{1}} : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, G) \to G$ en $\bar{1}$ est une injection avec image donnée par l'ensemble $\{g \in G : g^n = 1_G\}$. En conséquence, si $n, m \in \mathbb{N}^*$, $\mathsf{ev}_{\bar{1}} : \mathsf{Hom}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z}$ induit une bijection avec son image, $\{\bar{x} \in \mathbb{Z}/m\mathbb{Z} : n\bar{x} = \bar{0}\}$, ce qui nous dit qu'il existe un morphisme de groupes non trivial de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $\mathsf{PGCD}(n,m) \neq 1$. En outre, dans le même exercice on a montré que l'application $\mathsf{ev}_{\bar{1}}$ induit une bijection $\mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$. En conséquence, pour $p \in \mathbb{N}^*$ premier, il existe un morphisme de groupes non trivial $\mathbb{Z}/n\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ si et seulement si $\mathsf{PGCD}(n, p-1) > 1$. Si n est premier, il existe un morphisme de groupes non trivial $\mathbb{Z}/n\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ si et seulement si n divise $p-1$.

5. On considère les matrices suivantes

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } M_3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

de $\mathsf{M}_2(\mathbb{C})$. On indique ci-dessous les produits non triviaux suivants, où l'élément de la rangée indexée par $M \in \mathsf{M}_2(\mathbb{C})$ et la colonne indexée par $N \in \mathsf{M}_2(\mathbb{C})$ est $M \times N$:

$\times$	M_1	M_2	M_3
M_1	$-M_0$	M_3	$-M_2$
M_2	$-M_3$	$-M_0$	M_1
M_3	M_2	$-M_1$	$-M_0$

(*a*) En déduire que l'ensemble $Q = \{\pm M_0, \pm M_1, \pm M_2, \pm M_3\}$ est un sous-groupe non abélien de $\mathsf{GL}_2(\mathbb{C})$.

(*b*) Montrer que tous les sous-groupes de Q sont distingués dans Q.

(*c*) Peut-on écrire Q comme produit semi-direct interne de deux sous-groupes non triviaux ?

Solution.

(*a*) Il s'agit d'une conséquence directe de la définition de Q.

(*b*) Il s'agit d'une conséquence directe de la définition de Q.

(*c*) On a expliqué que ce n'est pas possible dans l'exercice **1**, (b).

6. On fixe un entier $n \geq 3$. Dans $\mathbb{R}^2$, on considère l'ensemble $P_n = \{A_0, \ldots, A_{n-1}\}$, où pour tout $k \in \mathbb{Z}$, A_k est le point d'affixe $e^{2i\pi k/n}$ pour $k \in \mathbb{Z}$. On note D_n le sous-groupe de $\mathsf{O}(\mathbb{R}^2)$ des isométries de $\mathbb{R}^2$ qui laissent l'ensemble P_n globalement invariant.

(*a*) En utilisant l'action naturelle du groupe D_n sur l'ensemble P_n, montrer que D_n est fini et $|\mathsf{D}_n| = 2n$.

(*b*) On note $H = \mathsf{D}_n \cap \mathsf{SO}(\mathbb{R}^2)$. Montrer que $|\mathsf{D}_n| = 2|H|$.

(*c*) Soient $s \in \mathsf{D}_n \setminus \mathsf{SO}(\mathbb{R}^2)$ et $K = \langle s \rangle$. Montrer que $\mathsf{D}_n = H \rtimes K$.

(*d*) Montrer que pour toute rotation r on a $srs^{-1} = r^{-1}$.

(*e*) En déduire que le produit $\mathsf{D}_n = H \rtimes K$ n'est pas direct.

(*f*) Dans le cas où $n = 6$, le groupe D_6 contient $-\mathsf{id}_{\mathbb{R}^2}$ et une rotation r d'ordre 3. Montrer que $\mathsf{D}_6 = H_1 \rtimes K_1$, où $H_1 = \langle r \rangle$, $K_1 = \langle -\mathsf{id}_{\mathbb{R}^2}, s \rangle$ et $s \in \mathsf{O}(\mathbb{R}^2) \setminus \mathsf{SO}(\mathbb{R}^2)$.

Solution.

(*a*) On considère l'application

$$\mathsf{ev} : \mathsf{D}_n \to P_n^2$$

qui associe $(\rho(A_0), \rho(A_1))$ à $\rho \in \mathsf{D}_n$. Comme $\{A_0, A_1\}$ est un base de l'espace vectoriel $\mathbb{R}^2$, l'application précédente est injective, ce qui implique que D_n est fini. En outre, comme les arguments de ev sont des isométries, un calcul élémentaire nous dit que

$$\mathsf{Img}(\mathsf{ev}) \subseteq \big\{(A_i, A_j) : i, j \in [\![0, n-1]\!], |j-i| = 1 \text{ ou } |j-i| = n-1\big\}. \tag{1}$$

En plus, en employant que

$$\mathsf{O}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}$$

et les valeurs particulières données par $a = \cos(2k\pi/n)$ et $b = \sin(2k\pi/n)$ pour $k \in [\![0, n-1]\!]$, c'est facile à voir que l'inclusion dans (1) est une égalité. Cela nous dit que $|\mathsf{D}_n| = 2n$.

(*b*) On voit bien que l'image directe de H sous ev est précisément

$$\big\{(A_i, A_j) : i, j \in [\![0, n-1]\!], j - i = 1 \text{ ou } i - j = n-1\big\}, \tag{2}$$

en employant que

$$\mathsf{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1 \right\}$$

et les valeurs particulières données par $a = \cos(2k\pi/n)$ et $b = \sin(2k\pi/n)$ pour $k \in [\![0, n-1]\!]$. En conséquence, $|H| = n$ et $|\mathsf{D}_n| = 2|H|$.

(*c*) Noter que $[\mathsf{D}_n : H] = 2$, ce qui implique que H est un sous-groupe distingué. En outre, on remarque que si $s \in \mathsf{O}(\mathbb{R}^2) \setminus \mathsf{SO}(\mathbb{R}^2)$, alors

$$s = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

avec $a, b \in \mathbb{R}$ et $a^2 + b^2 = 1$, ce qui dit en particulier que $s^2 = \mathsf{I}_2$ est la matrice unité. Alors, $K = \langle s \rangle = \{\mathsf{I}_2, s\}$, ce qui nous dit que $H \cap K = \{\mathsf{I}_2\}$. Comme $|H|.|K| = |\mathsf{D}_n|$, on conclut que $\mathsf{D}_n = H \rtimes K$.

(*d*) Un calcul direct nous dit que

$$\underbrace{\begin{pmatrix} a & b \\ b & -a \end{pmatrix}}_{s}\underbrace{\begin{pmatrix} c & -d \\ d & -c \end{pmatrix}}_{r}\underbrace{\begin{pmatrix} a & b \\ b & -a \end{pmatrix}}_{s^{-1}} = \underbrace{\begin{pmatrix} c & d \\ -d & c \end{pmatrix}}_{r^{-1}}$$

pour tous $a, b, c, d \in \mathbb{R}$ et $a^2 + b^2 = c^2 + d^2 = 1$. Noter que $s \in \mathsf{O}(\mathbb{R}^2) \setminus \mathsf{SO}(\mathbb{R}^2)$ et $r \in \mathsf{SO}(\mathbb{R}^2)$ sont des éléments génériques.

(*e*) Comme H et K ne commutent pas, le produit $\mathsf{D}_n = H \rtimes K$ n'est pas direct.

(*f*) Noter que $-\mathsf{id}_{\mathbb{R}^2} \in \mathsf{SO}(\mathbb{R}^2)$ envoie A_i à A_j pour $i, j \in [\![0, n-1]\!]$ et $|j - i| = 3$, ce qui nous dit que $-\mathsf{id}_{\mathbb{R}^2} \in \mathsf{D}_6$. Soit

$$r = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \in \mathsf{SO}(\mathbb{R}^2).$$

et $s \in \mathsf{O}(\mathbb{R}^2) \setminus \mathsf{SO}(\mathbb{R}^2)$. En plus, $K_1 = \langle -\mathsf{id}_{\mathbb{R}^2}, s \rangle = \{\pm \mathsf{id}_{\mathbb{R}^2}, \pm s\}$ a ordre 4. Par ailleurs, $H_1 = \langle r \rangle = \{\mathsf{id}_{\mathbb{R}^2}, r, r^2\}$ a ordre 3 et H_1 est un sous-groupe distingué de D_n d'après l'item (d). Finalement, c'est facile à vérifier que $H_1 \cap K_1 = \{\mathsf{id}_{\mathbb{R}^2}\}$, ce qui implique $\mathsf{D}_6 = H_1 \rtimes K_1$, vu que $|\mathsf{D}_6| = 12 = |H_1|.|K_1|$.

7. Soient H et K deux groupes et φ un morphisme de groupes de K dans $\mathsf{Aut}_{\mathsf{Gr}}(H)$. Montrer que le produit semi-direct $H \rtimes_\varphi K$ est abélien si et seulement si H et K sont abéliens et φ est trivial.

Solution. C'est clair que si $H \rtimes_\varphi K$ est abélien, alors H et K sont abéliens, car H et K sont isomorphes aux sous-groupes de $H \rtimes_\varphi K$ de la forme $\{(h, 1_K) : h \in H\}$ et $\{(1_H, k) : k \in K\}$, respectivement, et tout sous-groupe d'un groupe abélien est abélien. En outre, comme $H \rtimes_\varphi K$ est abélien, $(h, k) = (h, 1_K)(1_H, k) = (1_H, k)(h, 1_K) = (\varphi(k)(h), k)$ pour tous $h \in H$ et $k \in K$, ce qui implique $\varphi(k)(h) = h$ pour tous $h \in H$ et $k \in K$, *i.e.* φ est trivial. Réciproquement, si H et K sont abélien et φ est trivial, on a que $\varphi(k)(h) = h$ pour tous $h \in H$ et $k \in K$. En plus,

$$\begin{aligned}(h, k)(h', k') &= \big(h\varphi(k)(h'), kk'\big) = (hh', kk') = (h'h, k'k) \\ &= \big(h'\varphi(k')(h'), k'k\big) = (h', k')(h, k),\end{aligned}$$

pour tous $h, h' \in H$ et $k, k' \in K$, ce qui implique que $H \rtimes_\varphi K$ est abélien.

8. Soit E un K-espace vectoriel. On appelle T le groupe de translations de E, c'est-à-dire des applications de E dans E de la forme $\tau_c : x \mapsto x + c$ avec $c \in E$. On définit le groupe affine par

$$\mathsf{GA}(E) = \big\{f \in \mathsf{Aut}_{\mathsf{Ens}}(E) : \text{ il existe } g \in \mathsf{GL}(E) \text{ et } t \in \mathsf{T} \text{ tels que } f = t \circ g\big\}.$$

Pour $v \in E$, on pose $K_v = \{f \in \mathsf{GA}(E) : f(v) = v\}$.

(a) Montrer que $\mathsf{GA}(E)$ est un groupe et $GL(E)$ et T des sous-groupes de $\mathsf{GA}(E)$.

(b) Montrer que $\mathsf{GA}(E) = \mathsf{T} \rtimes K_v$ pour tout $v \in E$. Ce produit est-il direct ?

Solution.

(a) On rappelle qu'une application $A : E \to E$ est dite **affine** s'il existe une application linéaire $L \in \mathsf{L}(E,E)$ et $c \in E$ tels que $A(v) = L(v) + c$ pour tout $v \in E$. On écrira dans ce cas $A = \mathsf{Aff}(c,L)$ et $\mathsf{Aff}(E) = \{\mathsf{Aff}(c,L) : c \in E, L \in \mathsf{L}(E,E)\}$. Noter que $A = \mathsf{Aff}(c,L)$ est bijectif si et seulement si $L \in \mathsf{GL}(E)$, ce qui nous dit que $\mathsf{GA}(E) = \{\mathsf{Aff}(c,L) : c \in E, L \in \mathsf{GL}(E)\} \subseteq \mathsf{Aff}(E)$. C'est clair que

$$\mathsf{Aff}(c,L) \circ \mathsf{Aff}(c',L')(v) = L(L'(v) + c') + c = \mathsf{Aff}(c + L(c'), LL')(v), \tag{3}$$

pour tout $v, c, c' \in E$ et $L, L' \in \mathsf{L}(E,E)$. L'identité (3) implique que la composition d'éléments de $\mathsf{GA}(E)$ est dans $\mathsf{GA}(E)$ et que $\mathsf{id}_E = \mathsf{Aff}(\mathbf{0}_E, \mathsf{id}_E)$ est le neutre de $\mathsf{GA}(E)$. En outre, (3) nous dit aussi que

$$\mathsf{Aff}(c,L)^{-1} = \mathsf{Aff}(-L^{-1}(c), L^{-1}) \tag{4}$$

pour tout $v, c \in E$ et $L \in \mathsf{GL}(E)$. En conséquence, $\mathsf{GA}(E)$ est un groupe pour la composition. En outre, (3) et (4) nous disent que $\mathsf{T} = \{\mathsf{Aff}(c, \mathsf{id}_E) : c \in E\}$ et $\mathsf{GL}(E) = \{\mathsf{Aff}(\mathbf{0}_E, L) : L \in \mathsf{GL}(E)\}$ sont des sous-groupes de $\mathsf{GA}(E)$. Noter que $K_{\mathbf{0}_E} = \mathsf{GL}(E)$. Pour le démontrer, il suffit de prouver que $K_{\mathbf{0}_E} \subseteq \mathsf{GL}(E)$, vu que l'autre inclusion est directe. Soit $f = \mathsf{Aff}(c,L) \in K_{\mathbf{0}_E}$. On voit bien que

$$\mathbf{0}_E = f(\mathbf{0}_E) = \mathsf{Aff}(c,L)(\mathbf{0}_E) = c + L(\mathbf{0}_E) = c + \mathbf{0}_E = c,$$

ce qui implique que $f = \mathsf{Aff}(\mathbf{0}_E, L) \in \mathsf{GL}(E)$. De façon plus générale, on note aussi que $K_v = \mathsf{Aff}(v, \mathsf{id}_E)\,\mathsf{GL}(E)\,\mathsf{Aff}(-v, \mathsf{id}_E)$ pour tout $v \in E$, car $f \in K_v$ si et seulement si $\mathsf{Aff}(-v, \mathsf{id}_E) \circ f \circ \mathsf{Aff}(v, \mathsf{id}_E) \in K_{\mathbf{0}_E} = \mathsf{GL}(E)$.

(b) On voit bien que l'application

$$m : \mathsf{T} \times \mathsf{GL}(E) \to \mathsf{GA}(E)$$

qui associe $F \circ L$ à (F, L) est surjective. En effet,

$$\mathsf{Aff}(c, \mathsf{id}_E)\,\mathsf{Aff}(\mathbf{0}_E, L) = \mathsf{Aff}(c, L),$$

pour tous $v \in E$ et $L \in \mathsf{GL}(E)$. En outre, $\mathsf{T} \cap \mathsf{GL}(E) = \{\mathsf{id}_E\}$, vu que $\mathsf{Aff}(c, \mathsf{id}_E) \in \mathsf{GL}(E)$ implique que $c = \mathsf{Aff}(c, \mathsf{id}_E)(\mathbf{0}_E) = \mathbf{0}_E$, *i.e.* $\mathsf{Aff}(c, \mathsf{id}_E) = \mathsf{id}_E$. En conséquence, $\mathsf{GA}(E) = \mathsf{T} \rtimes \mathsf{GL}(E)$.

Par ailleurs, on affirme que si $K \rtimes H = G$ est un produit semi-direct (interne), alors on a aussi le produit semi-direct (interne) $K \rtimes gHg^{-1} = G$ pour tout $g \in G$. Pour cela il suffit de montrer que l'application $K \times gHg^{-1} \to G$ qui associe $kghg^{-1}$ à $(k, ghg^{-1}) \in K \times gHg^{-1}$ est bijective. Or, $kghg^{-1} = k'gh'g^{-1}$ équivaut à $g^{-1}kgh = g^{-1}k'gh'$, ce qui implique que $g^{-1}kg = g^{-1}k'g$ et $h = h'$, vu que $K \rtimes H = G$ est un produit semi-direct (interne), ce qui nous dit que $k = k'$ et $h = h'$, *i.e.* l'application $K \times gHg^{-1} \to G$ est injective. Soit $x \in G$. Comme $K \rtimes H = G$ est un produit semi-direct (interne), il existe $k \in K$ et $h \in H$ tels que $g^{-1}xg = kh$, ce qui nous dit que $x = gkg^{-1}ghg^{-1}$, *i.e.* x est l'image de (gkg^{-1}, ghg^{-1}) sous l'application $K \times gHg^{-1} \to G$. En conséquence, on a le produit semi-direct (interne) $K \rtimes gHg^{-1} = G$. si l'on applique ce résultat au produit semi-direct (interne) $\mathsf{GA}(E) = \mathsf{T} \rtimes \mathsf{GL}(E)$ pour $g = \mathsf{Aff}(v, \mathsf{id}_E)$, on obtient le produit semi-direct (interne) $\mathsf{GA}(E) = \mathsf{T} \rtimes K_v$ pour tout $v \in E$.

Finalement, comme le sous-groupe $\mathsf{GL}(E)$ n'est pas distingué si $\dim(E) > 0$, on a de même pour $K_v = \mathsf{Aff}(v, \mathsf{id}_E)\,\mathsf{GL}(E)\,\mathsf{Aff}(-v, \mathsf{id}_E)$ pour tout $v \in E$, ce qui nous dit que le produit semi-direct interne ne peut pas être direct.

9. Montrer qu'un groupe abélien fini est le produit direct de ses sous-groupes de Sylow.

Solution. Soient G un groupe fini abélien d'ordre $p_1^{r_1}\dots p_n^{r_n}$, avec $p_1,\dots,p_n \in \mathbb{N}^*$ premiers et $r_1,\dots,r_n \in \mathbb{N}^*$, et $P_1,\dots,P_n$ les sous-groupes de Sylow de G, où $|P_i| = p_i^{r_i}$ pour $i \in [\![1,n]\!]$. On remarque que, comme G est abélien, il existe un unique p_i-groupe de Sylow pour chaque $i \in [\![1,n]\!]$. On considère l'application

$$m : \prod_{i=1}^{n} P_i \to G$$

qui associe $x_1\dots x_n$ à $(x_1,\dots,x_n) \in P_1 \times \cdots \times P_n$. Comme G est abélien, m est un morphisme de groupes. En plus, m est injectif. En effet, soit $(x_1,\dots,x_n) \in \mathsf{Ker}(m)$, *i.e.* $x_1\dots x_n = 1_G$. On affirme que $x_i = 1_G$ pour tout $i \in [\![1,n]\!]$. Or, $x_1\dots x_n = 1_G$ nous dit que $x_i = x_1^{-1}\dots x_{i-1}^{-1}x_{i+1}^{-1}\dots x_n^{-1} \in P_i$, pour tout $i \in\in [\![1,n]\!]$. En plus, x_i est dans le sous-groupe $Q_i = m(\prod_{j\in[\![1,n]\!]\setminus\{i\}} P_j) \subseteq G$, dont l'ordre est un diviseur de $|G|/p_i^{r_i} = \prod_{j\in[\![1,n]\!]\setminus\{i\}} p_j^{r_j}$. Comme l'ordre de $P_i \cap Q_i$ divise $p_i^{r_i}$ et $\prod_{j\in[\![1,n]\!]\setminus\{i\}} p_j^{r_j}$, $|P_i \cap Q_i| = 1$, ce qui implique que $P_i \cap Q_i = \{1_G\}$. En conséquence, $x_i = 1_G$, pour tout $i \in [\![1,n]\!]$. Comme m est un morphisme de groupes injectif, les ensembles de départ et d'arrivé ont le même cardinal fini, il est un isomorphisme de groupes. En conséquence, G est le produit direct de ses sous-groupes de Sylow.

10. Quels sont les sous-groupes de Sylow de $\mathbb{A}_4$? de $\mathbb{S}_4$?

Solution. On rappelle que $|\mathbb{A}_4| = 12 = 2^2 3$. On sait que

$$K = \left\{ \mathsf{id}_{[\![1,4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \right\} \subseteq \mathbb{A}_4$$

est un sous-groupe d'ordre $4 = 2^2$. En conséquence, K est un sous-groupe de Sylow pour $p = 2$. En plus, comme K est distingué, il est le seul sous-groupe de Sylow pour $p = 2$. En outre, on affirme que tout sous-groupe d'ordre 3 de $\mathbb{A}_4$ est de la forme $\langle\sigma\rangle$, avec $\sigma \in \mathbb{A}_4$ un 3-cycle. En effet, c'est clair que $\langle\sigma\rangle$, avec $\sigma \in \mathbb{A}_4$ un 3-cycle, est un sous-groupe d'ordre 3. Réciproquement, si H est sous-groupe d'ordre 3 de $\mathbb{A}_4$, il est cyclique, *i.e.* $H = \langle\sigma\rangle$ pour une permutation $\sigma \in \mathbb{A}_4$ d'ordre 3, et en regardant la décomposition du générateur σ de H en produit de cycles disjoints on conclut que σ est un 3-cycle. En conséquence, la famille de sous-groupes de Sylow de $\mathbb{A}_4$ pour $p = 3$ est $\mathscr{P}_3 = \{\langle(i\ j\ k)\rangle : i,j,k \in [\![1,4]\!] \text{ différents}\}$. La lectrice minutieuse/le lecteur minutieux pourra vérifier que cette famille comporte précisément 4 sous-groupes de Sylow, car $\mathscr{P}_3 = \{\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle\}$.

On rappelle que $|\mathbb{S}_4| = 24 = 2^3 3$. La description précédente des sous-groupes de Sylow de $\mathbb{A}_4$ pour $p = 3$ est aussi valable pour $\mathbb{S}_4$. En conséquence, la famille de sous-groupes de Sylow de $\mathbb{S}_4$ pour $p = 3$ est $\{\langle(i\ j\ k)\rangle : i,j,k \in [\![1,4]\!] \text{ différents}\}$. On rappelle que cette famille comporte précisément 4 sous-groupes de Sylow. En outre, on considère le sous-groupe H de $\mathbb{S}_4$ engendré par K et $(1\ 2)$, *i.e.*

$$H = \left\{ \mathsf{id}_{[\![1,4]\!]}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3) \right\}.$$

C'est clair que H est un sous-groupe d'ordre $8 = 2^3$ et en particulier un sous-groupe de Sylow de $\mathbb{S}_4$ pour $p = 2$. Comme tous les sous-groupes de Sylow pour un même nombre premier p sont conjugués, on conclut que la famille de sous-groupes de Sylow de $\mathbb{S}_4$ pour $p = 2$ est $\mathscr{P}_2 = \{\langle K, (i\ j)\rangle : i,j \in [\![1,4]\!] \text{ différents}\}$, vu que K est le sous-groupe de Sylow pour $p = 2$ de $\mathbb{A}_4$. C'est facile à vérifier que $\mathscr{P}_2$ comporte précisément 3 sous-groupes de Sylow, car $\mathscr{P}_2 = \{\langle K, (1\ 2)\rangle, \langle K, (1\ 3)\rangle, \langle K, (1\ 4)\rangle\}$.

11. Soit G un groupe d'ordre 63.

(*a*) Montrer que G contient un unique sous-groupe d'ordre 7, qu'on notera H, et qu'il admet un sous-groupe K d'ordre 9.

(*b*) Montrer que G est produit semi-direct interne de H et K.

(*c*) Montrer que ce produit interne est direct si et seulement si K est l'unique sous-groupe d'ordre 9 dans G.

(*d*) Lorsque ce produit interne n'est pas direct, combien y a-t-il de sous-groupes d'ordre 9 dans G ?

(*e*) Construire un morphisme de groupe non trivial θ de $\mathbb{Z}/9\mathbb{Z}$ vers $\mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/7\mathbb{Z})$ et en déduire un groupe d'ordre 63 ayant exactement 7 sous-groupes d'ordre 9.

Solution.

(*a*) On rappelle que pour un groupe fini G, si $p \in \mathbb{N}^*$ est un premier tel que $|G| = p^r m$ avec $\mathsf{PGCD}(p,m) = 1$, alors $N_p = \#(\{P \subseteq G : P \text{ Sylow sous-groupe pour } p\})$ satisfait que $N_p \equiv 1 \pmod p$ et $N_p | m$. En particulier, $N_7 \equiv 1 \pmod 7$, $N_3 \equiv 1 \pmod 3$, $N_7 | 9$ et $N_3 | 7$, vu que $|G| = 3^2 7$. Les deux dernières conditions disent que $N_7 \in \{1,3,9\}$ et $N_3 \in \{1,7\}$. En plus, la première condition nous dit alors que $N_7 = 1$. En conséquence, le groupe G d'ordre 63 possède un unique sous-groupe de Sylow pour 7, que l'on notera H.

(*b*) Comme tous les sous-groupes de Sylow pour un premier fixe p qui divise l'ordre de G sont conjugués, on conclut que dans ce cas l'unique sous-groupe de Sylow H de G est distingué. En outre, on voit bien que $H \cap K = \{1_G\}$, vu qu'il s'agit d'un groupe d'ordre divisant 7 et 9. Comme l'application $m : H \times K \to G$ qui associe hk à (h,k) est injective, et les ensembles de départ et d'arrivée ont la même cardinalité, elle est bijective. En conséquence, $G = H \rtimes K$.

(*c*) Comme on a expliqué dans l'exercice **1** le produit interne $H \rtimes K$ est direct si et seulement si K est distingué. Comme tous les sous-groupes de Sylow pour un premier fixe p qui divise l'ordre de G sont conjugués, K est distingué si et seulement si $N_3 = 1$.

(*d*) Si $N_3 \neq 1$, alors $N_3 = 7$, d'après le premier item.

(*e*) Comme on a montré dans l'exercice **4**, item (b), il existe un morphisme de groupes non trivial $\theta : \mathbb{Z}/9\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/7\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}$, vu que $\mathsf{PGCD}(6,9) = 3 > 1$. Or, on rappelle que dans un produit semi-direct (externe) $H \rtimes_\varphi K$, le sous-groupe $\{1_H\} \times K$ de $H \rtimes_\varphi K$ est distingué si et seulement si le morphisme de groupes $\varphi : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$ est trivial. En conséquence, le groupe $(\mathbb{Z}/7\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/9\mathbb{Z})$ a ordre 63 et comme θ n'est pas trivial, le sous-groupe $\{\bar{0}\} \times \mathbb{Z}/9\mathbb{Z} \subseteq (\mathbb{Z}/7\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/9\mathbb{Z})$ n'est pas distingué, ce qui implique que $N_3 \neq 1$. D'après l'item précédent, il existe alors 7 sous-groupes d'ordre 9 dans $(\mathbb{Z}/7\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/9\mathbb{Z})$.

12. Soient H et K deux groupes, et $\varphi, \psi : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$ deux morphismes de groupes.

(*a*) On suppose qu'il existe un automorphisme $\alpha \in \mathsf{Aut}_{\mathsf{Gr}}(K)$ tel que $\varphi = \psi \circ \alpha$. Montrer que l'application $f : H \times K \to H \times K$ définie par $f(h,k) = (h, \alpha(k))$ induit un isomorphisme de groupes de $H \rtimes_\varphi K$ vers $H \rtimes_\psi K$.

(*b*) Montrer que si H' est un sous-groupe isomorphe à H et K' est un sous-groupe isomorphe à K, alors $H \rtimes_\varphi K$ est isomorphe à un produit semi-direct $H' \rtimes_{\varphi'} K'$. **Indication :** construire un morphisme φ' de K' dans $\mathsf{Aut}_{\mathsf{Gr}}(H')$ à l'aide d'un isomorphisme f_H de H vers H', d'un isomorphisme f_K de K vers K' et de φ.

(*c*) Soient $\sigma \in \mathsf{Aut}_{\mathsf{Gr}}(H)$ et $\alpha \in \mathsf{Aut}_{\mathsf{Gr}}(K)$ tels que $\mathsf{Ad}_\sigma \circ \varphi = \psi \circ \alpha$, où l'on dénote $\mathsf{Ad}_\sigma : \mathsf{Aut}_{\mathsf{Gr}}(H) \to \mathsf{Aut}_{\mathsf{Gr}}(H)$ le morphisme de groupes qui associe $\sigma \circ \theta \circ \sigma^{-1}$ à $\theta \in \mathsf{Aut}_{\mathsf{Gr}}(H)$. Montrer que l'application $F : H \times K \to H \times K$ définie par $f(h,k) = (\sigma(h), \alpha(k))$ induit un isomorphisme de groupes de $H \rtimes_\varphi K$ vers $H \rtimes_\psi K$.

Solution.

(*a*) Soient (h,k) et (h',k') dans $H \times K$. On voit bien que

$$\begin{aligned} f\big((h,k) \cdot_{H \times_\varphi K} (h',k')\big) &= f\big((h\varphi(k)(h'), kk'\big) = \big(h\varphi(k)(h'), \alpha(kk')\big) \\ &= \big(h\psi\big(\alpha(k)\big)(h'), \alpha(k)\alpha(k')\big) = \big(h, \alpha(k)\big) \cdot_{H \times_\psi K} \big(h', \alpha(k')\big) \\ &= f(h,k) \cdot_{H \times_\psi K} f(h',k'), \end{aligned}$$

ce qui montre le résultat.

(*b*) Soient $f_H : H \to H'$ et $f_K : K \to K'$ deux isomorphismes de groupes. On rappelle que le morphisme de groupes $\mathsf{Ad}_{f_H} : \mathsf{Aut}_{\mathsf{Gr}}(H) \to \mathsf{Aut}_{\mathsf{Gr}}(H')$ défini par $\mathsf{Ad}_{f_H}(\theta) = f_H \circ \theta \circ f_H^{-1}$ pour $\theta \in \mathsf{Aut}_{\mathsf{Gr}}(H)$ est un isomorphisme. On considère le morphisme de groupes $\varphi' : K' \to \mathsf{Aut}_{\mathsf{Gr}}(H')$ donné par $\varphi' = \mathsf{Ad}_{f_H} \circ \varphi \circ f_K^{-1}$. En conséquence,

$$\varphi'(f_K(k))(f_H(h)) = f_H(\varphi(k)(h)) \tag{5}$$

pour tous $h \in H$ et $k \in K$. On définit en plus l'application $f : H \rtimes_\varphi K \to H' \rtimes_{\varphi'} K'$ donnée par $f(h,k) = (f_H(h), f_K(k))$ pour $h \in H$ et $k \in K$. Alors, f est bijective car f_H et f_K le sont. On affirme en plus que f est un morphisme de groupes. En effet, cela suit du fait que

$$\begin{aligned} f\big((h_1,k_1) \cdot_{H \rtimes_\varphi K} (h_2,k_2)\big) &= F\big(h_1\varphi(k_1)(h_2), k_1k_2\big) = \big(f_H\big(h_1\varphi(k)(h_2)\big), f_K(k_1k_2)\big) \\ &= \big(f_H(h_1)f_H\big(\varphi(k_1)(h_2)\big), f_K(k_1)f_K(k_2)\big) \\ &= \big(f_H(h_1)\varphi'\big(f_K(k_1)\big)\big(f_H(h_2)\big), f_K(k_1)f_K(k_2)\big) \\ &= \big(f_H(h_1), f_K(k_1)\big) \cdot_{H' \rtimes_{\varphi'} K'} \big(f_H(h_2), f_K(k_2)\big) \\ &= f(h_1,k_1) \cdot_{H' \rtimes_{\varphi'} K'} f(h_2,k_2) \end{aligned}$$

pour tous (h_1,k_1) et (h_2,k_2) dans $H \times K$, où l'on a utilisé (5) dans le quatrième égalité.

(*c*) Il suffit d'appliquer la question précédente dans le cas particulier où $H' = H$, $K' = K$, $f_H = \sigma$ et $f_K = \alpha$.

13. Soient p et q deux entiers premiers avec $p < q$. On se propose de faire la liste des groupes d'ordre pq à isomorphisme près. Soit G un groupe d'ordre pq.

(*a*) Montrer que G contient un unique q-Sylow Q et que Q est distingué dans G.

(*b*) Soit P un p-Sylow de G. Montrer que $G = Q \rtimes P$.

(*c*) Montrer que $|\mathsf{Aut}_{\mathsf{Gr}}(Q)| = q-1$ et décrire les éléments de $\mathsf{Aut}_{\mathsf{Gr}}(Q)$.

(*d*) Montrer que si p ne divise pas $q-1$, alors $G = Q \times P$ et G est cyclique.

(*e*) Montrer que si p divise $q-1$, alors il existe exactement deux groupes d'ordre pq à isomorphisme près.

Solution.

(*a*) Soit Q un sous-groupe de Sylow pour q, alors $[G : Q] = p$. D'après l'exercice **2** de la fiche 4, Q est distingué. Comme tous les sous-groupes de Sylow pour un premier fixe p qui divise l'ordre de G sont conjugués, on conclut que dans ce cas Q est l'unique sous-groupe de Sylow de G pour p.

(*b*) On voit bien que $P \cap Q = \{1_G\}$, vu qu'il s'agit d'un groupe d'ordre divisant p et q. Comme l'application $m : Q \times P \to G$ qui associe hk à (h, k) est injective, et les ensembles de départ et d'arrivée ont la même cardinalité, elle est bijective. En conséquence, $G = Q \rtimes P$.

(*c*) Comme Q est d'ordre premier, il est cyclique. En conséquence, $Q \simeq \mathbb{Z}/q\mathbb{Z}$, vu que $|Q| = q$. D'après l'exercice **19** on sait que l'application $\mathsf{ev} : \mathsf{Aut}_{\mathsf{Gr}}(Q) \to Q \setminus \{1_Q\} \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ qui associe $f(q)$ à $f \in \mathsf{Aut}_{\mathsf{Gr}}(Q)$, où $q \in Q \setminus \{1_Q\}$ est une élément fixe, est une bijection. En plus, la composition $\mathsf{Aut}_{\mathsf{Gr}}(Q) \to \mathbb{Z}/(q-1)\mathbb{Z}$ est un isomorphisme de groupes. En particulier, $|\mathsf{Aut}_{\mathsf{Gr}}(Q)| = q - 1$.

(*d*) On remarque que P est cyclique, vu que P est d'ordre premier. En conséquence, $P \simeq \mathbb{Z}/p\mathbb{Z}$, car $|P| = p$. D'après l'exercice **4**, si p ne divise pas $q - 1$, tout morphisme de groupes $P \to \mathsf{Aut}_{\mathsf{Gr}}(Q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ est trivial, ce qui implique que le morphisme de groupes $P \to \mathsf{Aut}_{\mathsf{Gr}}(Q)$ qui associe $\mathsf{Ad}_p : Q \to Q$ à $p \in P$, où $\mathsf{Ad}_p(q) = pqp^{-1}$ pour $q \in Q$. En conséquence, P et Q commutent, ce qui implique que $G = Q \times P$. Comme le produit cartésien de groupes cycliques d'ordres premiers entre eux est cyclique, G est cyclique.

(*e*) On suppose dans cet item que p divise $q - 1$. On considère d'abord le groupe $Q \times P$. Comme le produit cartésien de groupes cycliques d'ordres premiers entre eux est cyclique, $Q \times P$ est cyclique d'ordre pq.

Or, d'après l'exercice **4**, comme p divise $q - 1$, il existe un morphisme de groupes non trivial $\varphi : P \to \mathsf{Aut}_{\mathsf{Gr}}(Q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. Dans ce cas, le groupe $Q \rtimes_\varphi P$ ne peut pas être abélien, et en particulier il ne peut pas être cyclique, vu qu'il contient le sous-groupe non distingué $\{1_Q\} \times P$. En conséquence, si φ est non trivial, $Q \rtimes_\varphi P$ et $Q \times P$ sont groupes non isomorphes.

Par ailleurs, on va montrer que, étant donné deux morphismes de groupes non triviaux $\varphi, \psi : P \to \mathsf{Aut}_{\mathsf{Gr}}(Q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$, les groupes $Q \rtimes_\varphi P$ et $Q \rtimes_\psi P$ sont isomorphes. Comme p divise $q - 1$ et le groupe cyclique $\mathsf{Aut}_{\mathsf{Gr}}(Q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ possède un seul sous-groupe d'ordre p. On utilisera un isomorphisme de groupes $P \simeq \mathbb{Z}/p\mathbb{Z}$ et pour $k \in \mathbb{Z}$ notons $\bar{k}$ la classe de k dans $\mathbb{Z}/p\mathbb{Z}$. Comme $\bar{1}$ est un générateur de $\mathbb{Z}/p\mathbb{Z}$ et les morphismes φ et ψ sont non triviaux, $\varphi(\bar{1})$ et $\psi(\bar{1})$ sont des éléments de $\mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/q\mathbb{Z})$ autres que l'élément neutre. On remarque en plus que $\varphi(\bar{1})$ et $\psi(\bar{1})$ ont ordre p, vu que $\bar{1} \in \mathbb{Z}/p\mathbb{Z}$ a ordre p. En conséquence, $\varphi(\bar{1})$ et $\psi(\bar{1})$ engendrent le même sous-groupe de $\mathsf{Aut}_{\mathsf{Gr}}(Q) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. En particulier, il existe un entier k tel que $\mathsf{PGCD}(k, p) = 1$ et $\psi(\bar{1}) = \varphi(\bar{1})^k = \varphi(\bar{k})$. Soit $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ le morphisme de groupes $\bar{x} \mapsto k\bar{x}$. En particulier, $\alpha \in \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p\mathbb{Z})$ et $\psi = \varphi \circ \alpha$. D'après l'exercice **12**, (a), les groupes $Q \rtimes_\varphi P$ et $Q \rtimes_\psi P$ sont isomorphes.

14. On se propose de faire la liste des groupes d'ordre 12 à isomorphisme près.

(*a*) Soit G un groupe d'ordre 12. Montrer que le groupe G contient un sous-groupe distingué d'ordre 3 ou un sous-groupe distingué d'ordre 4.

(*b*) Utiliser l'item précédent pour montrer qu'il existe exactement cinq groupes d'ordre 12 à isomorphisme près. Reconnaître $\mathbb{A}_4$ et D_6.

Solution.

(*a*) On rappelle que pour un groupe fini G, si $p \in \mathbb{N}^*$ est un premier tel que $|G| = p^r m$ avec $\mathsf{PGCD}(p,m) = 1$, alors $N_p = \#(\{P \subseteq G : P \text{ Sylow sous-groupe pour } p\})$ satisfait que $N_p \equiv 1 \pmod p$ et $N_p | m$. En particulier, $N_2 \equiv 1 \pmod 2$, $N_3 \equiv 1 \pmod 3$, $N_2 | 3$ et $N_3 | 4$, vu que $|G| = 2^2 3$. Les deux dernières conditions disent que $N_2 \in \{1,3\}$ et $N_3 \in \{1,2,4\}$. En plus, la deuxième condition nous dit que $N_3 \in \{1,4\}$.

Soit H un sous-groupe de Sylow pour $p = 2$ et K un sous-groupe de Sylow pour $p = 3$. On va montrer que si H n'est pas distingué, alors K est distingué. Comme $|K| = 3$, K est cyclique, *i.e.* $K \simeq \mathbb{Z}/3\mathbb{Z}$. On remarque que $H \simeq \mathbb{Z}/4\mathbb{Z}$ ou $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'après l'exercice **7** de la fiche 2. On considère l'action (à gauche) $G \times G/K \to G/K$ par multiplication à gauche. Si K n'est pas distingué, cette action est fidèle, ce qui nous donne un morphisme injectif de groupes $\rho' : G \to \mathbb{S}_4$. En effet, le noyau du morphisme de groupes $\rho : G \to \mathsf{Aut}_{\mathsf{Ens}}(G/K)$ associé à l'action est le sous-groupe

$$\left\{g \in G : gxK = xK, \text{ pour tout } x \in G\right\} = \bigcap_{x \in G} xKx^{-1} \subsetneq K,$$

et comme $|K| = 3$, on conclut que l'ordre du noyau de ρ est 1, *i.e.* il est trivial, ce qui nous dit que ρ est injectif. Or, comme on a morphisme injectif de groupes $\rho' : G \to \mathbb{S}_4$, l'image de ρ' a indice 2. D'après l'exercice **2** de la fiche 4, $\mathsf{Img}(\rho')$ est distingué, ce qui implique que $G \simeq \mathsf{Img}(\rho') = \mathbb{A}_4$. Comme $\mathbb{A}_4$ possède un sous-groupe de Sylow pour $p = 2$ distingué (voir l'exercice **10**), on conclut que H est distingué dans G.

(*b*) Si H et K sont distingués, alors $G \simeq H \times K$. Dans ce cas, G est abélien, vu que H et K le sont. On trouve dans ce cas les deux groupes non isomorphes

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$$

et

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Si H est distingué mais K n'est pas distingué, alors $G \simeq H \rtimes_\varphi K$, pour un morphisme non trivial $\varphi : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$. On affirme que cela est impossible si H est cyclique. En effet, si l'on utilise des isomorphismes $H \simeq \mathbb{Z}/4\mathbb{Z}$ et $K \simeq \mathbb{Z}/3\mathbb{Z}$, alors φ est équivalent à un morphisme de groupes $\mathbb{Z}/3\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. D'après l'exercice **4**, tout morphisme de groupes $\mathbb{Z}/3\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/4\mathbb{Z})$ est trivial, ce qui implique que H ne peut pas être cyclique dans ce cas. Si $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, alors un morphisme de groupes $\varphi : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$ est équivalent à un morphisme de groupes $\mathbb{Z}/3\mathbb{Z} \to \mathsf{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{S}_3$, d'après l'exercice **5** de la fiche 4. Comme $\mathbb{S}_3$ possède un seul sous-groupe de Sylow pour $p = 3$, on conclut qu'il existe un unique morphisme de groupes non trivial $\varphi : K \to \mathsf{Aut}_{\mathsf{Gr}}(H)$. Cela nous dit qu'il existe un unique groupe $H \rtimes_\varphi K$ et, en conséquence, un seul groupe G à isomorphisme près d'ordre 12 tel que son sous-groupe de Sylow H pour $p = 2$ soit distingué et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et son sous-groupe de Sylow K pour $p = 3$ soit non distingué. C'est facile à voir que $G = \mathbb{A}_4$ est précisément un exemple.

Si H est non distingué mais K est distingué, alors $G \simeq K \rtimes_\varphi H$, pour un morphisme non trivial $\varphi : H \to \mathsf{Aut}_{\mathsf{Gr}}(K)$. On va utiliser l"isomorphisme $K \simeq \mathbb{Z}/3\mathbb{Z}$. Or, ou bien $H \simeq \mathbb{Z}/4\mathbb{Z}$ ou $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dans le premier cas on voit bien qu'il existe un unique morphisme non trivial $\varphi : H \to \mathsf{Aut}_{\mathsf{Gr}}(K) \simeq \mathbb{Z}/2\mathbb{Z}$, ce qui implique qu'il existe un unique groupe $K \rtimes_\varphi H$ et, en conséquence, un seul groupe G à isomorphisme près d'ordre 12 tel que son sous-groupe de Sylow H pour $p = 2$ soit non distingué et isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et son sous-groupe de Sylow K pour $p = 3$ soit distingué. Un exemple

concret est le groupe dicyclique Dic_3. On rappelle que, étant donné un entier $n \geq$, le **groupe dicyclique** Dic_n est le sous-groupe de $\mathsf{SL}_2(\mathbb{C})$ engendré par les matrices

$$\begin{pmatrix} \zeta_{2n} & 0 \\ 0 & \zeta_{2n}^{-1} \end{pmatrix} \text{ et } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

où $\zeta_{2n} = e^{i\pi/n} \in \mathbb{C}$ est une racine primitive de l'unité d'ordre $2n$.

Dans le cas $H \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ on voit bien qu'il existe trois morphismes non triviaux différents $\varphi : \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \simeq H \to \mathsf{Aut}_{\mathsf{Gr}}(K) \simeq \mathbb{Z}/2\mathbb{Z}$. En employant les isomorphismes précédents, on voit bien que ces trois morphismes

$$\varphi_i : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

pour $i \in \{1,2,3\}$ sont donnés par $\varphi_1(a,b) = a$, $\varphi_2(a,b) = b$ et $\varphi_3(a,b) = a+b$. C'est clair que $\varphi_2 = \varphi_1 \circ \alpha_{12}$ et $\varphi_3 = \varphi_1 \circ \alpha_{13}$ où $\alpha_{12}(a,b) = (b,a)$ et $\alpha_{12}(a,b) = (a+b,b)$ pour $a, b \in \mathbb{Z}/2\mathbb{Z}$. Alors, l'exercice **12**, (a), nous dit que les 3 produits semi-directs $K \rtimes_{\varphi_i} H$ obtenus à partir des 3 morphismes non triviaux φ_i pour $i \in \{1,2,3\}$ sont isomorphes En conséquence, il existe un seul groupe G à isomorphisme près d'ordre 12 tel que son sous-groupe de Sylow H pour $p = 2$ soit non distingué et isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et son sous-groupe de Sylow K pour $p = 3$ soit distingué. C'est facile à voir que $G = \mathsf{D}_6 \simeq \mathbb{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ est précisément un exemple.

On a donc montré qu'il existe exactement cinq groupes d'ordre 12 à isomorphisme près : $\{\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{A}_4, \mathsf{Dic}_3, \mathsf{D}_6\}$.