MAT35B - L3A ALGÈBRE
Premier semestre — 2022-2023

Fiche 2: Groupes, sous-groupes et morphismes

1. Soit $(G,\cdot)$ un groupe. Pour $a \in G$, on note τ_a, δ_a et γ_a les applications de G dans G définies par $\tau_a(x) = ax$, $\delta_a(x) = xa$ et $\gamma_a(x) = axa^{-1}$, pour tout $x \in G$. Elles sont appelées **translation à gauche**, **translation à droite** et **conjugaison** par a, respectivement.

(*a*) Ces applications sont-elles des permutations de G ? des automorphismes de groupe ?

(*b*) Montrer qu'il existe un groupe d'ordre 2 et un groupe d'ordre 3 à isomorphisme près.

(*c*) Les applications $\tau : a \mapsto \tau_a$, $\delta : a \mapsto \delta_a$ et $\gamma : a \mapsto \gamma_a$ sont-elles des morphismes de $(G,\cdot)$ dans $(\mathsf{Aut}_{\mathsf{Ens}}(G),\circ)$? Si, oui quel est leur noyau ?

Solution.

(*a*) Soient $\omega \in \{\tau,\delta,\gamma\}$ et $a \in G$. Alors, un calcul immédiat nous dit que $\omega_{a^{-1}} \circ \omega_a = \mathsf{id}_G = \omega_a \circ \omega_{a^{-1}}$, ce qui implique que ω_a est une bijection de G dans G. Comme $\tau_a(1_G) = \delta_a(1_G) = a \neq 1_G$ si $a \neq 1_G$, on conclut que τ_a et δ_a ne sont pas de morphismes de groupes si $a \neq 1_G$. Comme $\tau_{1_G} = \delta_{1_G} = \mathsf{id}_G$, c'est clair que τ_{1_G} et δ_{1_G} sont pas de morphismes de groupes. Enfin, on voit bien que $\gamma_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \gamma_a(x)\gamma_a(y)$, pour tous $a,x,y \in G$, ce qui implique que γ_a est un morphisme de groupes.

(*b*) On voit que les rangées et les colonnes de la table d'un groupe fini G sont des permutations des éléments de G. On conclut que tout groupe d'ordre 2 est isomorphe a $(\mathbb{Z}/2\mathbb{Z},+)$ et que tout groupe d'ordre 3 est isomorphe a $(\mathbb{Z}/3\mathbb{Z},+)$.

(*c*) Soient $\omega \in \{\tau,\gamma\}$. Un calcul immédiat nous dit que $\omega_{ab} = \omega_a \circ \omega_b$, pour tous $a,b \in G$, ce qui nous dit que ω est un morphism de groupes. Par ailleurs, on voit bien aussi que $\delta_{ab} = \delta_b \circ \delta_a$, pour tous $a,b \in G$, car $\delta_{ab}(x) = xab = \delta_a(x)b = \delta_b(\delta_a(x))$, pour $x \in G$. En conséquence, δ n'est pas un morphisme de groupes de G dans $(\mathsf{Aut}_{\mathsf{Ens}}(G),\circ)$ si G n'est pas commutatif.

Finalement, on voit bien que $\mathsf{Ker}(\tau) = \{a \in G : \tau_a = \mathsf{id}_G\} = \{1_G\}$, car $\tau_a(1_G) = a \neq 1_G$ si $a \neq 1_G$ et $\mathsf{Ker}(\gamma) = \{a \in G : \gamma_a = \mathsf{id}_G\} = \mathscr{Z}(G)$, car $\gamma_a(x) = axa^{-1} = x$ pour tout $x \in G$ équivaut à $ax = xa$ pour tout $x \in G$.

2. Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$. L'objet de l'exercice est de montrer que les sous-groupes de $(\mathbb{Z},+)$ sont les parties de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$.

(*a*) Montrer que si $a \in \mathbb{Z}$, alors $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

(*b*) Soit H un sous-groupe de $\mathbb{Z}$. Montrer que H est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$ et que cet entier a est uniquement déterminé. On distinguera deux cas, suivant que H est ou non réduit à $\{0\}$.

Solution.

(*a*) C'est clair que $0 \in a\mathbb{Z}$, car $0 = a.0$. En outre, étant données $x = a.n \in a\mathbb{Z}$ et $y = a.m \in a\mathbb{Z}$, avec $n, m \in \mathbb{Z}$, on voit bien que $x - y = a(n-m) \in a\mathbb{Z}$, ce qui nous dit que $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

(*b*) Si $H = \{0\}$, alors $H = a\mathbb{Z}$, avec $a = 0$. On suppose que $H \neq \{0\}$. On affimr que $H \cap \mathbb{N}^* \neq \emptyset$. En effet, comme $H \neq \{0\}$, il existe $x \in \mathbb{Z} \setminus \{0\}$ tel que $x \in H$. Si $x > 0$, alors $x \in H \cap \mathbb{N}^*$, et si $x < 0$, alors $-x \in H \cap \mathbb{N}^*$, car H est un sous-groupe de $\mathbb{Z}$. On pose $a = \mathsf{min}(H \cap \mathbb{N}^*)$. Le minimum existe car l'ordre de $\mathbb{N}^*$ est bon. On affirme que $H = a\mathbb{Z}$. En effet, comme $a \in H \cap \mathbb{N}^*$, $a\mathbb{Z} \subseteq H$. En outre, soit $b \in H$. On va montrer que $b \in a\mathbb{Z}$. Pour cela, on suppose d'abord que $b > 0$, on écrit $b = pa + r$, avec $p, r \in \mathbb{N}$ et $r < a$. Comme $b \in H$, alors $b - pa = r \in H$, tandis que la condition $r < a$ nous dit que $r = 0$, par définition de a. Si $b < 0$, l'argument précédent nous dit que $-b \in H$ s'écrit de la forme $-b = pa$, avec $p \in \mathbb{Z}$, ce qui implique que $b \in a\mathbb{Z}$. Le cas $b = 0$ est trivial.

3. Soient G un groupe et $a \in G$. On note $f_a : \mathbb{Z} \to G$ l'application qui associe a^k à un entier k.

(*a*) Montrer que f_a est un morphisme de groupes.

(*b*) Montrer que l'image de f_a est $\langle a \rangle$, le sous-groupe engendré par a.

(*c*) Expliquer pourquoi le noyau de f_a est de la forme $d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$, uniquement déterminé.
Remarque : pour tout $n \in \mathbb{Z}$, on a $a^n = 1_G$ si et seulement si $d|n$. Cette équivalence est très utile dans les exercices sur l'ordre d'un élément.

(*d*) Si $d = 0$, à quel groupe est isomorphe le sous-groupe $\langle a \rangle$ engendré par a ? En déduire que a est d'ordre infini.

(*e*) Si $d \in \mathbb{N}^*$, montrer que le sous-groupe $\langle a \rangle$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et donner la liste de ses éléments. En déduire que a est d'ordre fini d, et que d divise $|G|$ si G est fini.

(*f*) Montrer que si a est d'ordre fini d, alors pour tout $\ell \in \mathbb{Z}$, l'ordre de a^ℓ est $d/\,\mathsf{PGCD}(d, \ell)$. En déduire que a^{-1} a le même ordre que a.

(*g*) Montrer que si a est d'ordre fini d, tout conjugué de a (*i.e.*, tout élément de la forme gag^{-1} avec $g \in G$) a le même ordre que a.

(*h*) Soit $\phi : G \to G'$ un morphisme de groupes. Si $a \in G$ est d'ordre fini d, que peut-on dire de l'ordre de $\phi(a)$ dans G' ?

Solution.

(*a*) On rappelle que, étant donné $n \in \mathbb{N}_0$ et $a \in G$, on définit a^n par récurrence de la façon suivante. On pose $a^0 = 1_G$ et $a^{n+1} = a \cdot a^n$ pour tout $n \ni \mathbb{N}_0$. Si n est un entier négatif, on définit $a^n = (a^{-1})^{-n}$. On laisse à la/au lectrice/lecteur la vérification directe de l'identité $a^{n+m} = a^n a^m$ pour tous $m, n \in \mathbb{Z}$. En conséquence, $f_a(n+m) = a^{n+m} = a^n a^m = f_a(n) f_a(m)$, pour tous $m, n \in \mathbb{Z}$, ce qui implique que f_a est un morphisme de groupes.

(*b*) Comme l'image d'un morphisme de groupes est un sous-groupe et $a = f_a(1) \in \mathsf{Img}(f_a)$, $\mathsf{Img}(f_a) \supseteq \langle a \rangle$. En outre, on voit bien que si a est un élement d'un sous-groupe H, un argument par récurrence nous dit que $a^k \in H$ pour tout $k \in \mathbb{N}$. En effet, $1_G = a^0 \in H$, et si $a^k \in H$ pour $k \in \mathbb{N}$ alors $a^{k+1} = a^k a \in H$. En outre, comme $a \in H$, $a^{-1} \in H$, et le résultat précédent nous dit que $a^{-k} \in H$ pour tout $k \in \mathbb{N}$. En conséquence, $a^k \in H$ pour

tout $k \in \mathbb{Z}$ si $a \in H$. Si l'on applique ce résultat appliqué au sous-groupe $H = \langle a \rangle$, on conclut que $f_a(k) = a^k \in \langle a \rangle$ pour tout $k \in \mathbb{Z}$, *i.e.* $\mathsf{Img}(f_a) \subseteq \langle a \rangle$. En conclusion, on a bien montré que $\mathsf{Img}(f_a) = \langle a \rangle$.

(*c*) Comme $\mathsf{Ker}(f_a)$ est un sous-groupe de $\mathbb{Z}$, il existe un unique $d \in \mathbb{N}$ tel que $\mathsf{Ker}(f_a) = d\mathbb{Z}$, d'après l'exercice **2**.

(*d*) On voit bien que f_a est une application injective, car son noyau est nul. En plus, son image est $\langle a \rangle$, ce qui nous dit que f_a est un isomorphisme entre $\mathbb{Z}$ et $\langle a \rangle$. L'ordre de a est donc infini.

(*e*) Le premier théorème d'isomorphisme nous dit que f_a induit un morphisme injectif de groupes $\bar{f}_a : \mathbb{Z}/\mathsf{Ker}(f_a) \to G$ dont l'image est $\langle a \rangle$. En conséquence, $\bar{f}_a$ établit un isomorphisme de groupes de $\mathbb{Z}/\mathsf{Ker}(f_a) = \mathbb{Z}/d\mathbb{Z}$ dans $\langle a \rangle$. En composant la bijection $\bar{f}_a$ avec la bijection $[\![0, d-1]\!] \to \mathbb{Z}/d\mathbb{Z}$ donnée par la composition de l'inclusion $[\![0, d-1]\!] \subseteq \mathbb{Z}$ et la projection canonique $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$, on trouve la bijection $[\![0, d-1]\!] \to \langle a \rangle$ donnée par $k \mapsto a^k$, pour $k \in [\![0, d-1]\!]$. En outre, on voit bien que $1_G = \bar{f}_a(\bar{0}) = \bar{f}_a(\bar{d}) = a^d$ et que l'ordre d de $\langle a \rangle$ divise l'ordre de G, si G est fini.

(*f*) Soit $q = d/\mathsf{PGCD}(d, \ell)$, *i.e.* $d = q\,\mathsf{PGCD}(d, \ell)$. Comme d divise $q\ell$, on voit bien que $(a^\ell)^q = a^{\ell q} = 1_G$. En outre, si $q' \in \mathbb{N}^*$ satisfait que $(a^\ell)^{q'} = a^{\ell q'} = 1_G$, alors $d = q\,\mathsf{PGCD}(d, \ell)$ divise $q'\ell = q'\,\mathsf{PGCD}(d, \ell)\ell/\mathsf{PGCD}(d, \ell)$, ce qui implique que q divise $q\ell/\mathsf{PGCD}(d, \ell)$. Comme q et $\mathsf{PGCD}(d, \ell)$ sont premiers entre eux, on conclut que q divise q'.

(*g*) Il suffit de montrer que, étant donné $d \in \mathbb{N}^*$, $a^d = 1_G$ implique que $(gag^{-1})^d = 1_G$, pour tout $g \in G$. Par ailleurs, ce calcul est immédiat car $(gag^{-1})^d = ga^d g^{-1} = gg^{-1} = 1_G$.

(*h*) Si $a^d = 1_G$ pour $d \in \mathbb{N}^*$, alors $\phi(a)^d = \phi(a^d) = \phi(1_G) = 1_{G'}$. En conséquence, l'ordre de $\phi(a)$ divise l'ordre de a.

4. Soit G un groupe de cardinal $n \in \mathbb{N}^*$ et g un élément de G tel que $G = \langle g \rangle$ (on dit dans ce cas que G est **cyclique**). Un élément a de G est appelé un **générateur** de G si l'on a aussi $G = \langle a \rangle$.

(*a*) Montrer que G contient $\varphi(n)$ générateurs, qui sont exactement les éléments de la forme g^k avec k premier à n.

(*b*) Soit $d \in \mathbb{N}^*$ un diviseur de n.

(i) Montrer que l'ensemble $E_d = \{x \in G : x^d = 1_G\}$ est un sous-groupe cyclique de G de cardinal d, engendré par $g^{n/d}$.

(ii) Soit H un sous-groupe de G de cardinal d. Montrer que $H = E_d$.

(*c*) Déduire de la question précédente que tous les sous-groupes d'un groupe cyclique sont cycliques.

(*d*) Montrer que si d est un diviseur de n, le groupe G contient exactement $\varphi(d)$ éléments d'ordre d.

(*e*) Déduire des questions précédentes l'identité suivante

$$n = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \varphi(d),$$

pour tout $n \in \mathbb{N}^*$

Solution.

(*a*) D'après l'exercice **3**, (b) et (c), $g^n = 1_G$ et n est la période de g. En plus, l'item (e) du même exercice nous dit que l'application $\bar{f}_g : \mathbb{Z}/n\mathbb{Z} \to G$ qui associe g^k à $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme de groupes. Les générateurs de G sont donc en bijection avec les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$, via $\bar{f}_g$. Un calcul immédiat nous dit que les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont précisément les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Le résultat suit alors de l'exercice **3**, (e), de la fiche 1.

(*b*) On considère le morphisme surjectif de groupes $f_g : \mathbb{Z} \to G$ qui associe g^k à $k \in \mathbb{Z}$. On va montrer que, si d est un divisor de n, il existe un unique sous-groupe de G d'ordre d, et que ce sous-groupe est cyclique. Pour montrer l'existence, on pose $n' = n/d$. L'image directe H du sous-groupe $n'\mathbb{Z}$ de $\mathbb{Z}$ par f_g est un sous-groupe cylique de G, vu que c'est l'image d'un groupe cyclique par un morphisme de groupes. En plus, comme $n'|n$, $n'\mathbb{Z} \supseteq n\mathbb{Z}$ et f_g induit un isomorphisme de groupes $\mathbb{Z}/n'\mathbb{Z} \to G/H$. Comme l'indice de H dans G est n', l'ordre du sous-groupe cyclique H est exactement $n/n' = d$. On va montrer maintenant que l'unicité. Soit H un sous-groupe de G de cardinal d. Soit $f_g^{-1}(H)$ le sous-groupe de $\mathbb{Z}$. Noter que $f_g^{-1}(H)$ inclut le noyau $n\mathbb{Z}$ de f_g. D'après l'exercice **2**, il existe un unique $n' \in \mathbb{N}^*$ tel que $f_g^{-1}(H) = n'\mathbb{Z}$. Comme $H = f(f^{-1}(H))$, le sous-groupe H est determiné de façon unique par n'. En plus, on remarque que $H = f(f^{-1}(H))$ est un groupe cyclique, car c'est l'imagen directe d'un sous-groupe cyclique par un morphisme de groupes.

On revient maintent à la question dans l'item. On va monter que E_d est un sous-groupe. On voit bien que $1_G^d = 1_G$, *i.e.* $1_G \in E_d$. En plus, si $x, y \in E_d$, alors $(xy)^d = x^d y^d = 1_G 1_G = 1_G$, *i.e.* $xy \in E_d$. Comme $(x^{-1})^d = (x^d)^{-1}$, on conlut que $x^{-1} \in E_d$ si $x \in E_d$. En conséquence, E_d est un sous-groupe de G. Le résultat dans le paragraphe précédent nous dit que E_d est cylique. En plus, $f_g(E_d) = \{m \in \mathbb{Z} : g^{md} = 1_G\} = (n/d)\mathbb{Z}$, car g a ordre n, ce qui nous dit que E_d est engendré par $f_g(n/d) = g^{n/d}$. On conclut aussi que l'indice de E_d est n/d, ce qui implique que l'ordre de E_d est d.

(*c*) On a démontré cette question dans l'item précédent.

(*d*) Pour $d \in \mathbb{N}^*$ diviseur de $n = |G|$, on définit $G_d = \{g \in G : g \text{ a ordre } d\}$. On remarque que G_d est précisément l'ensemble de générateurs du sous-groupe E_d. En effet, si $g \in G_d$, alors $g^d = 1_G$, ce qui nous dit que $g \in E_d$. En outre, comme l'ordre de g est d le sous-groupe engendré par g, qui est inclus dans E_d, est précisément E_d, vu que les deux ont le même cardinal. Réciproquement, si $g \in E_d$ est un générateur de E_d, son ordre est précisément d. D'après le premier item, le cardinal de l'ensemble de générateurs G_d du sous-groupe E_d est $\varphi(d)$.

(*e*) Comme

$$G = \bigsqcup_{\substack{d \in \mathbb{N}^* \\ d|n}} G_d,$$

et $\#(G_d) = \varphi(d)$ pour tout $d \in \mathbb{N}^*$ diviseur de n, d'après l'item précédent, on trouve que

$$n = |G| = \sum_{\substack{d \in \mathbb{N}^* \\ d|n}} \varphi(d).$$

5. Soient p et q deux nombres premiers distincts.

(*a*) Montrer que $a^{p-1} \equiv 1 \pmod p$ si a est un entier non multiple de p.

(*b*) Montrer que $a^p \equiv a \pmod p$ pour tout $a \in \mathbb{Z}$.

(*c*) On fixe $e \in \mathbb{N}^*$ et $d \in \mathbb{N}^*$ tels que $de \equiv 1 \pmod{(p-1)(q-1)}$. Montrer que $M^{de} \equiv M \pmod{pq}$ pour tout $M \in \mathbb{Z}$.
Indication : montrer la congruence modulo p et modulo q. Ce résultat est à la base de l'algorithme RSA introduit par R. Rivest, A. Shamir et L. Adleman en 1977.

(*d*) Soit $n \in \mathbb{N}^*$. Montrer que $a^{\varphi(n)} \equiv 1 \pmod{n}$ pour tout entier a premier avec n.

Solution.

(*a*) Comme $\varphi(p) = p - 1$, pour p premier, vu que $\mathbb{Z}/p\mathbb{Z}$ est un corps, *i.e.* $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, il s'agit d'un conséquence du dernier item.

(*b*) Si a n'est pas divisible par p, alors $a^p \equiv a^{p-1}a \equiv a \pmod{p}$, d'après la question précédente. Si a est divisible par p, alors $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$.

(*c*) Il suffit de montrer que $M^{de} \equiv M \pmod{p}$ et $M^{de} \equiv M \pmod{q}$, car cela nous dit que $p|(M^{de} - M)$ et $q|(M^{de} - M)$, et en conséquence $pq|(M^{de} - M)$, vu que p et q sont premiers entre eux. On va montrer que $p|(M^{de} - M)$, puisque l'autre identité est analogue. Si $p|M$, alors $M^{de} \equiv 0^{de} \equiv 0 \equiv M \pmod{p}$. On suppose désormais $p \nmid M$. Comme $de \equiv 1 \pmod{(p-1)(q-1)}$, alors $de \equiv 1 \pmod{(p-1)}$, ce qui implique qu'il existe $k \in \mathbb{N}$ tel que $de = 1 + k(p-1)$. En conséquence,

$$M^{de} \equiv M^{1+k(p-1)} \equiv M(M^{(p-1)})^k \equiv M1^k \equiv M \pmod{(p-1)(q-1)},$$

où l'on a utilisait le premier item dans la trousième congruence.

(*d*) Soit $x = \bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Comme a est premier avec n, alors $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. En outre, vu que l'ordre d'un élément d'un groupe divise l'ordre du groupe, on conclut que l'ordre d de x divise $\varphi(n)$, *i.e.* il existe $k \in \mathbb{N}^*$ tel que $\varphi(n) = dk$. En conséquence, $x^{\varphi(n)} = (x^d)^k = \bar{1}^k = \bar{1}$, ce qui nous dit que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

6. Soient G_1 et G_2 deux groupes.

(*a*) Montrer que $G_1 \times G_2$ possède une structure naturelle de groupe.

(*b*) Soient $a_1 \in G_1$ d'ordre fini d_1 et $a_2 \in G_2$ d'ordre fini d_2. Quel est l'ordre de (a_1, a_2) dans le groupe $G_1 \times G_2$?

(*c*) Montrer que $G_1 \times G_2$ est cyclique si et seulement si G_1 et G_2 sont cycliques et d'ordres premiers entre eux.

Solution.

(*a*) On laisse à la/au lectrice/lecteur la vérification immédiate que la loi de composition donnée par $(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$ donne bien une structure de groupe sur $G_1 \times G_2$, pour $g_I, g_i' \in G_i$ et $i \in \{1, 2\}$. On note que le neutre de $G_1 \times G_2$ est $(1_{G_1}, 1_{G_2})$ et l'inverse de $(g_1, g_2) \in G_1 \times G_2$ est (g_1^{-1}, g_2^{-1}) En plus, la projection canonique $\pi_i : G_1 \times G_2 \to G_i$ est un morphisme surjectif de groupes pour $i \in \{1, 2\}$.

(*b*) Soit $d_i \in \mathbb{N}^*$ l'ordre de a_i pour $i \in \{1, 2\}$ et soit $\hat{m} = \mathsf{PPCM}(d_1, d_2)$. C'est clair que $(a_1, a_2)^{\hat{m}} = (a_1^{\hat{d}}, a_2^{\hat{m}}) = (1_{G_1}, 1_{G_2})$, vu que $d_i | \hat{m}$ pour $i \in \{1, 2\}$, ce qui nous dit que l'ordre $m \in \mathbb{N}^*$ de (a_1, a_2) divise $\hat{m}$. En outre, comme $(a_1, a_2)^m = (1_{G_1}, 1_{G_2})$, alors $a_i^m = 1_{G_i}$ pour $i \in \{1, 2\}$, ce qui nous dit que $d_i | m$ pour $i \in \{1, 2\}$ et en particulier $\hat{m} | m$. En conséquence, $\hat{m} = m$.

(*c*) On suppose d'abord que G_1 et G_2 sont cycliques et d'ordres $d_1 \in \mathbb{N}^*$ et $d_2 \in \mathbb{N}^*$, respectivement, avec d_1 et d_2 premiers entre eux. On remarque que G_1 et G_2 sont groupes finis, ce qui implique que $G_1 \times G_2$ est aussi fini. Soit $g_i \in G_i$ un générateur de G_i pour $i \in \{1,2\}$. Alors, $g = (g_1, g_2)$ est ungénérateur de $G_1 \times G_2$. En effet, l'ordre de g est $\mathsf{PPCM}(d_1, d_2) = d_1 d_2$, *i.e.* le sous-groupe $\langle g \rangle$ engendré par g a cardinal $d_1 d_2 = |G_1|.|G_2| = |G_1 \times G_2|$, ce qui implique que $G_1 \times G_2$ coïncide avec $\langle g \rangle$.

On suppose maintenant que $G_1 \times G_2$ est cyclique. Comme la projection canonique $\pi_i : G_1 \times G_2 \to G_i$ est un morphisme surjectif de groupes pour $i \in \{1,2\}$, on conclut que $G_i = \mathsf{Img}(\pi_i)$ est cyclique. Soient $d_1 \in \mathbb{N}^*$ et $d_2 \in \mathbb{N}^*$ les ordres de G_1 et G_2, respectivement On va montrer que si d_1 et d_2 ne sont pas premiers entre eux, alors $G_1 \times G_2$ n'est pas cyclique. Soient $d = \mathsf{PGCD}(d_1, d_2)$ et $d_i' = d_i/d$ pour $i \in \{1,2\}$. On voit bien que les sousgroupes $H_1 = \langle (g_1^{d_1'}, 1_{G_2}) \rangle$ et $H_2 = \langle (1_{G_1}, g_2^{d_2'}) \rangle$ sont cycliques d'ordre d, car H_i est l'image du sous-groupe cyclique de G_i engendré par $g_i^{d_i'}$, qui a ordre d, via l'application qui associe $(x, 1_{G_2})$ à $x \in G_1$ si $i = 1$, et $(1_{G_1}, x)$ à $x \in G_2$ si $i = 2$. En outre, $H_1 \cap H_2 = \{(1_{G_1}, 1_{G_2})\}$. Comme $G_1 \times G_2$ a deux sous-groupes différents du même ordre, alors il n'est pas cyclique.

7. (*a*) Soit p un nombre premier. Montrer que tout groupe fini G d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(*b*) Montrer que tout groupe fini G d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $(\mathbb{Z}/2\mathbb{Z})^2$

Solution.

(*a*) Soit $g \in G$ différent de l'élément neutre de G. Alors, son ordre $d \in \mathbb{N}^*$ est strictément supérieur à 1. Par le théorème de Lagrange, d divise p, ce qui implique que $d = p$. On considère le morphisme de groupes $f_g : \mathbb{Z} \to G$ qui associe g^n à $n \in \mathbb{Z}$. L'argument précédent nous dit que f_g est surjectif. Le premier théorème d'isomorphisme nous dit que f_g induit un morphisme de groupes $\bar{f}_g : \mathbb{Z}/d\mathbb{Z} \to G$, qui est injectif et surjectif. En conséquence, G est isomorphe au groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ d'ordre p.

(*b*) Soit $g \in G$ un élément différent de l'élément neutre de G. Alors, son ordre $d \in \mathbb{N}^*$ est strictément supérieur à 1. Par le théorème de Lagrange, d divise 4. Si $d = 4$, alors le sous-groupe $\langle g \rangle$ engendré par g a ordre 4, ce qui nous dit que $G = \langle g \rangle$, *i.e.* G est isomorphe au groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ d'ordre 4. On suppose par ailleurs que tout élément g de G différent de l'élément neutre de G a ordre strictément inférieur à 4. Cela équivaut à dire que l'ordre de tout élément de G différent de l'élément neutre de G est 2. Soit $g \in G$ un élément d'ordre 2. Comme $\langle g \rangle \subsetneq G$, il existe $h \in G \setminus \langle g \rangle$, qui a forcément degré 2. C'est clair que l'élément $gh = hg$ a ordre 2, et que $h \neq hg \neq g$. On conclut que $\{1_G, g, h, gh\}$ est un sous-groupe de G. Par des raisons de cardinalité on voit alors que $G = \{1_G, g, h, gh\}$. En outre, l'application $(\mathbb{Z}/2\mathbb{Z})^2 \to G$ qui associe $g^n h^m$ à $(\bar{n}, \bar{m})$ pour $n, m \in \mathbb{Z}$ est un isomorphisme de groupes bien défini.

8. Soit G un groupe abélien.

(*a*) On suppose que tous les éléments de G sont d'ordre fini. Le groupe G est-il fini ? Même question si les ordres sont bornés.

(*b*) On utilisera désormais la notation additive. On suppose qu'il existe un entier premier p tel que tous les éléments non nuls de G soient d'ordre p. Montrer que le groupe G possède une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En déduire que si le groupe G est fini alors il existe un entier positif d tel que G

soit isomorphe au groupe produit $(\mathbb{Z}/p\mathbb{Z})^d$.

Solution.

(*a*) Non aux deux question, car on peut considérer le groupe $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}} = \prod_{i\in\mathbb{N}}(\mathbb{Z}/2\mathbb{Z})$. Dans ce cas tous les éléments ont ordre 2, mais G est infini.

(*b*) On rappelle que, étant donné $n \in \mathbb{Z}$ et $x \in G$, on définit le morphisme de groupes $f_x : \mathbb{Z} \to G$ donné par $f_x(0) = \mathbf{0}_G$,

$$f_x(n) = \underbrace{x + \cdots + x}_{n \text{ opérandes}}$$

si $n > 0$, et

$$f_x(n) = \underbrace{(-x) + \cdots + (-x)}_{-n \text{ opérandes}}$$

si $n < 0$, où $-x$ est l'inverse de $x \in G$ dans G. On écrit d'habitude $n \cdot x$ au lieu de $f_x(n)$. Comme tout élément non nul de G possède ordre p, $\mathsf{Ker}(f_x) = p\mathbb{Z}$ et l'application f_x induit un morphisme de groupes $\bar{f}_x : \mathbb{Z}/p\mathbb{Z} \to G$ tel que $\bar{f}_x \circ \pi = f_x$, où $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ est la projection canonique.

On définit l'application

$$a : \mathbb{Z}/p\mathbb{Z} \times G \to G$$

via $a(\bar{n}, x) = \bar{f}_x(\bar{n})$, pour $n \in \mathbb{Z}$ et $x \in G$. On écrit d'habitude $\bar{n} \cdot x$ au lieu de $a(\bar{n}, x)$. On laisse à la/au lectrice/lecteur la vérification immédiate du fait que

$$\begin{aligned}(\bar{n}.\bar{m}) \cdot x &= \bar{n} \cdot (\bar{m} \cdot x),\\ (\bar{n} + \bar{m}) \cdot x &= \bar{n} \cdot x + \bar{m} \cdot x,\\ \bar{n} \cdot (x + y) &= \bar{n} \cdot x + \bar{n} \cdot y,\\ \bar{1} \cdot x &= x,\end{aligned}$$

pour tous $x, y \in G$ et $n, m \in \mathbb{Z}$. En conséquence, G possède une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. En particulier, si $|G|$ est fini, il est un espace vectoriel de dimension finie d sur $\mathbb{Z}/p\mathbb{Z}$, ce qui implique que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^d$ comme espaces vectoriels sur $\mathbb{Z}/p\mathbb{Z}$, ce qui implique *a fortiori* que G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^d$ comme groupes.

9. Soit G un groupe dont tous les éléments sont d'ordre 1 ou 2. Montrer que G est abélien. Si de plus G est fini, pourquoi son ordre est-il une puissance de 2 ?

Solution. Soient $x, y \in G$. Comme $1_G = (xy)^2 = xyxy = xyxy$, alors

$$yx = xyxyyx = xyxy^2x = xyx1_Gx = xyx^2 = xy1_G = xy,$$

où l'on a utilisé que $x^2 = y^2 = 1_G$. En conséquence, $xy = yx$ pour tous $x, y \in G$, ce qui nous dit que G est abélien. La dernière question est une conséquence de l'item (b) de l'exercice **8**.

10. Soit G un groupe. Soient a et b deux éléments d'ordres finis dans G, tels que $ab = ba$. On note $\mathsf{ord}(a) = m$ et $\mathsf{ord}(b) = n$ les ordres, $d = \mathsf{PGCD}(m, n)$, $m = dm'$, $n = dn'$.

(*a*) Montrer ab est d'ordre fini divisant $\mathsf{PPCM}(m,n)$.

(*b*) Montrer que cette divisibilité peut être stricte.

(*c*) Montrer que l'ordre de ab est multiple de $\mathsf{PPCM}(m,n)/\mathsf{PGCD}(m,n)$.
Indication : poser $r = \mathsf{ord}(ab)$ et, en utilisant l'égalité $a = (ab)b^{-1}$, montrer que m divise rn.

(*d*) En déduire que si $\mathsf{PGCD}(m,n) = 1$, alors $\mathsf{ord}(ab) = mn = \mathsf{ord}(a)\,\mathsf{ord}(b)$.

(*e*) Montrer que ces conclusions peuvent êtres fausses sans l'hypothèse $ab = ba$.

Solution.

(*a*) Soit $M = \mathsf{PPCM}(m,n)$. On voit bien que

$$(ab)^M = a^M b^M = 1_G 1_G = 1_G,$$

vu que $m|M$ et $n|M$.

(*b*) Si $b = a^{-1} \neq 1_G$, alors $m = n = \mathsf{PPCM}(m,n) \neq 1$ mais l'ordre de $ab = 1_G$ est 1.

(*c*) Comme $a = (ab)b^{-1}$, alors le premier item nous dit que $m = \mathsf{ord}(a)$ divise $\mathsf{PPCM}(r,n)$ et *a fortiori* il divise rn, ce qui nous dit que $m/\mathsf{PGCD}(m,n)$ divise $rn/\mathsf{PGCD}(m,n)$. Comme $m/\mathsf{PGCD}(m,n)$ et $n/\mathsf{PGCD}(m,n)$ sont premiers entre eux, on conclut que $m/\mathsf{PGCD}(m,n)$ divise $r = \mathsf{ord}(ab)$. De la même façon, on conclut que $n/\mathsf{PGCD}(m,n) = \mathsf{ord}(b)/\mathsf{PGCD}(m,n)$ divise $r = \mathsf{ord}(ab)$. Comme $m/\mathsf{PGCD}(m,n)$ et $n/\mathsf{PGCD}(m,n)$ sont premiers entre eux, on conclut que $mn/\mathsf{PGCD}(m,n)^2 = \mathsf{PPCM}(m,n)/\mathsf{PGCD}(m,n)$ divise $r = \mathsf{ord}(ab)$.

(*d*) L'item précédent nous dit que, si $\mathsf{PGCD}(m,n) = 1$, alors $\mathsf{PPCM}(m,n)$ divise $r = \mathsf{ord}(ab)$, tandis que le premier item nous dit que $r = \mathsf{ord}(ab)$ divise $\mathsf{PPCM}(m,n)$. En conclusion, $r = \mathsf{PPCM}(m,n)$.

(*e*) On considère le groupe $G = \mathsf{SL}_2(\mathbb{Z})$. Soient

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

On voit bien dans ce cas que $a^4 = b^3 = I_2$, mais ab a ordre infini, car

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

pour tout $n \in \mathbb{Z}$. En particulier, $\langle ab \rangle$ est un sous-groupe infini.

11. Soit G un groupe abélien fini. On note m le PPCM des ordres des éléments de G. Cet entier s'appelle l'**exposant** de G.

(*a*) Montrer que m divise l'ordre de G, et que cette divisibilité peut être stricte.

(*b*) Montrer que G possède au moins un élément d'ordre m.
Indication : utiliser les résultats des exercices précédents et la décomposition de m en facteurs premiers.

Solution.

(*a*) Comme $\mathsf{ord}(g) = |\langle g \rangle|$ divise $|G|$ pour tout $g \in G$, d'après le théorème de Lagrange, on conclut que $m = \mathsf{PPCM}(\mathsf{ord}(g) : g \in G) \in \mathbb{N}^*$ divise $|G|$ aussi, par la définition du plus petit commun diviseur.

On voit bien que tout élément non nul de $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a ordre 2, ce qui implique $m = 2$ mais $|G| = 4$.

(*b*) On dit que $N \in \mathbb{N}^*$ est **un exposant** de G si $g^N = 1_G$ pour tout $g \in G$. On note $\mathsf{Exp}(G) \subseteq \mathbb{N}^*$ l'ensemble d'exposants de G. Noter que

$$\mathsf{Exp}(G) = \big\{N \in \mathbb{N}^* : \mathsf{ord}(g) \text{ divise } N, \text{ pour tout } g \in G\big\}, \tag{1}$$

car $g^N = 1_G$ équivaut à dire que $\mathsf{ord}(g)$ divise N. Un argument de divisibilté immédiate nous dit qu'il existe $d \in \mathbb{N}^*$ tel que $\mathsf{Exp}(G) = d\mathbb{N}^*$. En effet, si l'on prend $d = \mathsf{min}(\mathsf{Exp}(G))$ et $N \in \mathsf{Exp}(G)$, alors on peut écrire $N = qd + r$, avec $r \in [\![0, d-1]\!]$. Si $r = N - qd > 0$, alors $r \in \mathsf{Exp}(G)$, vu que $\mathsf{ord}(g)$ divise N et $d \in \mathsf{Exp}(G)$, mais comme $r < d = \mathsf{min}(\mathsf{Exp}(G))$ on trouve une contradiction. En conséquence, $r = 0$, *i.e.* $N = dq \in d\mathbb{N}^*$. Par définition du plus petit commun multiple et (1), $d = \mathsf{PPCM}(\mathsf{ord}(g) : g \in G)$. En conséquence, $\mathsf{exp}(G) = \mathsf{PPCM}(\mathsf{ord}(g) : g \in G)$.

On écrit $\mathsf{exp}(G) = \prod_{i=1}^{\ell} p_i^{r_i}$, avec $\{p_1, \dots, p_\ell\} \subseteq \mathbb{N}^*$ une famille de nombres premiers distincts et $\{r_1, \dots, r_\ell\} \subseteq \mathbb{N}^*$. On va montrer que, étant donné $i \in [\![1, \ell]\!]$, il existe $g_i \in G$ d'ordre $p_i^{r_i}$. Si ce n'est pas vrai, alors il existe $i \in [\![1, \ell]\!]$ tel que l'ordre de tout élément $g \in G$ est de la forme $p_i^{s_g} q_g$ avec $s_g \in [\![0, r_i - 1]\!]$ et $\mathsf{PGCD}(p_i, q_g) = 1$. Cela suit du fait que, s'il existe $g \in G$ tel que $\mathsf{ord}(g) = p_i^s q$ avec $s \geq r_i$ et $\mathsf{PGCD}(p_i, q_g) = 1$, alors $g^{qp_i^{s-r_i}}$ a ordre $p_i^{r_i}$. Or, l'hypothèse précédente nous dit que

$$\mathsf{PPCM}(\mathsf{ord}(g) : g \in G) = p_i^M q,$$

avec $M = \mathsf{max}\{s_g : g \in G\}$ et $\mathsf{PGCD}(p_i, q) = 1$, ce qui est absurde. En conséquence, étant donné $i \in [\![1, \ell]\!]$, il existe $g_i \in G$ d'ordre $p_i^{r_i}$. D'après l'item (d) de l'exercice **10**, on conclut que $g = \prod_{i=1}^{\ell} g_i$ a ordre $\prod_{i=1}^{\ell} p_i^{r_i} = \mathsf{exp}(G)$. En particulier, on en déduit que

$$\mathsf{exp}(G) = \mathsf{max}\{\mathsf{ord}(g) : g \in G\},$$

car $\mathsf{ord}(g) | \mathsf{exp}(G)$ pour tout $g \in G$ mais il existe $g \in G$ tel que $\mathsf{ord}(g) = \mathsf{exp}(G)$.

12. On va montrer que $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{S}_3 = \mathsf{Aut}_{\mathsf{Ens}}(\{1,2,3\})$ sont les seuls groupes d'ordre 6 à isomorphisme près.

(*a*) On note τ et γ les bijections de $\{1,2,3\}$ définies par $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 3$ et $\gamma(1) = 2$, $\gamma(2) = 3$, $\gamma(3) = 1$. Déterminer les images de 1, 2, 3 par $\tau^2 = \tau \circ \tau$, γ^2, γ^3, $\tau \circ \gamma$ et $\tau \circ \gamma^2$, $\gamma \circ \tau$, $\gamma^2 \circ \tau$. Mettre les résultats sous forme de tableau. En déduire que $\mathbb{S}_3 = \{\mathsf{id}_{\{1,2,3\}}, \gamma, \gamma^2, \tau, \tau \circ \gamma, \tau \circ \gamma^2\}$ et donner la table du groupe $(\mathbb{S}_3, \circ)$.

(*b*) Soit G un groupe d'ordre 6, non isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

(i) Montrer que G possède nécessairement un élément d'ordre 3.

(ii) Montrer que G possède nécessairement un élément d'ordre 2.

(iii) Soient α un élément d'ordre 3 et β un élément d'ordre 2. Montrer que $G = \{1_G, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$.

(iv) En remarquant que $\alpha\beta \neq \beta\alpha$ (pourquoi ?), dresser la table de multiplication de G et en déduire que G est isomorphe à $\mathbb{S}_3$.

(*c*) Soit $A_1A_2A_3$ un triangle non-aplati de $\mathbb{R}^2$ d'isobarycentre $O = (0,0)$. Soit T le sous-groupe de $\mathsf{GL}(\mathbb{R}^2)$ formé des automorphismes linéaires de $\mathbb{R}^2$ laissant l'ensemble $\{A_1, A_2, A_3\}$ globalement invariant. Exhiber un isomorphisme de $\mathbb{S}_3$ vers T.

Solution.

(*a*) On voit bien que

$\sigma \in \mathbb{S}_3$	τ^2	γ^2	γ^3	$\tau\circ\gamma$	$\tau\circ\gamma^2$	$\gamma\circ\tau$	$\gamma^2\circ\tau$
$\sigma(1)$	1	3	1	1	3	3	1
$\sigma(2)$	2	1	2	3	2	2	3
$\sigma(3)$	3	2	3	2	1	1	2

En particulier, on note que $\tau^2 = \gamma^3 = \mathsf{id}_{\{1,2,3\}}$, $\tau\circ\gamma = \gamma^2\circ\tau$ et $\tau\circ\gamma^2 = \gamma\circ\tau$. On déduit que $\{\mathsf{id}_{\{1,2,3\}}, \gamma, \gamma^2, \tau, \tau\circ\gamma, \tau\circ\gamma^2\}$ a cardinal 6, ce qui implique que $\mathbb{S}_3 = \{\mathsf{id}_{\{1,2,3\}}, \gamma, \gamma^2, \tau, \tau\circ\gamma, \tau\circ\gamma^2\}$.

C'est facile à vérifier que la table de multiplication du groupe $(\mathbb{S}_3, \circ)$ est donnée par les résultats suivants, où la cellule dans la ligne indéxée par $\sigma_1 \in \mathbb{S}_3$ et la colonne indexée par $\sigma_2 \in \mathbb{S}_3$ indique $\sigma_1 \circ \sigma_2$.

σ_1 \ σ_2	$\mathsf{id}_{\{1,2,3\}}$	γ	γ^2	τ	$\tau\circ\gamma$	$\tau\circ\gamma^2$
$\mathsf{id}_{\{1,2,3\}}$	$\mathsf{id}_{\{1,2,3\}}$	γ	γ^2	τ	$\tau\circ\gamma$	$\tau\circ\gamma^2$
γ	γ	γ^2	$\mathsf{id}_{\{1,2,3\}}$	$\tau\circ\gamma^2$	τ	$\tau\circ\gamma$
γ^2	γ^2	$\mathsf{id}_{\{1,2,3\}}$	γ	$\tau\circ\gamma$	$\tau\circ\gamma^2$	τ
τ	τ	$\tau\circ\gamma$	$\tau\circ\gamma^2$	$\mathsf{id}_{\{1,2,3\}}$	γ^2	γ^2
$\tau\circ\gamma$	$\tau\circ\gamma$	$\tau\circ\gamma^2$	τ	γ^2	$\mathsf{id}_{\{1,2,3\}}$	γ
$\tau\circ\gamma^2$	$\tau\circ\gamma^2$	τ	$\tau\circ\gamma$	γ	γ^2	$\mathsf{id}_{\{1,2,3\}}$

(*b*) Soit G un groupe d'ordre 6, non isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

(i) Comme $\mathsf{ord}(g)$ divise $|G| = 6$ pour tout $g \in G$, on voit que $\mathsf{ord}(g) \in \{1,2,3,6\}$. S'il existe $g \in G$ tel que $\mathsf{ord}(g) = 6$, alors G est cyclique d'ordre 6, ce qui implique que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$, ce qui est absurde. Alors $\mathsf{ord}(g) \in \{2,3\}$ pour tout $g \in G \setminus \{1_G\}$. Si $\mathsf{ord}(g) \neq 3$ pour tout $g \in G \setminus \{1_G\}$, alors $\mathsf{ord}(g) = 2$ pour tout $g \in G \setminus \{1_G\}$, ce qui impliqueque G est abélien et $|G|$ est une puissance de 2, d'après l'exercice **9**. Comme $|G| = 6$ n'est pas une puissance de 2, on conclut qu'il existe $g \in G$ tel que $\mathsf{ord}(g) = 3$.

(ii) On remarque d'abord le fait élémentaire que deux sous-groupes cycliques H, H' d'ordre m d'un groupe G coïncident si et seulement si $H \cap H'$ contient un élément d'ordre m. On suppose maintenant que $\mathsf{ord}(g) = 3$ pour tout $g \in G \setminus \{1_G\}$. Soient $\alpha \in G\setminus\{1_G\}$ et $\alpha' \in G\setminus\langle\alpha\rangle$ d'ordre 3. D'après la remarque initiale, $\langle\alpha\rangle \cap \langle\alpha'\rangle = \{1_G\}$, vu que tous les éléments non triviaux de un groupe cyclique H d'ordre premier p ont ordre p. En conséquence, $S = \langle\alpha\rangle \cup \langle\alpha'\rangle$ contient 5 éléments. Soit $\alpha'' \in G\setminus S$, qui possède ordre 3 par hypothèse. En conséquence, $\langle\alpha''\rangle \cap \langle\alpha\rangle = \langle\alpha''\rangle \cap \langle\alpha'\rangle = \{1_G\}$,

ce qui nous dit que $S \cup \langle \alpha'' \rangle \subseteq G$ possède 7 éléments, ce qui est absurde. En conséquence, G possède un élément d'ordre 2.

(iii) Comme l'application $\tau_g : G \to G$ donnée par $\tau_g(x) = gx$ est une bijection, $\{\beta, \beta\alpha, \beta\alpha^2\}$ a cardinal 3. En plus, on voit bien que $\beta\alpha \notin \{1_G, \alpha, \alpha^2\}$, car cela impliquerait $\beta = \alpha^{-1} = \alpha^2$, $\beta = 1_G$ ou $\beta = \alpha$, qui sont des contradictions. De la même façon on note que $\beta\alpha^2 \notin \{1_G, \alpha, \alpha^2\}$, car cela impliquerait $\beta = \alpha^{-2} = \alpha$, $\beta = \alpha$ ou $\beta = 1_G$, qui sont des contradictions. En conséquence, $\{1_G, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\} \subseteq G$ a 6 éléments et donc $\{1_G, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\} = G$.

(iv) Noter d'abord que $\alpha\beta \neq \beta\alpha$, car $\alpha\beta = \beta\alpha$, impliquerait que l'ordre de $\alpha\beta$ est 6, ce qui est impossible. Un calcul direct nous dit que $\alpha\beta \notin \{1_G, \alpha, \alpha^2, \beta\}$, ce qui implique que $\alpha\beta = \beta\alpha^2$. Finalement, la table de multiplication du groupe G est donnée par les résultats suivants, où la cellule dans la ligne indéxée par $g_1 \in G$ et la colonne indexée par $g_2 \in G$ indique $g_1 \cdot g_2$.

g_1 \ g_2	1_G	α	α^2	β	$\beta \circ \alpha$	$\beta \circ \alpha^2$
1_G	1_G	α	α^2	β	$\beta \circ \alpha$	$\beta \circ \alpha^2$
α	α	α^2	1_G	$\beta \circ \alpha^2$	β	$\beta \circ \alpha$
α^2	α^2	1_G	α	$\beta \circ \alpha$	$\beta \circ \alpha^2$	β
β	β	$\beta \circ \alpha$	$\beta \circ \alpha^2$	1_G	α^2	α^2
$\beta \circ \alpha$	$\beta \circ \alpha$	$\beta \circ \alpha^2$	β	α^2	1_G	α
$\beta \circ \alpha^2$	$\beta \circ \alpha^2$	β	$\beta \circ \alpha$	α	α^2	1_G

En comparant avec la table de multiplication de $\mathbb{S}_3$ on conclut que l'application $\beta^j\alpha^k \mapsto \tau^j\gamma^k$, avec $j \in \{0,1\}$ et $k \in \{0,1,2\}$ induit un isomorphisme de groupes de $\mathbb{S}_3$ dans G.

(*c*) On remarque d'abord que l'hypothèse sur l'isobarycentre est précisément $A_1 + A_2 + A_3 = (0,0)$, tandis que l'hypothèse sur le triangle nous dit que $\{A_i, A_j\}$ est une base $\mathbb{R}^2$ pour tous $i \neq j$ dans $[\![1,3]\!]$. On considère l'application

$$\Psi : T \to \mathbb{S}_3$$

qui associe à $\phi \in T \subseteq \mathsf{GL}(\mathbb{R}^2)$ la seule bijection $\sigma \in \mathbb{S}_3$ satisfaisant $\phi(A_i) = A_{\sigma(i)}$ pour $i \in [\![1,3]\!]$. C'est facile à vérifier que Ψ est un morphisme de groupes, car

$$(\phi' \circ \phi)(A_i) = \phi'(A_{\Psi(\psi)(i)}) = A_{\Psi(\psi')(\Psi(\phi)(i))} = A_{(\Psi(\psi') \circ \Psi(\phi))(i)}$$

pour $i \in [\![1,3]\!]$. Comme $\{A_1, A_2\}$ est une base de $\mathbb{R}^2$, Ψ est injective, car $\Psi(\phi) = \mathsf{id}_{[\![1,3]\!]}$, veut dire que $\phi(A_i) = A_i$ pour $i \in \{1,2\}$. En outre, Ψ est clairement surjective, car donné $\sigma \in \mathbb{S}_3$, il existe une unique application linéaire $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ telle que $\phi(A_i) = A_{\sigma(i)}$ pour $i \in \{1,2\}$. Comme σ est bijectif, ϕ l'est aussi, *i.e.* $\phi \in \mathsf{GL}(\mathbb{R}^2)$, tandis que $A_i = -A_j - A_k$, pour $\{i,j,k\} = [\![1,3]\!]$ nous dit que $\phi \in T$, car

$$\phi(A_3) = \phi(-A_1 - A_2) = -\phi(A_1) - \phi(A_2) = -A_{\sigma(1)} - A_{\sigma(2)} = A_{\sigma(3)}.$$

C'est clair que $\Psi(\phi) = \sigma$.

13. (*a*) Soient E un ensemble, G un groupe et $\phi : E \to G$ une bijection. Montrer que l'on peut définir une loi de groupe sur E par

$$a * b = \phi^{-1}\big(\phi(a)\phi(b)\big),$$

pour tous $a, b \in E$. Que peut-on dire alors de l'application ϕ ?

(*b*) Soit X un ensemble. On munit $\{0,1\}$ de l'addition modulo 2, notée $\oplus$. On note encore $\oplus$ l'addition sur $\{0,1\}^X$ définie par $(f \oplus g)(x) = f(x) \oplus g(x)$, pour tous $f, g \in \{0,1\}^X$ et $x \in X$. On rappelle que, à toute partie A de X, on associe sa fonction indicatrice $\mathbf{1}_A : X \to \{0,1\}$ définie par $\mathbf{1}_A(x) = 1$ si $x \in A$, et $\mathbf{1}_A(x) = 0$ si $x \in X \setminus A$. Montrer que l'application $\Phi : \mathscr{P}(X) \to \{0,1\}^X$ donnée par $\Phi(A) = \mathbf{1}_A$ est une bijection, et que la loi de groupe induite sur $\mathscr{P}(X)$ par transport de structure est la différence symétrique.

Solution.

(*a*) C'est clair que la loi $*$ est associative car

$$\begin{aligned}(a * b) * c &= \phi^{-1}\big(\phi(a)\phi(b)\big) * c = \phi^{-1}\Big(\big(\phi(a)\phi(b)\big)\phi(c)\Big)\phi^{-1}\Big(\phi(a)\big(\phi(b)\phi(c)\big)\Big) \\ &= a * \phi^{-1}\big(\phi(b)\phi(c)\big) = a * (b * c),\end{aligned}$$

pour tous $a, b, c \in E$. En plus l'élément $e = \phi^{-1}(1_G)$ est le neutre de $(E, *)$, vu que

$$\begin{aligned}a * e &= \phi^{-1}\big(\phi(a)\phi(e)\big) = \phi^{-1}\big(\phi(a)1_G\big) = \phi^{-1}\big(\phi(a)\big) = a \\ &= \phi^{-1}\big(1_G\phi(a)\big) = \phi^{-1}\big(\phi(e)\phi(a)\big) = e * a.\end{aligned}$$

Finalement, étant donné $a \in E$, $\phi^{-1}(\phi(a)^{-1})$ est l'inverse de a, car

$$\begin{aligned}a * \phi^{-1}(\phi(a)^{-1}) &= \phi^{-1}\big(\phi(a)\phi(a)^{-1}\big) = \phi^{-1}(1_G) = e \\ &= \phi^{-1}\big(\phi(a)^{-1}\phi(a)\big) = \phi^{-1}(\phi(a)^{-1}) * a.\end{aligned}$$

La définition de la loi $*$ implique directement que l'application ϕ est un isomorphisme de groupes.

(*b*) Soit $\Psi : \{0,1\}^X \to \mathscr{P}(X)$ l'application donnée par $\Psi(f) = f^{-1}(\{1\})$. On voit bien que

$$(\Psi \circ \Phi)(A) = \Psi(\mathbf{1}_A) = \mathbf{1}_A^{-1}(\{1\}) = A,$$

pour tout $A \in \mathscr{P}(X)$, *i.e.* $\Psi \circ \Phi = \mathsf{id}_{\mathscr{P}(X)}$, et

$$(\Phi \circ \Psi)(f) = \Phi\big(f^{-1}(\{1\})\big) = \mathbf{1}_{f^{-1}(\{1\}} = f,$$

pour tout $f \in \{0,1\}^X$, *i.e.* $\Phi \circ \Psi = \mathsf{id}_{\{0,1\}^X}$. En conséquence, Φ est une bijection, avec réciproque Ψ.

En outre, la loi $*$ définie par transport de structures est donnée par

$$\begin{aligned}A * B &= \Psi\big(\Phi(A) \oplus \Phi(B)\big) = \Psi(\mathbf{1}_A \oplus \mathbf{1}_B) = (\mathbf{1}_A \oplus \mathbf{1}_B)^{-1}(\{1\}) \\ &= \{x \in X : \mathbf{1}_A(x) \oplus \mathbf{1}_B(x) = 1\} \\ &= \{x \in X : \mathbf{1}_A(x) = 1 \text{ et } \mathbf{1}_B(x) = 0, \text{ ou } \mathbf{1}_A(x) = 0 \text{ et } \mathbf{1}_B(x) = 1\} \\ &= (A \setminus B) \cup (B \setminus A) = A \ominus B,\end{aligned}$$

pour tous $A, B \in \mathscr{P}(X)$, où $A \ominus B$ dénote la différence symmétrique de A et B.

14. On veut montrer que tout sous-groupe de $\mathbb{R}$ est soit dense dans $\mathbb{R}$, soit de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}_{\geq 0}$. On prend donc G un sous-groupe de $\mathbb{R}$ différent de $\{0\} = 0\mathbb{Z}$ et on pose $\alpha = \inf(G \cap \mathbb{R}_{>0})$.

(*a*) Montrer que $\alpha \in \mathbb{R}_{\geq 0}$.

(*b*) Montrer que si $\alpha = 0$, alors G est dense dans $\mathbb{R}$.

(*c*) Montrer que si $\alpha > 0$, alors $G = \alpha\mathbb{Z}$.

Solution.

(*a*) Comme $G \setminus \{0\} \neq \emptyset$ il existe $x \in G$ non nul. Si $x > 0$, alors $G \cap \mathbb{R}_{>0} \neq \emptyset$, car $x \in G \cap \mathbb{R}_{>0}$. Si $x < 0$, alors $-x \in G \cap \mathbb{R}_{>0}$, vu que G est un groupe, ce qui nous dit que $G \cap \mathbb{R}_{>0} \neq \emptyset$. En conséquence, $G \cap \mathbb{R}_{>0} \neq \emptyset$, ce qui implique que $\alpha = \inf(G \cap \mathbb{R}_{>0})$ existe, d'après la complétude $\mathbb{R}$. En plus, comme $G \cap \mathbb{R}_{>0} \subseteq \mathbb{R}_{\geq 0}$ et $\mathbb{R}_{\geq 0}$ est fermé, on conclut que $\alpha \in \mathbb{R}_{\geq 0}$.

(*b*) Il suffit de montrer que, étant donné $y \in \mathbb{R}$ et $\epsilon > 0$ il existe $x \in G$ tel que $|x - y| \leq \epsilon$. Comme $\alpha = 0$, il existe $x' \in G \cap \mathbb{R}_{>0}$ tel que $x' < \epsilon$. Or,

$$\mathbb{R} = \bigcup_{n \in \mathbb{Z}} [nx', (n+1)x']$$

nous dit qu'il existe $n \in \mathbb{Z}$ tel que $nx' \leq y \leq (n+1)x'$. En effet, il suffit de prendre $n = \lfloor y/x \rfloor$. Soit $x = nx'$. Noter que $x \in G$, vu que $x' \in G$. On conclut que $|y - x| = y - x \leq x' < \epsilon$, comme on voulait démontrer.

(*c*) On remarque d'abord que $\alpha \in G$. En effet, si $\alpha \notin G$, il existe une suite strictément décroissante $(x_n)_{n \in \mathbb{N}} \in (G \cap \mathbb{R}_{>0})^{\mathbb{N}}$ qui converge vers α. Cela nous dit que la suite $(x_n - x_{n+1})_{n \in \mathbb{N}} \in (G \cap \mathbb{R}_{>0})^{\mathbb{N}}$ converge vers 0, *i.e.* $\alpha = 0$. Comme $\alpha > 0$, on conclut que $\alpha \in G$. En conséquence, $\alpha\mathbb{Z} \subseteq G$. On montrera l'inclusion $G \subseteq \alpha\mathbb{Z}$. Soit $x \in G$. Alors, il existe $n \in \mathbb{Z}$ tel que $0 \leq x - n\alpha < \alpha$. Comme $\alpha \in G$, on voit bien que $x - n\alpha \in G$. Si $x - n\alpha \neq 0$, alors $x - n\alpha \in G \cap \mathbb{R}_{>0}$ ce qui nous dit que $x - n\alpha < \alpha$, qui est absurde. En conséquence, $x - n\alpha = 0$, *i.e.* $x \in \alpha\mathbb{Z}$. En conclusion, $G = \alpha\mathbb{Z}$.

15. Soit G un sous-groupe fini du groupe multiplicatif $\mathbb{C}^*$. On considère le sous-groupe de $\mathbb{C}^*$ donné par $\mathsf{U}(1) = \{z \in \mathbb{C}^* : |z| = 1\}$ et l'application $f : \mathbb{R} \to \mathsf{U}(1)$ donnée par $f(t) = e^{2\pi i t}$.

(*a*) Montrer que G est un sous-groupe du groupe $\mathsf{U}(1)$.

(*b*) Montrer que $f^{-1}(G)$ est un sous-groupe de $\mathbb{R}$ qui contient $\mathbb{Z}$.

(*c*) Montrer que $f^{-1}(G)$ n'est pas dense dans $\mathbb{R}$.

(*d*) En déduire que $f^{-1}(G)$ est de la forme $n^{-1}\mathbb{Z}$ avec $n \in \mathbb{N}^*$.

(*e*) En déduire que G est un groupe cyclique d'ordre n.

Solution.

(*a*) Il faut montrer que $G \subseteq \mathsf{U}(1)$, *i.e.* $|z| = 1$ pour tout $z \in G$. Si ce n'est pas le cas, il existe $z_0 \in G$ tel que $|z_0| \neq 1$. On considère le sous-groupe $\langle z \rangle = \{z^k : k \in \mathbb{Z}\} \subseteq G$ engendré par z. On affirme que l'application $\imath : \mathbb{Z} \to \langle z \rangle$ qui associe z^k à $k \in \mathbb{Z}$ est injective. En effet, si ce n'est pas le cas, il existe $j, k \in \mathbb{Z}$ tels que $j < k$ et $z^j = z^k$, ce qui implique que $z^{k-j} = 1$ et en particulier $|z|^{k-j} = 1$, *i.e.* $|z| = 1$, ce qui est absurde. Or, comme l'application $\imath$ est injective, son image est infinie et *a fortiori* G est infini, ce qui est absurde. On conclut que $G \subseteq \mathsf{U}(1)$.

(*b*) On rappelle que, étant donné un morphisme de groupes $f : G \to G'$ et H' un sous-groupe de G', $f^{-1}(H')$ est un sous-groupe de G contenant le noyau $\mathsf{Ker}(f)$ de f. En effet, comme $f(1_G) = 1_{G'} \in H$, $1_G \in f^{-1}(H')$, tandis que, étant donnés $x, y \in f^{-1}(H')$, $f(x^{-1}y) = f(x)^{-1}f(y) \in H'$ nous dit que $x^{-1}y \in f^{-1}(H')$. L'inclusion $\mathsf{Ker}(f) \subseteq f^{-1}(H')$ suit directement du fait que, si $f : X \to Y$ est une application alors $B \subseteq B' \subseteq Y$ implique que $f^{-1}(B) \subseteq f^{-1}(B')$. En effet, comme H' est un sous-groupe de G', $\{1_{G'}\} \subseteq H'$, ce qui implique que $\mathsf{Ker}(f) = f^{-1}(\{1_{G'}\}) \subseteq f^{-1}(H')$. Dans ce cas, l'application $f : \mathbb{R} \to \mathsf{U}(1)$ est clairement un morphisme de groupes et son noyau est précisément $\mathbb{Z}$, ce qui nous dit que $f^{-1}(G)$ est un sous-groupe de $\mathbb{R}$ incluant $\mathbb{Z}$.

(*c*) On rappelle qu'une application $f : X \to Y$ entre deux espaces topologiques est continue si et seulement si $f(\bar{E}) \subseteq \overline{f(E)}$ pour tout $E \subseteq X$. Cela implique que, si f est surjectif et $E \subseteq X$ est dense, alors $f(E)$ est dense en Y, vu que $Y = f(X) = f(\bar{E}) \subseteq \overline{f(E)} \subseteq Y$. On remarque que l'application $f : \mathbb{R} \to \mathsf{U}(1)$ est clairement continue et surjective. Cela nous dit en particulier que $f(f^{-1}(G)) = G$. Si $E = f^{-1}(G) \subseteq \mathbb{R}$ est dense, alors $f(E) = f(f^{-1}(G)) = G$ est dense dans $\mathsf{U}(1)$. Or, comme G est fini et $\mathsf{U}(1)$ est Hausdorff, G est fermé, ce qui implique que

$$G = \bar{G} = \overline{f(f^{-1}(G))} = \mathsf{U}(1),$$

qui est absurde, vu que G est fini mais $\mathsf{U}(1)$ n'est pas fini.

(*d*) D'après l'exercice **14**, $f^{-1}(G) = \alpha\mathbb{Z}$, pour $\alpha \in \mathbb{R}_{>0}$. Comme $\mathbb{Z} \subseteq \alpha\mathbb{Z}$, il existe $n \in \mathbb{Z}$ tel que $1 = \alpha n$. La condition $\alpha > 0$ implique que $n \in \mathbb{N}^*$, et en conséquence $\alpha = 1/n$ pour $n \in \mathbb{N}^*$. On conclut que $f^{-1}(G) = n^{-1}\mathbb{Z}$ avec $n \in \mathbb{N}^*$.

(*e*) Comme f est surjective,

$$G = f(f^{-1}(G)) = f(n^{-1}\mathbb{Z}) = \left\{e^{\frac{2\pi i k}{n}} : k \in \mathbb{Z}\right\}$$

est le groupe cyclique engendré par $z = e^{2\pi i/n}$. Comme $z = e^{2\pi i/n}$ a ordre n, vu que $z^n = e^{2\pi i} = 1$ et $z^m = e^{2\pi i m/n} \neq 1$ pour tout $m \in [\![1, m-1]\!]$, G est un groupe cyclique d'ordre n.

16. Soient a et b dans $\mathbb{N}^*$.

(*a*) Soit f l'application de $\mathbb{Z}$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ définie par $f(k) = (k+a\mathbb{Z}, k+b\mathbb{Z})$. Montrer que f est un morphisme de groupes. Déterminer $\mathsf{Ker}(f)$.

(*b*) En déduire que si a et b sont premiers entre eux, le groupe $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Qu'en est-il dans le cas contraire ?

(*c*) Lorsque a et b sont premiers entre eux, expliciter l'isomorphisme réciproque en utilisant une relation de Bézout. On pourra commencer par chercher les images réciproques de $(1 + a\mathbb{Z}, 0 + b\mathbb{Z})$ et de $(0 + a\mathbb{Z}, 1 + b\mathbb{Z})$.

Solution.

(*a*) Comme $f(k + k') = (k + k' + a\mathbb{Z}, k + k' + b\mathbb{Z}) = (k + a\mathbb{Z}, k + b\mathbb{Z}) + (k' + a\mathbb{Z}, k' + b\mathbb{Z})$, pour tous $k, k' \in \mathbb{Z}$, f est un morphisme de groupes. En plus, c'est clair que

$$\mathsf{Ker}(f) = \{k \in \mathbb{Z} : a|k \text{ et } b|k\} = \mathsf{PPCM}(a, b)\mathbb{Z}.$$

(*b*) Si a et b sont premiers entre eux, alors $\mathsf{Ker}(f) = ab\mathbb{Z}$. En outre, dans ce cas f est surjectif. En effet, comme $\mathsf{PGCD}(a, b) = 1$ il existe $n, m \in \mathbb{Z}$ tels que $na + mb = 1$.

Étant donné $(k_a, k_b) \in \mathbb{Z}^2$, alors $(k_a - k_b)na + (k_a - k_b)mb = (k_a - k_b)$ implique que $k_a - (k_a - k_b)na = k_b + (k_a - k_b)ma$ et, en particulier, $f(k) = (k_a + a\mathbb{Z}, k_b + b\mathbb{Z})$ pour $k = k_a - (k_a - k_b)na$.

Si a et b ne sont pas premiers entre eux, f n'est pas forcément surjectif, comme on peut observer dans le cas où $a = b = 2$, vu que $\mathsf{Img}(f) = \{(2\mathbb{Z}, 2\mathbb{Z}), (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z})\}$ dans ce cas. En conséquence, f induit un isomorphime de groupes $\bar{f} : \mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. La/le lectrice/lecteur peut vérifier que f est aussi un morphisme d'anneaux, ce qui nous dit que $\bar{f}$ est un isomorphisme d'anneaux.

(*c*) Comme $\mathsf{PGCD}(a, b) = 1$ il existe $n, m \in \mathbb{Z}$ tels que $na + mb = 1$. On a montré dans la preuve de l'item précédent que l'application $\bar{g} : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/ab\mathbb{Z}$ qui associe $k_a - (k_a - k_b)na + ab\mathbb{Z} = k_b + (k_a - k_b)ma + ab\mathbb{Z}$ à $(k_a + a\mathbb{Z}, k_b + b\mathbb{Z})$ pour $k_a, k_b \in \mathbb{Z}$ est bien définie et la réciproque de $\bar{f}$.

17. Pour $1 \leq n \leq 17$, déterminer si le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique et donner une partie génératrice minimale.

Solution. On affirme d'abord que, pour $n \in [\![1, 17]\!]$, $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \neq 8, 12, 15, 16$. Si $n = 1$ ou $n = 2$, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ est la groupe trivial, qui est clairement cyclique. On suppose désormais que $n \geq 3$. D'une part on voit bien que

(i) $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ et tous les élements ont ordre inférieur ou égal à 2 ;
(ii) $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ et tous les élements ont ordre inférieur ou égal à 2 ;
(iii) $(\mathbb{Z}/15\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \overline{11}, \overline{13}, \overline{14}\}$ et tous les élements ont ordre inférieur ou égal à 4 ;
(iv) $(\mathbb{Z}/16\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{15}\}$ et tous les élements ont ordre inférieur ou égal à 4.

Cela nous dit que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique si $n \in \{8, 12, 15, 16\}$. On remarque que l'isomorphisme $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ obtenu dans l'exercice **16** induit un isomorphisme de groupes $(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, qui implique aussi que $(\mathbb{Z}/15\mathbb{Z})^\times$ n'est pas cyclique, d'après l'exercice **6**. Finalement, pour montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique pour $n \in [\![3, 17]\!] \setminus \{8, 12, 15, 16\}$ on indiquera un générateur du groupe, mais on laisse la vérification à la/au lectrice/lecteur. En effet, la/le lectrice/lecteur peut vérifier que $\bar{2}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \{3, 5, 9, 11, 13\}$, $\bar{3}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \{4, 7, 10, 14, 17\}$ et $\bar{5}$ est un générateur de $(\mathbb{Z}/6\mathbb{Z})^\times$.

De façon générale, on remarque que $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique. Pour cela, on va montrer d'abord que, si $\mathscr{G}_d$ dénote l'ensemble de générateurs d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$, pour $d \in \mathbb{N}^*$ diviseur de $p - 1$, alors $\#(\mathscr{G}_d) \in \{0, \varphi(d)\}$. Noter que par définition, $\mathscr{G}_d \subseteq \mathsf{Z}(P) = \{\alpha \in \mathbb{Z}/p\mathbb{Z} : P(\alpha) = 0\}$, où $P = X^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[X]$, et $\#(\mathsf{Z}(P)) \leq d$. Si $\mathscr{G}_d \neq \emptyset$, soit $a \in \mathscr{G}_d$. Comme le polynôme P s'annule sur l'ensemble $\langle a \rangle = \{1, a, \ldots, a^{d-1}\} \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ de cardinal d, alors $Z(P) = \langle a \rangle$. En outre, d'après l'exercice **4**, (d), $\#(\mathscr{G}_d) \geq \#(\{g \in \langle a \rangle : g \text{ est générateur }\}) = \varphi(d)$, ce qui implique que $\#(\mathscr{G}_d) = \varphi(d)$. En conséquence, $\#(\mathscr{G}_d) \in \{0, \varphi(d)\}$. Comme

$$(\mathbb{Z}/p\mathbb{Z})^\times = \bigsqcup_{\substack{d \in \mathbb{N}^* \\ d|(p-1)}} \mathscr{G}_d,$$

et $\#(\mathscr{G}_d) \in \{0, \varphi(d)\}$ pour tout $d \in \mathbb{N}^*$ diviseur de $p - 1$, on trouve que

$$p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times| = \sum_{\substack{d \in \mathbb{N}^* \\ d|(p-1)}} \#(\mathscr{G}_d) \leq \sum_{\substack{d \in \mathbb{N}^* \\ d|(p-1)}} \varphi(d) = p - 1,$$

d'après l'exercice **4**, (e). Cela implique que $\#(\mathscr{G}_d) \neq 0$ et, en particulier, $\#(\mathscr{G}_d) = \varphi(d)$, pour tout $d \in \mathbb{N}^*$ diviseur de $p-1$. En particulier, $\#(\mathscr{G}_{p-1}) = \varphi(p-1) \neq 0$, et $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique.

De façon encore plus générale, un théorème de Gauss dit que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si n est de la forme 1, 2, 4, p^k ou $2p^k$, pour $p \in \mathbb{N}^*$ premier impair et $k \in \mathbb{N}^*$. La preuve utilise l'isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_\ell^{r_\ell}\mathbb{Z})^\times$$

induit par l'isomorphisme de l'exercice **16**, où $n = p_1^{r_1} \dots p_\ell^{r_\ell}$, avec $p_1, r_1, \dots, p_\ell, r_\ell \in \mathbb{N}^*$ et $p_1, \dots, p_\ell$ premiers distincts, ainsi que les isomorphismes de groupes

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)p^{r-1}\mathbb{Z} \qquad \text{et} \qquad (\mathbb{Z}/2^s\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$$

pour tous $r, s \in \mathbb{N}^*$ avec $s \geq 3$.

18. Soient $(G, \cdot)$ et $(G', \cdot)$ deux groupes et A une partie génératrice de $(G, \cdot)$.

(*a*) Montrer que si deux morphismes de groupes de $(G, \cdot)$ dans $(G', \cdot)$ coïncident sur A, ils sont égaux.

(*b*) Montrer que si un élément $g \in G$ commute avec tous les éléments de A, alors il appartient au centre de G.
Indication : utiliser l'automorphisme intérieur associé à g.

Solution.

(*a*) Soient $f_1, f_2 : G \to G'$ deux mosphismes de groupes qui coïncident sur A. On considère l'ensemble

$$H = \{g \in G : f_1(g) = f_2(g)\} \subseteq G.$$

Par hypothèse, $A \subseteq H$. En plus, on voit bien que H est un sous-groupe de G, car $f_1(1_G) = 1_{G'} = f_2(1_G)$ nous dit que $1_G \in H$ et si $g, g' \in H$, alors

$$f_1(g'g^{-1}) = f_1(g')f_1(g)^{-1} = f_2(g')f_2(g)^{-1} = f_2(g'g^{-1})$$

implique que $g'g^{-1} \in H$. Comme $G = \langle A \rangle$ est le plus petit sous-groupe de G contenant A, on conclut que $G \subseteq H$, ce qui nous dit que $H = G$.

(*b*) Soit $\delta_g : G \to G$ le morphisme de groupes qui associe ghg^{-1} à $h \in G$. Les morphismes de groupes δ_g et id_G coïncident sur A, ce qui nous dit que $\delta_g = \mathsf{id}_G$, ce qui nous dit que $ghg^{-1} = h$ pour tout $h \in G$, *i.e.* $gh = hg$ pour tout $h \in G$. On conclut que g appartient au centre de G.

19. Soit $(G, \cdot)$ un groupe et $n \in \mathbb{N}^*$.

(*a*) Quels sont les morphismes de groupes de $(\mathbb{Z}, +)$ dans $(G, \cdot)$? Les endomorphismes de $(\mathbb{Z}, +)$? Les automorphismes de $(\mathbb{Z}, +)$?

(*b*) Quels sont les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(G, \cdot)$? Les endomorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$? Les automorphismes de $(\mathbb{Z}/n\mathbb{Z}, +)$?

(*c*) Quels sont les morphismes de groupes de $(\mathbb{Z}^2, +)$ dans $(G, \cdot)$? Les endomorphismes de $(\mathbb{Z}^2, +)$? Les automorphismes de $(\mathbb{Z}^2, +)$?

Solution.

(*a*) Étant donné deux groupes G et G' on notera $\mathsf{Mor}_{\mathsf{Gr}}(G, G')$ l'ensemble de morphismes de groupes de G dans G'. On affirme que l'application

$$\mathsf{ev}_1 : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, G) \to G$$

qui associe $\phi(1)$ à $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, G)$ est une bijection. D'une part, ev_1 est injectif, car, étant donné $\phi, \psi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, G)$ tels que $\phi(1) = \psi(1)$, alors $\phi = \psi$, d'après l'exercice **18**, vu que $A = \{1\}$ est un générateur de $\mathbb{Z}$. D'une autre part, ev_1 est surjectif puisque, étant donné $g \in G$, l'application $f_g : \mathbb{Z} \to G$ donnée par $f_g(n) = g^n$ pour tout $n \in \mathbb{Z}$ est un morphisme de groups tel que $\mathsf{ev}_1(f_g) = g$. On en déduit que $\mathsf{ev}_1 : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, \mathbb{Z}) \to \mathbb{Z}$ est une bijection.

Finalement, on affirme que $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, \mathbb{Z})$ est un automorphisme si et seulement si $\mathsf{ev}_1(\phi) = \phi(1) \in \{\pm 1\}$. En effet, on remarque d'abord que tout morphisme non nul $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, \mathbb{Z})$ est injectif, car $\phi(n) = \phi(m)$ pour $n, m \in \mathbb{Z}$ nous dit que $n\phi(1) = \phi(n) = \phi(m) = m\phi(1)$, ce qui implique $n = m$, vu que $\mathsf{ev}_1(\phi) = \phi(1) \neq 0$ précisément si ϕ est non nul. Le résultat affirmé suit maintenant du fait que ϕ est un surjectif si et seulement si $\phi(1)$ est un générateur de $\mathbb{Z}$ et les seuls générateurs de $\mathbb{Z}$ sont -1 et 1.

(*b*) Comme la projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est surjective, l'application

$$\pi^* : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, G) \to \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, G)$$

qui associe $\psi \circ \pi$ à $\psi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, G)$ est injective. En plus, d'après le premier théorème d'isomorphisme, l'image de π^* est précisément

$$\{\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}, G) : n\mathbb{Z} \subseteq \mathsf{Ker}(\phi)\}.$$

En conséquence, l'application

$$\mathsf{ev}_{\bar{1}} = \mathsf{ev}_1 \circ \pi^* : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, G) \to G$$

est injective et son image est donnée par le sous-groupe $G_{\leq n} = \{g \in G : g^n = 1_G\}$ de G, *i.e.*

$$\mathsf{ev}_{\bar{1}} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, G) \to G_{\leq n}$$

est une bijection. Cela nous donne en particulier une bijection $\mathsf{ev}_{\bar{1}} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$, vu que tout élément $\bar{m}$ de $\mathbb{Z}/n\mathbb{Z}$ satisfait que $n\bar{m} = \bar{0}$.

Finalement, on affirme que $\psi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ est un automorphisme si et seulement si $\mathsf{ev}_{\bar{1}}(\psi) = \psi(\bar{1})$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$, ce qui équivaut à dire que $\psi(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^\times$. En effet, comme $\mathbb{Z}/n\mathbb{Z}$ est fini, $\psi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ est un automorphisme si et seulement si ψ est surjectif, ce qui équivaut au fait que $\mathsf{ev}_{\bar{1}}(\psi) = \psi(\bar{1})$ soit un générateur de $\mathbb{Z}/n\mathbb{Z}$.

(*c*) On affirme que l'application

$$\mathsf{ev}_{1,1} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, G) \to G \times G$$

qui associe $(\phi(1,0), \phi(0,1))$ à $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, G)$ est une injection. En effet, $\mathsf{ev}_{1,1}$ est injectif, car, étant donné $\phi, \psi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^1, G)$ tels que $\phi(1,0) = \psi(0,1)$, alors $\phi = \psi$, d'après l'exercice **18**, vu que $A = \{(1,0), (0,1)\}$ est un ensemble de générateurs de $\mathbb{Z}^2$.

En plus, l'image de $\mathsf{ev}_{1,1}$ est précisément $C_2(G) = \{(g_1, g_2) \in G \times G : g_1 g_2 = g_2 g_1\}$. En effet, si $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, G)$ et $\mathsf{ev}_{1,1}(\phi) = (g_1, g_2)$, alors

$$\begin{aligned} g_1 g_2 &= \phi(1,0)\phi(0,1) = \phi\big((1,0)+(0,1)\big) = \phi(1,1) \\ &= \phi\big((0,1)+(1,0)\big) = \phi(0,1)\phi(1,0) = g_2 g_1 \end{aligned}$$

nous dit que $\mathsf{ev}_{1,1}(\phi) \in C_2(G)$. En plus étant donné $(g_1, g_2) \in C_2(G)$, l'application $f_{g_1,g_2} : \mathbb{Z}^2 \to G$ donnée par $f_{g_1,g_2}(n_1, n_2) = g_1^{n_1} g_2^{n_2}$ pour tous $n_1, n_2 \in \mathbb{Z}$ est un morphisme de groups tel que $\mathsf{ev}_{1,1}(\phi) = (g_1, g_2)$. En conclusion, on a construit la bijection

$$\mathsf{ev}_{1,1} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, G) \to C_2(G).$$

On en déduit que $\mathsf{ev}_{1,1} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, \mathbb{Z}^2) \to \mathbb{Z}^2 \times \mathbb{Z}^2$ est une bijection. On considère la bijection $\Phi : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathsf{M}_2(\mathbb{Z})$ qui associe la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à $((a,c),(b,d)) \in \mathbb{Z}^2 \times \mathbb{Z}^2$ et soit $\Psi = \Phi \circ \mathsf{ev}_{1,1} : \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, \mathbb{Z}^2) \to \mathsf{M}_2(\mathbb{Z})$. On affime que Ψ satisfait que $\Psi(\phi' \circ \phi) = \Psi(\phi') \cdot \Psi(\phi)$ pour tous $\phi, \phi' \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, \mathbb{Z}^2)$, où $\cdot$ dénote le produit matriciel. En effet, si

$$\Psi(\phi') = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \text{ et } \Psi(\phi) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

on voit bien que

$$(\phi' \circ \phi)(1,0) = \phi'(a,c) = a\phi'(1,0) + c\phi'(0,1) = (a'a + b'c, c'a + d'c)$$

et

$$(\phi' \circ \phi)(0,1) = \phi'(b,d) = b\phi'(1,0) + d\phi'(0,1) = (a'b + b'd, c'b + d'd),$$

ce qui implique que $\Psi(\phi' \circ \phi) = \Psi(\phi') \cdot \Psi(\phi)$. Cette identité nous dit que $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, \mathbb{Z}^2)$ est un automorphisme si et seulement si $\Psi(\phi) \in \mathsf{M}_2(\mathbb{Z})$ est une matrice inversible dans $\mathsf{M}_2(\mathbb{Z})$, ce qui équivaut à dire que $\det(\Psi(\phi)) = ad - bc \in \{\pm 1\}$, d'après le théorème de Cramer. En conséquence, $\phi \in \mathsf{Mor}_{\mathsf{Gr}}(\mathbb{Z}^2, \mathbb{Z}^2)$ est un automorphisme si et seulement si $\Psi(\phi) \in \mathsf{SL}_2(\mathbb{Z}) \cup \mathsf{SL}_2(\mathbb{Z}) \cdot E$, où

$$E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

20. Soient G et G' deux groupes isomorphes, et f un isomorphisme de G dans G'. On note $\mathsf{Aut}_{\mathsf{Gr}}(G)$ le groupe des automorphismes du groupe G. On considère l'application $\mathsf{Ad}_f : \mathsf{Aut}_{\mathsf{Gr}}(G) \to \mathsf{Aut}_{\mathsf{Gr}}(G')$ donnée par $\mathsf{Ad}_f(\varphi) = f \circ \varphi \circ f^{-1}$, pour tout $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$. Montrer que Ad_f est un isomorphisme de groupes.

Solution. C'est clair que Ad_f est un morphisme de groupes, car

$$\mathsf{Ad}_f(\varphi' \circ \varphi) = f \circ \varphi' \circ \varphi \circ f^{-1} = f \circ \varphi' \circ f^{-1} \circ f \circ \varphi \circ f^{-1} = \mathsf{Ad}_f(\varphi') \circ \mathsf{Ad}_f(\varphi),$$

pour tous $\varphi, \varphi' \in \mathsf{Aut}_{\mathsf{Gr}}(G)$. En outre, on voit bien que $\mathsf{Ad}_f \circ \mathsf{Ad}_{f^{-1}} = \mathsf{id}_{\mathsf{Aut}_{\mathsf{Gr}}(G')}$ et $\mathsf{Ad}_{f^{-1}} \circ \mathsf{Ad}_f = \mathsf{id}_{\mathsf{Aut}_{\mathsf{Gr}}(G)}$. On vérifie la dernière identité, vu que la première suit de remplacer

f par f^{-1}. Or,

$$(\mathsf{Ad}_{f^{-1}} \circ \mathsf{Ad}_f)(\varphi) = \mathsf{Ad}_{f^{-1}}(f \circ \varphi \circ f^{-1}) = f^{-1} \circ f \circ \varphi \circ f^{-1} \circ f = \varphi$$

pour tout $\varphi \in \mathsf{Aut}_{\mathsf{Gr}}(G)$ nous dit que $\mathsf{Ad}_{f^{-1}} \circ \mathsf{Ad}_f = \mathsf{id}_{\mathsf{Aut}_{\mathsf{Gr}}(G)}$. En conséquence, Ad_f est un isomorphisme de groupes.

21. On considère le groupe additif $(\mathbb{Z}^2, +)$. Soient $u = (a, c) \in \mathbb{Z}^2$ et $v = (b, d) \in \mathbb{Z}^2$.

(a) À quelle condition a-t-on $\mathbb{Z}^2 = \langle u, v \rangle$?

(b) Soit $H = \{(x, y) \in \mathbb{Z}^2 : x + y \in 2\mathbb{Z}\}$.

(i) Montrer que H est un sous-groupe de $\mathbb{Z}^2$.

(ii) Donner une partie génératrice de H à deux éléments.

(iii) Déterminer $\mathbb{Z}^2/H$.

(c) On suppose que $ad - bc \neq 0$ et on note $H = \langle u, v \rangle$.

(i) Soit $P = \{\alpha u + \beta v : 0 \leq \alpha < 1,\ 0 \leq \beta < 1\}$. Établir une bijection entre $P \cap \mathbb{Z}^2$ et $\mathbb{Z}^2/H$.

(ii) On prend $u = (1, 4)$ et $v = (2, 3)$. Déterminer l'ordre du groupe $\mathbb{Z}^2/H$.

Solution.

(a) Soit

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{M}_2(\mathbb{Z}).$$

On voit bien que $\mathbb{Z}^2 = \langle u, v \rangle$ si et seulement s'il existe une matrice $M' \in \mathsf{M}_2(\mathbb{Z})$ telle que $M'M = I_2$, où $I_2 \in \mathsf{M}_2(\mathbb{Z})$ est la matrice identité. Si l'on applique le déterminant à la identité précédente on conclut que $\mathsf{det}(M')\mathsf{det}(M) = 1$, qui implique que $\mathsf{det}(M) \in \mathbb{Z}$ est inversible, *i.e.* $\mathsf{det}(M) \in \{\pm 1\}$. Réciproquement, si $\mathsf{det}(M) \in \{\pm 1\}$, la formule de Cramer nous dit que M est une matrice inversible dans $\mathsf{M}_2(\mathbb{Z})$, ce qui implique qu'il existe $M' \in \mathsf{M}_2(\mathbb{Z})$ telle que $M'M = I_2$. En conséquence, $\mathbb{Z}^2 = \langle (a, c), (b, d) \rangle$ si et seulement si $\mathsf{det}(M) = ad - bc = \pm 1$.

(b) (i) On considère l'application

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z}$$

qui associe la classe de $x + y$ dans $\mathbb{Z}/2\mathbb{Z}$ à $(x, y) \in \mathbb{Z}^2$. C'est facile à vérifier que ϕ est un morphisme de groupes, car

$$\begin{aligned} \phi\big((x, y) + (x', y')\big) = \phi(x + x', y + y') &= \overline{x + x' + y + y'} \\ &= \overline{x + y} + \overline{x' + y'} = \phi(x, y) + \phi(x', y'), \end{aligned}$$

pour tous $x, y, x', y' \in \mathbb{Z}$. En plus, $H = \mathsf{Ker}(\phi)$, par définition. En conséquence, H est un sous-groupe de $\mathbb{Z}^2$.

(ii) On affirme que H est engendré par $w_1 = (1, -1)$ et $w_2 = (0, 2)$. En effet, on voit bien que $w_1, w_2 \in H$. En plus, étant donné $(x, y) \in H$, on voit que

$$(x, y) = x(1, -1) + \frac{x + y}{2}(0, 2) = xw_1 + \frac{x + y}{2} w_2.$$

Noter que le coefficient devant w_2 est entier car $(x, y) \in H$. En conséquence, $S = \{w_1, w_2\}$ est une partie génératrice de H.

(iii) Comme $\phi(0,0) = \bar{0}$ et $\phi(1,0) = \bar{1}$, le morphisme de groupes $\phi : \mathbb{Z}^2 \to \mathbb{Z}/2\mathbb{Z}$ est surjectif. Le premier théorème d'isomorphisme nous dit alors que ϕ induit un isomorphisme de groupes $\bar{\phi} : \mathbb{Z}^2/H \to \mathbb{Z}/2\mathbb{Z}$, vu que $H = \mathsf{Ker}(\phi)$.

(*c*) (i) On considère l'application

$$F : P \cap \mathbb{Z}^2 \to \mathbb{Z}^2/H$$

donnée par la composition de l'inclusion de $P \cap \mathbb{Z}^2$ dans $\mathbb{Z}^2$ et la projection canonique $\mathbb{Z}^2 \to \mathbb{Z}^2/H$. On affirme que F est une bijection.

On montrera d'abord que F est un application injective. Étant donné $(x,y) = \alpha u + \beta v$ et $(x',y') = \alpha' u + \beta' v$ dans $P \cap \mathbb{Z}^2$, $F(x,y) = F(x',y')$ équivaut à dire que $(x-x', y-y') = (\alpha-\alpha')u + (\beta-\beta')v \in H$, *i.e.* il existe $n, m \in \mathbb{Z}$ tels que $(\alpha-\alpha')u + (\beta-\beta')v = nu + mv$. Comme $\{u, v\}$ est une base de $\mathbb{R}^2$, car $ad - bc \neq 0$, on conclut que $\alpha - \alpha' = n$ et $\beta - \beta' = m$ sont des entiers. En outre, la condition $\alpha, \alpha', \beta, \beta' \in [0,1[$ nous dit alors que $\alpha = \alpha'$ et $\beta = \beta'$, *i.e.* $(x,y) = (x',y')$ et l'application F est bien injective.

On montrera finalement que F est une surjection. Étant donné $(x,y) \in \mathbb{Z}^2$, on peut écrire $(x,y) = \gamma u + \delta v$, avec $\gamma, \delta \in \mathbb{R}$, vu que $\{u, v\}$ est une base de $\mathbb{R}^2$, car $ad - bc \neq 0$. Soient $n = \lfloor \gamma \rfloor$ et $m = \lfloor \delta \rfloor$ les parties entières de γ et δ, respectivement, et $\alpha = \gamma - n$ et $\beta = \delta - m$. Noter que $\alpha, \beta \in [0,1[$, ce qui nous dit que $(\alpha u + \beta v) = (x,y) - (nu + mv) \in P$, tandis que $(x,y) = (nu + mv) + (\alpha u + \beta v)$ nous dit que $(\alpha u + \beta v) = (x,y) - (nu + mv) \in \mathbb{Z}^2$, *i.e.* $(\alpha u + \beta v) \in \mathbb{Z}^2 \cap P$. Comme $(nu + mv) \in H$, on conclut que $F(\alpha u + \beta v) = (x,y) + H$, ce qui nous dit que l'application F est surjective.

(ii) D'après l'item précédent, l'ordre du groupe $\mathbb{Z}^2/H$ coïncide avec le cardinal de $P \cap \mathbb{Z}^2$. On voit bien que $P \subseteq \mathbb{R}^2$ est l'enveloppe convexe de $S = \{\mathbf{0}_{\mathbb{R}^2}, u, v, u+v\}$ (*i.e.* la intersection de tous les sous-ensembles convexes de $\mathbb{R}^2$ contenant S) privée des segments $[u, u+v] = \{tu + (1-t)(u+v) : t \in [0,1]\}$ et $[v, u+v] = \{tv + (1-t)(u+v) : t \in [0,1]\}$. Un calcul élémentaire nous dit que $P \cap \mathbb{Z}^2 = \{(0,0), (1,2), (1,3), (2,4), (2,5)\}$, ce qui implique que $\#(P \cap \mathbb{Z}^2) = 5$. En conséquence, $\mathbb{Z}^2/H$ a ordre 5.

22. Soit E un espace vectoriel euclidien de dimension $n \geq 3$. En utilisant le fait que les réflexions de E engendrent $\mathsf{O}(E)$, montrer que les renversements de E engendrent $\mathsf{SO}(E)$.
Indication : montrer que si u et v sont deux vecteurs unitaires orthogonaux, la composée des réflexions par rapport aux hyperplans $(\mathbb{R}u)^\perp$ et $(\mathbb{R}v)^\perp$ est un renversement. Puis montrer que pour deux vecteurs unitaires quelconques u_1 et u_2, la composée des réflexions par rapport aux hyperplans $(\mathbb{R}u_1)^\perp$ et $(\mathbb{R}u_2)^\perp$ est une composée de deux renversements.

Solution. On rappelle d'abord qu'une application linéaire $f : E \to E$ sur un espace vectoriel euclidien E de dimension n muni d'un produit scalaire $\langle , \rangle$ est une **isométrie (vectorielle)** si $\langle v, w \rangle = \langle f(v), f(w) \rangle$ pour tous $v, w \in E$. On rappelle aussi que, étant donné une décomposition orthogonal $E = F \oplus G$, la **symétrie orthogonale associée** est la seule application linéaire $s : E \to E$ qui satisfait que $s(F) = F$, $s(G) = G$, $s|_F = \mathsf{id}_F$ et $s|_G = -\mathsf{id}_G$. C'est clair que $s \in \mathsf{O}(E)$. On dit que s est une **réflexion** si $\mathsf{dim}(F) = n - 1$ et un **renversement** si $\mathsf{dim}(F) = n - 2$. D'après le théorème de Cartan-Dieudonné, tout élément $g \in \mathsf{O}(E)$ (resp., $g \in \mathsf{SO}(E)$) s'écrit comme une composition de k réflexions, avec $k \leq n$ (resp., et pair). Pour

démontrer l'énoncé de l'exercice il suffit de montrer que, étant donné deux réflexions s_1 et s_2, il existe deux renversement r_1 et r_2 tels que $s_1 \circ s_2 = r_1 \circ r_2$.

Si $s_1 = s_2$, alors $s_1 \circ s_2 = \mathsf{id}_E = r \circ r$, pour tout renversement r. On suppose désormais $s_1 \neq s_2$. Soient F_1 et F_2 les hyperespaces de E sur lesquels les restrictions de s_1 et de s_2 coïncident avec l'identité, respectivement. Comme s_i est uniquement determiné par F_i, on voit que $F_1 \neq F_2$. Soit $F = F_1 \cap F_2$ le sous-espace de E de dimension $n-2$. On choisit une base orthonormal $\mathscr{B} = \{e_1, \dots, e_n\}$ de E tel que $\bar{\mathscr{B}} = \{e_1, \dots, e_{n-2}\}$ soit base de F. On complète aussi $\bar{\mathscr{B}}$ en une base orthonormale $\mathscr{B}'_i = \{e_1, \dots, e_{n-2}, e'_{n-1,i}, e'_{n,i}\}$ de E tel que $\{e_1, \dots, e_{n-2}, e'_{n-1,i}\}$ soit une base de F_i pour $i = 1, 2$. On pose $s' : E \to E$ la seule application linéaire donnée par $s'(e_1) = -e_1$ et $s'(e_j) = e_j$ pour tout $j \in [\![2, n]\!]$. C'est clair que $s' \circ s' = \mathsf{id}_E$ et $s' \circ s_i = s_i \circ s'$ pour $i = 1, 2$. On définit finalement $r_i = s' \circ s_i$ pour $i = 1, 2$. La propriété de commutativité précédente nous dit que

$$r_1 \circ r_2 = s' \circ s_1 \circ s' \circ s_2 = s_1 \circ s' \circ s' \circ s_2 = s_1 \circ s_2.$$

En outre, c'est clair que r_i est un renversement pour $i = 1, 2$ associé à la décomposition orthogonale $F'_i \oplus G'_i$, où F'_i est engendré par $\{e_2, \dots, e_{n-2}, e'_{n-1,i}\}$.

23. On se propose de classifier les isométries vectorielles de $\mathbb{R}^3$. Soit f une isométrie de $\mathbb{R}^3$. On sait que f s'écrit comme la composée de k réflexions orthogonales avec $k \leq 3$.

(*a*) Quel est le déterminant de f dans chacun des cas ci-dessus ?

(*b*) Dans cette question, on suppose que $f = s_2 \circ s_1$, où s_1 et s_2 sont les réflexions orthogonales par rapport à des plans P_1 et P_2 avec $P_1 \neq P_2$. Ces deux plans se coupent selon une droite D.

(i) Vérifier que le plan orthogonal à D, noté $D^\perp$, est stable par f.

(ii) En déduire que l'endomorphisme induit par f sur ce plan est une rotation. On dit dans ce cas que f est une **rotation d'axe** D.

En déduire que toute isométrie directe de $\mathbb{R}^3$ est une rotation.

(*c*) Dans cette question, on suppose que $f = s_3 \circ s_2 \circ s_1$, où s_1 et s_2 et s_3 sont des réflexions orthogonales.

(i) Vérifier que $-f$ est une isométrie directe de $\mathbb{R}^3$. Dans la suite, on suppose que $f \neq -\mathsf{id}_{\mathbb{R}^3}$, donc $-f$ est une rotation autre que $\mathsf{id}_{\mathbb{R}^3}$. On note D son axe.

(ii) Soient r le renversement d'axe D et s la réflexion par rapport au plan $D^\perp$. Que valent $s \circ r$ et $r \circ s$? En déduire que soit $f = s$, soit f est le produit commutatif d'une rotation non triviale d'axe D avec s.

On appelle **antirotation d'axe** D toute isométrie qui s'écrit comme le produit (commutatif) d'une rotation non triviale d'axe D et de la réflexion orthogonale par rapport au plan $D^\perp$. En déduire que toute isométrie indirecte de $\mathbb{R}^3$ est soit une réflexion orthogonale, soit une antirotation.

(*d*) Déduire des questions précédentes la classification des isométries vectorielles de $\mathbb{R}^3$ en fonction de leurs vecteurs fixes.

Solution.

(*a*) Comme le déterminant d'un réflexion est -1, on conclut que si f est la composition de $k \leq 3$ réflexions, alors $\det(f) = (-1)^k$. On note que $k = 0$ si et seulement si $f = \mathrm{id}_{\mathbb{R}^3}$.

(*b*) Noter que $\det(f) = 1$ dans ce cas.

(i) On remarque d'abord que $f(D) = D$ et $f|_D = \mathrm{id}_D$. En effet, comme $s_i(P_i) = P_i$ et $s_i|_{P_i} = \mathrm{id}_{P_i}$ pour $i = 1, 2$, $f(v) = s_2 \circ s_1(v) = v \in D$ pour tout $v \in D$. Cela implique que $f(D^\perp) = D^\perp$. En effet, étant donné $v \in D$ et $w \in D^\perp$, comme f est une isométrie, on a que $0 = \langle v, w\rangle = \langle f(v), f(w)\rangle = \langle v, f(w)\rangle$. ce qui nous dit que $f(w) \in D^\perp$.

(ii) Comme f est une isométrie, $f|_{D^\perp} : D^\perp \to D^\perp$ l'est aussi, pour la restriction du produit scalaire de $\mathbb{R}^3$ à $D^\perp$. En plus, $\det(f|_{D^\perp}) = 1$, car $f|_D : D \to D$ coïncide avec l'identité de D et $\det(f) = 1$. En conséquence, $f|_{D^\perp} \in \mathrm{SO}(D^\perp)$.

À partir des items précédents on déduit que, pour tout $f \in \mathrm{SO}(\mathbb{R}^3)$, il existe une droite $D \subseteq \mathbb{R}^3$ telle que $f|_D : D \to D$ coïncide avec l'identité de D et $f|_{D^\perp} \in \mathrm{SO}(D^\perp)$.

(*c*) Noter que $\det(f) = -1$ dans ce cas, ce qui nous dit que $\det(-f) = 1$, *i.e.* $-f \in \mathrm{SO}(\mathbb{R}^3)$.

(i) Noter que $\det(f) = -1$ dans ce cas, ce qui nous dit que $\det(-f) = 1$, *i.e.* $-f \in \mathrm{SO}(\mathbb{R}^3)$.

(ii) Comme $r(v) = v$ pour tout $v \in D$ et $r(w) = -w$ pour tout $w \in D^\perp$, tandis que $s(v) = -v$ pour tout $v \in D$ et $s(w) = w$ pour tout $w \in D^\perp$, on voit bien que $s \circ r = r \circ s = -\mathrm{id}_{\mathbb{R}^3}$. En plus, on note que $f \circ s = s \circ f$ et $r \circ f = f \circ r$, car les mêmes égalités sont valables pour $-f$ au lieu de f, vu que $(-f)(v) = v$ pour tout $v \in D$ et $(-f)|_{D^\perp} : D^\perp \to D^\perp$ est une application linéaire. En conséquence, $f = -(-f) = s \circ (r \circ (-f))$, nous dit que f s'écrit comme la composition de la réflexion s et $r \circ (-f) = (-f) \circ r$, qui est aussi une rotation d'axe D, car car $(r \circ (-f))|_D : D \to D$ coïncide avec l'identité de D et $(r \circ (-f)|_{D^\perp} \in \mathrm{SO}(D^\perp)$, vu que $\det(r) = 1$. Si $r \circ (-f) = (-f) \circ r = \mathrm{id}_{\mathbb{R}^3}$, alors $f = s$. Sinon, f est le produit commutatif de la rotation non triviale $r \circ (-f) = (-f) \circ r$ d'axe D avec s. On note que $f = -\mathrm{id}_{\mathbb{R}^3} = s \circ r$ est une antirotation d'axe D.

À partir des items précédents on déduit que, pour tout $f \in \mathrm{O}(\mathbb{R}^3) \setminus \mathrm{SO}(\mathbb{R}^3)$, alors f est soit une réflexion orthogonale, soit une antirotation.

(*d*) Soit $f \in \mathrm{O}(\mathbb{R}^3)$ une isométrie. On considère le sous-espace vectoriel $\mathrm{Fix}(f) = \{v \in \mathbb{R}^3 : f(v) = v\}$ de $\mathbb{R}^3$. À partir des items précédents, on déduit que toute isométrie de $\mathbb{R}^3$ est donnée par un des cas suivants :

(I.1) $f = \mathrm{id}_{\mathbb{R}^3}$ précisément lorsque $\mathrm{Fix}(f) = \mathbb{R}^3$;

(I.2) f est une rotation précisément lorsque $\det(f) = 1$ et $\dim(\mathrm{Fix}(f)) = 1$;

(I.3) f est une antirotation précisément lorsque $\det(f) = -1$ et $\dim(\mathrm{Fix}(f)) = 1$;

(I.4) f est une réflexion précisément lorsque $\det(f) = -1$ et $\dim(\mathrm{Fix}(f)) = 2$.