Exercices

action, monoïdes, groupes

Axiome de l'infini.

1. Supposons $o = \emptyset$ et que f est définie par $\left\{ \begin{array}{ccc} a \neq \mathfrak{P}(\emptyset) & \longmapsto & \mathfrak{P}(a) \\ \mathfrak{P}(\emptyset) & \longmapsto & \emptyset \end{array} \right.$. Alors f n'a pas de point fixe (car $\mathfrak{P}$ n'en a pas) et atteint o (en $\mathfrak{P}(\emptyset)$). Cependant, f est un recollement de deux injections (d'une part $\mathfrak{P}(\emptyset) \mapsto \emptyset$, d'autre part $\mathfrak{P}$ restreinte aux ensembles autres que $\mathfrak{P}(\emptyset)$) d'images disjointes (car un $\mathfrak{P}(a)$ n'est jamais vide), donc est injective.
2. Supposons $o = \emptyset$ et que f est définie par $\left\{ \begin{array}{ccc} a \neq \{\{\emptyset\}\} & \longmapsto & \{a\} \\ \{\{\emptyset\}\} & \longmapsto & \{\emptyset\} \end{array} \right.$. Toutes les images par f étant des singletons, elles sont non vides, donc f n'atteint pas o. Par ailleurs, f n'a pas de point fixe (car $a \mapsto \{a\}$ non plus). Cependant, les objets $\emptyset$ et $\{\{\emptyset\}\}$ ont même image, donc f n'est pas injective.
3. Supposons (1) et (2). Notons N la plus petit partie contenant o et stable par f. Pour tout $n \in N$, notons E_n l'implication $f(n) = n \Longrightarrow f(o) = o$. L'énoncé E_0 est tautologique. Soit par ailleurs $n \in N$ tel que E_n : supposant $f(f(n)) = f(n)$, l'hypothèse (1) donne $f(n) = n$, puis E_n donne $f(o) = o$, ce qui permet d'affirmer l'implication $E_n \Longrightarrow E_{f(n)}$. Par conséquent, la partie $\{n \in N \ ; \ E_n\}$ contient o et est stable par f, donc contient N (par minimalité de ce dernier), donc lui est égal. Enfin, si f admettait un point fixe n, appliquer E_n contredirait l'hypothèse (2).

Logique.

1. La conjonction de AS et NEU définit un monoïde, celle de AS, NEU et INV un groupe. Puisqu'il y a des monoïdes qui ne sont pas des groupes (par exemple $\mathbf{N}$), la première conjonction ne peut prouver la seconde.
2. Il y a des groupes non commutatifs (par exemple $\mathfrak{S}_3$ ou $GL_2(\mathbf{R})$), donc les axiomes d'un groupe ne peuvent prouver l'énoncé de commutativité.
3. Notons $*$ la loi indiquée. On interprète le symbole 1 dans $\mathbf{R}^*$ comme le réel 1 et on interprète le symbole de loi $^{-1}$ par $a \mapsto \frac{1}{|a|}$. Montrons que cette structure vérifie AS, NEU_g et INV_d mais ni NEU ni INV. Soient $a, b, c \in \mathbf{R}^*$. On a les égalités

$$a * (b * c) = a * (|b| c) = |a| |b| c \quad \text{et} \quad (a * b) * c = |a| b * c = ||a| b| c = |a| |b| c,$$

d'où AS. On a $1 * a = |1| a = 1a = a$, d'où NEU_g. Enfin, on a $a * a^{-1} = |a| \frac{1}{|a|} = 1$, d'où INV_d. Cependant, on a

$$\begin{array}{rcl} (-18) * 1 & = & |-18| 1 = 18 \neq -18, \text{ ce qui infirme } NEU_d, \text{ et} \\ (-42)^{-1} * -42 & = & \dfrac{1}{|-42|} * (-42) = \left| \dfrac{1}{42} \right| (-42) = -1 \neq 1, \text{ ce qui infirme } INV_g. \end{array}$$

4. Suivons l'indication. Soient $1, b, c$ trois objets distincts. On définit une loi $*$ sur $\{1, a, b\}$ par la table

$*$ ↱	1	a	b
1	1	a	b
a	a	1	1
b	b	1	1

.

On s'est arrangé pour que 1 soit neutre, d'où NEU.
Tout élément étant involutif (donc inversible), on a INV.
Cependant, les égalités $\left\{ \begin{array}{l} a * (a * b) = a * 1 = a \\ (a * a) * b = 1 * b = b \end{array} \right.$ infirment AS.

5. Soit M un magma vérifiant AS, NEU_g et INV_g. Montrons INV_d (ce qui montrera INV[1]). On en déduira pour tout $m \in M$ les égalités

$$m1 = m\left(m^{-1}m\right) = \left(mm^{-1}\right) m = 1m = m, \text{ d'où } NEU_d \text{ et } NEU, \text{ ce qui conclura.}$$

Soit $m \in M$. Abrégeons $m' := m^{-1}$ et $m'' := m'^{-1}$. Il s'agit de montrer $m'' = m$, puisqu'on aura alors $1 = m''m' = mm'$ et m' sera inverse à droite de m comme souhaité. Multipliant l'égalité $1 = m'm$ par m'' à gauche, il vient

$$m''1 = m''(m'm) = (m''m') m = 1m = m.$$

[1] Rappelons qu'un inverse bilatère est unique – pour une loi associative.

On en déduit les égalités

$$\begin{aligned} m' &= 1m' = (m'm)\,m' = m'\,(m)\,m' = m'\,(m''1)\,m' \\ &= m'm''\,(1m') = m'm''\,(m') = m'\,(m''m') = m'1, \end{aligned}$$

donc 1 est neutre à droite pour tous les éléments de la forme m', en particulier pour m'', d'où $m'' = m''1 = m$, *c. q. f. d.*.

Monoïdes et groupes.

1. [Analyse] Soit $f^\times$ un tel morphisme. Soit $m \in M^\times$. Suivre le diagramme montre que $f^\times(m) = f(m)$, donc $f^\times$ doit être définie comme la restriction de f à $M^\times$. De plus, $f^\times$ conserve l'inversion, donc pour tout $m \in M^\times$ l'inverse de $f(m) = f^\times(m)$ vaut $f^\times\left(m^{-1}\right) = f\left(m^{-1}\right)$. [Fin de l'analyse.]

   Montrons que $f_{|M^\times}$ prend ses valeurs dans $N^\times$, ce qui conclura en définissant $f^\times : \left\{ \begin{array}{ccc} M^\times & \longrightarrow & N^\times \\ m & \longmapsto & f(m) \end{array} \right.$. Soit $m \in M^\times$. Montrons que $f(m) \in N^\times$. Son inverse doit être $f\left(m^{-1}\right)$ d'après l'analyse. Vérifions : on a $f(m)\,f\left(m^{-1}\right) = f\left(mm^{-1}\right) = f(1) = 1$ (car f est un morphisme de monoïdes) et de même de l'autre côté, *c. q. f. d.*.

2. La commutativité du digramme $\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & O \\ \uparrow\cup & & \uparrow\cup & & \uparrow\cup \\ M^\times & \xrightarrow{f^\times} & N^\times & \xrightarrow{g^\times} & O^\times \end{array}$ est immédiate et découle de celle des deux diagrammes $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \uparrow\cup & & \uparrow\cup \\ M^\times & \xrightarrow{f^\times} & N^\times \end{array}$ et $\begin{array}{ccc} N & \xrightarrow{g} & O \\ \uparrow\cup & & \uparrow\cup \\ N^\times & \xrightarrow{g^\times} & O^\times \end{array}$. On en déduit que $g^\times \circ f^\times$ fait commuter le diagramme $\begin{array}{ccc} M & \xrightarrow{g\circ f} & O \\ \uparrow\cup & & \uparrow\cup \\ M^\times & \xrightarrow{g^\times\circ f^\times} & O^\times \end{array}$, ce qui montre (d'après l'unicité de la question précédente) l'égalité voulue[2] $[g \circ f]^\times = g^\times \circ f^\times$.

Groupe algébrique. Les automorphismes étudiés sont les bijections de $V := \mathbf{Q} + \mathbf{Q}\sqrt[3]{7} + \mathbf{Q}\sqrt[3]{49}$ dans lui-même qui préserve l'addition, la multiplication et les homothéties de rapport rationnel. Ces trois caractères préservatifs étant clairement conservés par composition, l'ensemble considéré est un sous-groupe de $GL(V)$, donc est un groupe.

Soit f dedans : par linéarité, il est déterminé par l'image d'une $\mathbf{Q}$-base de V, par exemple $\left(1, \sqrt[3]{7}, \sqrt[3]{7}^2\right)$. Or on aura toujours d'une part $f(1) = 1$ car f est $\mathbf{Q}$-linéaire et d'autre part $f\left(\sqrt[3]{49}\right) = f\left(\sqrt[3]{7}^2\right) = f\left(\sqrt[3]{7}\right)^2$, de sorte que f est entièrement déterminé par l'image $a := f\left(\sqrt[3]{7}\right)$. Par ailleurs, vu que $a^3 = f\left(\sqrt[3]{7}\right)^3 = f\left(\sqrt[3]{7}^3\right) = f(7) = 7$, le réel a ne peut valoir que $\sqrt[3]{7}$ (les autres racines de $X^3 - 7$ tombent hors de V). Finalement, f coïncide avec l'identité sur $\sqrt[3]{7}$, donc vaut l'identité. *Conclusion* : le groupe cherché est le groupe trivial.

Commutant. Abrégeons $C :=$ Comm. Montrons $A \subset \mathrm{Comm}\, C(A)$. Soit $a \in A$. Soit $c \in C(A)$. Par définition de $C(A)$, on a $ac = ca$, ce qui montre que a commute avec tous les éléments de $C(A)$, donc appartient à $\mathrm{Comm}\, C(A)$, d'où l'inclusion annoncée.

S'il y a égalité, alors A est bien de la forme $C(B)$ voulue en posant $B := C(A)$.

Supposons réciproquement que A est de la forme $C(B)$ pour une certaine partie $B \subset G$. Le point précédent $\forall P \subset G,\ P \subset CC(P)$ montre, en remplaçant P par B puis par $C(B)$, les inclusions $B \subset CC(B)$ et $C(B) \subset CCC(B)$ or la décroissance de Comm appliquée à la première inclusion donne $CCC(B) \subset C(B)$, d'où l'égalité $A = C(B) = CCC(B) = CC(A)$.

[2] On dit que la correspondance $M \mapsto M^\times$ est un ***foncteur*** de la catégorie des monoïdes vers la catégorie des groupes. L'égalité $[g \circ f]^\times = g^\times \circ f^\times$ permet de penser un foncteur comme un "morphisme de morphismes".

Sous-groupes denses. Notons s le morphisme surjectif $\left\{\begin{array}{ccc}\mathbf{R} & \twoheadrightarrow & \mathbf{U}\\ t & \longmapsto & e^{it}\end{array}\right.$. Soit H un sous-groupe de $\mathbf{U}$. Notons $G := \varphi^{-1}(H)$. Puisque s est surjective, le groupe H est l'image directe $\varphi(G)$ de sa préimage. Puisque s est un morphisme, la préimage du sous-groupe H est un sous-groupe de $\mathbf{R}$, donc est ou bien dense dans $\mathbf{R}$, ou bien discrète. Dans le premier cas, l'image H par l'application continue s est dense dans $s(\mathbf{R}) = \mathbf{U}$. Supposons donc le second cas, mettons $G = a\mathbf{Z}$ pour un certain réel $a > 0$. On en déduit une description de $H = s(G) = s(\langle a\rangle) = \langle a\rangle = \langle e^{ia}\rangle$. Si a est un multiple rationnel de π, en notant d le dénominateur réduit du rationnel $\frac{a}{2\pi}$, on aura $\langle e^{ia}\rangle = \left\langle e^{2\pi i\frac{1}{d}}\right\rangle = \mathbf{U}_d$. Dans le cas contraire, le sous-groupe $a\mathbf{Z} + 2\pi\mathbf{Z}$ sera dense dans $\mathbf{R}$, donc son image sera (toujours par continuité de s) dense dans $\mathbf{U}$; or cette image vaut $s(a\mathbf{Z} + 2\pi\mathbf{Z}) = s(a\mathbf{Z})\, s(2\pi\mathbf{Z}) = H\{1\} = H$, ce qui conclut.

Composé de sous-groupes. Soit G un groupe. Soient A et B deux sous-groupes de G. On note $AB := \{ab\ ;\ a \in A \text{ et } b \in B\}$ (idem dans l'autre sens).

1. [analyse] Soit $f : A \times B \xrightarrow{\sim} AB$ un isomorphisme faisant commuter le diagramme donné. Soit $(a, b) \in A \times B$. Lire le triangle de gauche donne $f\binom{a}{1} = a$ et celui de droite $f\binom{1}{b} = b$, d'où $f\binom{a}{b} = f\left(\binom{a}{1}\binom{1}{b}\right) = f\binom{a}{1}f\binom{1}{b} = ab$. [fin de l'analyse].

   Définissons $f : \left\{\begin{array}{ccc}A \times B & \longrightarrow & AB\\ (a,b) & \longmapsto & ab\end{array}\right.$ (forcé par l'analyse). Par définition de AB, l'application f est bien définie et surjective. Par hypothèse de commutativité, f est un morphisme. Montrons enfin qu'il est injectif. Soit $(a, b) \in A \times B$ tel que $ab = 1$. Alors l'élément $a = b^{-1}$ appartient à $A \cap B = \{1\}$, d'où l'égalité $\binom{a}{b} = \binom{1}{1}$.
2. Observer que la matrice b est inversible puisque le coefficient diagonal 2, étant étranger à n, est inversible *modulo* n. On a plus précisément $b^{\varphi(n)} = 1$ (vu que $2^{\varphi(n)} = 1$) et par ailleurs l'égalité $a^n = 1$. Ainsi a et b sont-ils d'ordre fini, mettons $\binom{\alpha}{\beta} := \binom{\omega(a)}{\omega(b)}$, et l'on pourra décrire au besoin $BA = \left\{b^\ell a^k\right\}_{0\le k<\alpha}^{0\le \ell<\beta} = \left\{b^\ell a^k\ ;\ k, \ell \in \mathbf{N}\right\}$.

   Deux récurrences immédiates montreraient pour tout naturel n les égalités $a^n := \begin{pmatrix}1 & n\\ \cdot & 1\end{pmatrix}$ et $b^n = \begin{pmatrix}1 & \cdot\\ \cdot & 2^n\end{pmatrix}$. On en déduit à $p, q \in \mathbf{N}$ fixés les égalités

$$\begin{aligned} a^p b^q &= \begin{pmatrix}1 & p\\ \cdot & 1\end{pmatrix}\begin{pmatrix}1 & \cdot\\ \cdot & 2^q\end{pmatrix} = \begin{pmatrix}1 & p2^q\\ \cdot & 2^q\end{pmatrix} \text{ et}\\ b^q (a^p)^{2^q} &= \begin{pmatrix}1 & \cdot\\ \cdot & 2^q\end{pmatrix}\begin{pmatrix}1 & p2^q\\ \cdot & 1\end{pmatrix} = \begin{pmatrix}1 & p2^q\\ \cdot & 2^q\end{pmatrix}, \end{aligned}$$

   ce qui montre que BA est stable par produit (écrire $b^\diamond a^p b^q a^\triangle = b^{\diamond+q} a^{p2^q+\triangle}$) et que $ab = ba^2 \neq ba$. Montrons que BA est stable par inverse, ce qui conclura à $AB = BA$ d'après la question suivante (BA contient trivialement $1 = b^0 a^0$). Nous savons a et b d'ordres finis α et β, d'où l'on déduit pour tous p et q naturels

$$(b^q a^p)^{-1} = 1a^{-p}1b^{-q} = a^{p\alpha}a^{-p}b^{q\beta}b^{-q} = a^{p(\alpha-1)}b^{q(\beta-1)} = b^{q(\beta-1)}\left(a^{p(\alpha-1)}\right)^{2^{q(\beta-1)}} \in BA.$$

3. Supposons $AB = BA$. On a alors $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$, ce qui montre que AB est stable par produit. De même, on a $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$, ce qui montre la stabilité par inversion. Enfin, la partie AB contient toujours $1 = 1 \cdot 1$.

   Supposons que AB est un sous-groupe. Soit $(a, b) \in A \times B$. Alors le produit $ba = (1b)(a1)$ reste dans AB, ce qui montre l'inclusion $BA \subset AB$. Réciproquement, l'inverse de ab reste dans AB, mettons $(ab)^{-1} = \alpha\beta$ pour un $(\alpha, \beta) \in A \times B$, d'où $ab = \beta^{-1}\alpha^{-1} \in BA$, ce qui montre l'inclusion $AB \subset BA$.

   La question précédente[3] fournit un contre-exemple à l'équivalence $AB = BA \iff \forall (a, b) \in A \times B,\ ab = ba$.

[3] On aurait pu simplifier ce contre-exemple en se plaçant dans $\mathbf{Z}/3$, il aurait alors été facile d'expliciter les six éléments de AB et de BA. Nous souhaitions montrer le caractère générique des contre-exemples où A et B sont cycliques et dont des générateurs a et b respectifs vérifient $ab = ba^2$ (cette dernière égalité étant l'idée la plus simple à imaginer, avec $ab = b^2a$, pour imposer $ab \in BA \setminus \{ba\}$).

Ordres. Soient a et b dans G. On a alors les égalités

$$ab = a1b = a\left(ab\right)^2 b = a\left(abab\right)b = \left(a^2\right)ba\left(b^2\right) = 1ba1 = ba,$$

ce qui montre que G est abélien.

Notons sa loi additivement, de sorte que l'on $\forall g \in G,\ 2g = 0$. On munit alors G d'une structure de $\mathbf{F}_2$-espace vectoriel en définissant[4] $\overline{1} \cdot g := g$ et $\overline{0} \cdot g = 0$ pour tout $g \in G$. La vérification des axiomes est laissée aux soins du lecteur. En notant I un ensemble indexant une $\mathbf{F}_2$-base[5] de G, la classification des espaces vectoriel nous dit alors que G est isomorphe (en tant que $\mathbf{F}_2$-espace vectoriel, *a fortiori* en tant que groupe additif) à $\mathbf{F}_2^{(I)}$, ce qui conclut.

Exposant d'un groupe abélien fini.

1. Soit $p \in \mathbf{P}$. La partie $\{n \in \mathbf{N}\ ;\ \exists g \in G,\ \omega\left(g\right) = p^n\}$ de $\mathbf{N}$ contient 0 car l'ordre de 1_G vaut $1 = p^0$, donc est non vide, donc admet un minimum.

2. Soit $p \in \mathbf{P}$. Alors p^{γ_p} divise $\omega\left(g\right)$ et $g^{\frac{\omega(g)}{p^{\gamma_p}}}$ est d'ordre p^{γ_p}, donc l'exposant γ_p appartient à la partie $\{n \in \mathbf{N}\ ;\ \exists g \in G,\ \omega\left(g\right) = p^n\}$, donc doit minorer son maximum α_p, d'où la divisibilité $p^{\gamma_p} \mid p^{\alpha_p}$. Faire le produit sur tous les premiers p donne la divisibilité $\omega\left(g\right) \mid \prod p^{\alpha_p}$. Par ailleurs, les a_p commutent et sont d'ordres deux à deux étrangers, d'où les égalités $\omega\left(\prod a_p\right) = \prod \omega\left(a_p\right) = \prod p^{\alpha_p}$. Finalement, l'ordre de $\prod a_p$ est multiple de tous les $\omega\left(g\right)$, ce qui conclut. (On a même montré que l'ordre de $\prod a_p$ est maxim*um* pour la divisibilité.)

3. Le groupe K^* étant abélien fini, on peut lui appliquer ce qui précède : soit $g \in K^*$ d'ordre maximal et montrons l'égalité $\langle g\rangle = K^*$. Vu l'inclusion $\subset$, il suffit de montrer la comparaison cardinale $\#\langle g\rangle \geq \#K^*$. Notons ω l'ordre de g. Soit $a \in K^*$ et notons α son ordre. Alors a est racine du polynôme $X^\alpha - 1$, lequel divise $X^\omega - 1$ puisque $\alpha \mid \omega$, ce qui montre que $X^\omega - 1$ s'annule sur tout K^*, d'où la comparaison $\deg\left(X^\omega - 1\right) \geq |K^*|$, *c. q. f. d.*.

Isomorphismes.

1. L'application $P \mapsto A \setminus P$ est un isomorphisme entre les monoïdes $\begin{pmatrix}\mathfrak{P}\left(A\right)\\ \cap\end{pmatrix}$ et $\begin{pmatrix}\mathfrak{P}\left(A\right)\\ \cup\end{pmatrix}$. Dans ces derniers, tous les éléments sont idempotents tandis que, dans $\begin{pmatrix}\mathfrak{P}\left(A\right)\\ \Delta\end{pmatrix}$, tous les éléments sont involutifs : ainsi, tout morphisme $f : \begin{pmatrix}\mathfrak{P}\left(A\right)\\ \cap\end{pmatrix} \longrightarrow \begin{pmatrix}\mathfrak{P}\left(A\right)\\ \Delta\end{pmatrix}$ doit vérifier pour toute partie $P \subset A$ les égalités

$$f\left(P\right) = f\left(P \cap P\right) = f\left(P\right)\Delta f\left(P\right) = \emptyset, \text{ donc est constant.}$$

   Ainsi les lois $\cap$ et Δ ne sont-elles jamais isomorphes sur $\mathfrak{P}\left(A\right)$, à l'exception du cas $A = \emptyset$.

2. Un monoïde étant toujours non vide (il possède un neutre), il n'y pas de monoïde d'ordre 0. Par ailleurs, tous les monoïdes d'ordre 1 sont trivialement isomorphes *via* les uniques applications entre deux monoïdes-singletons. On supposera donc $n \geq 2$. Soit alors N une matrice nilpotent d'ordre $n-1$: le monoïde qu'elle engendre vaut[6] $\left\{1, N, N^2, ..., N^{n-2}, N^{n-1} = 0\right\}$, donc est d'ordre n. Puisque ce monoïde n'est pas un groupe (0 n'y est pas inversible), il ne peut être isomorphe au monoïde $\mathbf{U}_n$. Finalement, si $n \geq 2$, on peut toujours trouver deux monoïdes d'ordre n non isomorphes.

3. Regardons les ordres des éléments :

$\begin{matrix} a & b \\ & c \end{matrix}$	$\begin{matrix}\cdot & \cdot\\ & \cdot\end{matrix}$	$\begin{matrix}1 & \cdot\\ & 1\end{matrix}$	$\begin{matrix}1 & 1\\ & 1\end{matrix}$	$\begin{matrix}\cdot & 1\\ & \cdot\end{matrix}$	$\begin{matrix}\cdot & \cdot\\ & 1\end{matrix}$	$\begin{matrix}1 & \cdot\\ & \cdot\end{matrix}$	$\begin{matrix}1 & 1\\ & \cdot\end{matrix}$	$\begin{matrix}\cdot & 1\\ & 1\end{matrix}$
$\omega\begin{pmatrix}1 & a & b\\ \cdot & 1 & c\\ \cdot & \cdot & 1\end{pmatrix}$	1	4	4	2	2	2	2	2

.

[4] cette structure provient de celle de $\mathbf{Z}$-"espace vectoriel" (que possède tout groupe abélien) qui passe modulo $2\mathbf{Z}$ grâce à l'hypothèse $\forall g \in G,\ 2g = 0$

[5] l'existence d'une base provient (dans le cas général où G est infini) de l'axiome du choix

[6] il s'agit d'un cas de boucle avortée vu en cours ; on pourrait tout à fait en imaginer d'autres

Ces ordres sont ceux des éléments du groupe des symétries du carré : essayons de calquer les deux groupes. En notant $s := \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & 1 \\ \cdot & \cdot & 1 \end{pmatrix}$ et $s' := \begin{pmatrix} 1 & 1 & \cdot \\ \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \end{pmatrix}$ (à penser comme deux réflexions), leur produit vaut $\begin{pmatrix} 1 & 1 & \cdot \\ \cdot & 1 & 1 \\ \cdot & \cdot & 1 \end{pmatrix} =: r$ (à penser comme une rotation d'angle $\frac{\pi}{2}$) dont le carré vaut $\begin{pmatrix} 1 & \cdot & 1 \\ \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \end{pmatrix}$ (à penser comme la symétrie centrale). En notant σ et σ' les réflexions d'axes respectifs $\mathbf{R}$ et $\mathbf{R}e^{i\frac{\pi}{4}}$ et ρ leur composée (rotation d'angle $\frac{\pi}{2}$), les réflexions d'axes $\mathbf{R}i$ et $\mathbf{R}e^{i\frac{3\pi}{4}}$ s'obtiennent en conjuguant respectivement σ et σ' par ρ (cela fait tourner les axes des réflexions d'un angle $\frac{\pi}{2}$) Tout cela permet d'intuiter un isomorphisme (avec les abréviations matricielles évidentes) :

1	s	s'	r	r^2	r^3	rsr^{-1}	$rs'r^{-1}$
$\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}$	$\begin{pmatrix} \cdot & \cdot \\ \cdot & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \cdot \\ \cdot & \cdot \end{pmatrix}$	$\begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix}$	$\begin{pmatrix} \cdot & 1 \\ \cdot & \cdot \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ \cdot & 1 \end{pmatrix}$	$\begin{pmatrix} \cdot & 1 \\ \cdot & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ \cdot & \cdot \end{pmatrix}$
Id	σ	σ'	ρ	ρ^2	ρ^3	$\rho\sigma\rho^{-1}$	$\rho\sigma'\rho^{-1}$

On laisse au lecteur le soin de vérifier que cette bijection préserve le produit (il lui suffira en fait d'établir la table de composition).

4. Soient $a, b \in \mathbf{Z}[i]$; la condition $|a|^2 + |b^2| = 1$ dit que $|a|^2$ et $|b|^2$ sont des entiers positifs de somme 1, ce qui équivaut à $\left\{|a|^2, |b|^2\right\} = \{0, 1\}$, ou encore à $\binom{a}{b} \in \left\{\binom{\pm 1}{0}, \binom{\pm i}{0}, \binom{0}{\pm 1}, \binom{0}{\pm i}\right\}$. Ainsi l'ensemble étudié possède-t-il huit éléments. Essayons de le bijecter avec un groupe de référence (si l'on trouve une bijection préservant le produit, alors cet ensemble sera automatiquement un groupe par transport de structure). Regardons pour cela les ordres[7] :

$\binom{a}{b}$	$\binom{1}{0}$	$\binom{-1}{0}$	$\binom{\pm i}{0}$	$\binom{0}{\pm 1}$	$\binom{0}{\pm i}$
$\omega\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$	1	2	4|4	4|4	4|4

On reconnaît les ordres de $\mathbf{H}_8$. Il est alors naturel d'essayer la bijection

$\binom{\pm 1}{0}$	$\binom{\pm i}{0}$	$\binom{0}{\pm 1}$	$\binom{0}{\pm i}$
± 1	$\pm i$	$\pm j$	$\pm k$

(seul le choix de j ou k n'est pas immédiat : on trouve deux signes possibles $ij = \pm k$ et il n'est alors pas bien difficile de trancher sur l'ordre à adopter pour obtenir un signe $+$). On laisse au lecteur le soin de vérifier que les tables de compositions sont préservées.

5. Trois de ces groupes sont dénombrables, au contraire de $\mathbf{R}$, ce qui met ce dernier hors course. Ensuite, le groupe $\mathbf{Z}$ est monogène mais pas les deux autres. Enfin, le groupe $\mathbf{Q}$ est divisible (tout élément est un double, un triple, un quadruple...), ce qui n'est pas le cas des deux autres (les éléments $1 \in \mathbf{Z}$ et $(1, 0) \in \mathbf{Z}^2$ n'ont pas de doubles). Finalement, les quatre groupes fournissent autant de classes d'isomorphie.

Automorphismes intérieurs.

1. Le lecteur pourra prendre du recul sur ces exercices s'il regarde un peu ce qu'est un produit ***semi-direct*** de groupes (ce sont les structures mises sur les groupes G_φ et $G^\Diamond$).

   (a) Soient $\binom{g}{a}, \binom{h}{b}, \binom{k}{c} \in G_a$.
   Montrons que le neutre $\binom{1_G}{0}$ du groupe produit est neutre pour G_φ : on a les égalités

$$\begin{aligned} \binom{g}{a}\binom{1}{0} &= \binom{g\ \varphi^a(1)}{a+0} = \binom{g\ 1}{a} = \binom{g}{a} \text{ et} \\ \binom{1}{0}\binom{g}{a} &= \binom{1\ \varphi^0(g)}{0+a} = \binom{\mathrm{Id}(g)}{a} = \binom{g}{a}, \text{ c. q. f. d..} \end{aligned}$$

[7] bien vérifier que tous les itérés bouclent sur 1 (comme on n'a pas *a priori* un groupe, on ne peut pas invoquer Lagrange)

Montrons que $\binom{g}{a}$ est inversible. Vu les équivalences

$$\binom{g}{a}\binom{h}{b} = 1_{G_\varphi} \Longleftrightarrow \binom{g\ \varphi^a(h)}{a+b} = \binom{1}{0} \Longleftrightarrow \binom{\varphi^a(h)}{b} = \binom{g^{-1}}{-a} \Longleftrightarrow \binom{h}{b} = \binom{\varphi^{-a}\left(g^{-1}\right)}{-a},$$

il reste à vérifier que l'inverse imposé $\binom{\varphi^{-a}\left(g^{-1}\right)}{-a}$ en est bien un de l'autre côté. Or on a bien les égalités

$$\binom{\varphi^{-a}\left(g^{-1}\right)}{-a}\binom{g}{a} = \binom{\varphi^{-a}\left(g^{-1}\right)\ \varphi^{-a}(g)}{-a+a} = \binom{\varphi^{-a}(g)^{-1}\ \varphi^{-a}(g)}{0} = \binom{1}{0}.$$

Montrons enfin l'associativité, qui découle directement des égalités

$$\begin{aligned}
\binom{g}{a}\left[\binom{h}{b}\binom{k}{c}\right] &= \binom{g}{a}\binom{h\ \varphi^b(k)}{b+c} = \binom{g\ \varphi^a\left(h\ \varphi^b(k)\right)}{a+(b+c)} = \binom{g\ \varphi^a(h)\ \ \varphi^{a+b}(k)}{a+b+c} \text{ et} \\
\left[\binom{g}{a}\binom{h}{b}\right]\binom{k}{c} &= \binom{g\ \varphi^a(h)}{a+b}\binom{k}{c} = \binom{(g\ \varphi^a(h))\ \ \varphi^{a+b}(k)}{(a+b)+c} = \binom{g\ \varphi^a(h)\ \ \varphi^{a+b}(k)}{a+b+c}.
\end{aligned}$$

(bonus) On en déduirait plus généralement des identités $\prod_{i=1}^n \binom{g_i}{a_i} = \binom{\prod_{i=1}^n \varphi^{a_1+a_2+\cdots+a_{i-1}}(g_i)}{a_1+a_2+\cdots+a_n}$.

(b) Montrons que l'application $i : g \mapsto \binom{g}{0}$ est un plongement. Son injectivité étant triviale (lire l'abscisse permet de récupérer l'antécédent), il suffit de montrer que c'est un morphisme. Or pour tous g et h dans G on a bien

$$i(g)\ \ i(h) = \binom{g}{0}\binom{h}{0} = \binom{g\ \varphi^0(h)}{0+0} = \binom{g\ \mathrm{Id}(h)}{0} = \binom{gh}{0} = i(gh).$$

(c) Soit $(g,a) \in G \times \mathbf{Z}$. On calcule directement

$$\begin{aligned}
\binom{1}{a}\binom{g}{0}\binom{1}{a}^{-1} &= \left[\binom{1}{a}\binom{g}{0}\right]\binom{1}{a}^{-1} = \binom{1\ \varphi^a(g)}{a+0}\binom{\varphi^{-a}\left(1^{-1}\right)}{-a} = \binom{\varphi^a(g)}{a}\binom{1}{-a} \\
&= \binom{\varphi^a(g)\ \ \varphi^a(1)}{a+(-a)} = \binom{\varphi^a(g)\ \ 1}{a-a} = \binom{\varphi^a(g)}{0}, \textit{ c. q. f. d.}.
\end{aligned}$$

(d) Soit c un tel morphisme : en suivant un $g \in G$ selon les deux composées $\longrightarrow\downarrow$ et $\downarrow\longrightarrow$, le morphisme c doit envoyer $\binom{g}{0}$ sur $\binom{\varphi(g)}{0}$. La question précédente montre que cela sera vérifié si c est la conjugaison[8] par $\binom{1}{1}$.

Le diagramme nous dit que l'action de φ (automorphisme de G), vue comme automorphisme de G_a grâce au plongement $G \overset{c}{\hookrightarrow} G_\varphi$ utilisé au départ et à l'arrivée, est celle d'une *conjugaison*. Tout automorphisme de G peut ainsi être réalisé comme automorphisme *intérieur* d'un sur-groupe de G.

Les questions suivantes montrent que l'on peut construire un tel sur-groupe indépendant de l'automorphisme φ choisi.

2.

(a) Tout se passe comme pour les groupes G_φ des questions précédentes : on vérifiera que $\binom{1}{\mathrm{Id}}$ est neutre, que l'inverse d'un $\binom{g}{\alpha}$ est $\binom{\alpha^{-1}\left(g^{-1}\right)}{\alpha^{-1}}$ et que le composé de trois éléments $\binom{g}{\alpha}$, $\binom{h}{\beta}$ et $\binom{k}{\gamma}$ vaut $\binom{g\ \alpha(h)\ \alpha\beta(k)}{\alpha\beta\gamma}$. On montrerait en bonus les égalités $\prod_{i=1}^n \binom{g_i}{\alpha_i} = \binom{\prod_{i=1}^n \left[\alpha_1\alpha_2\cdots\alpha_{i-1}\right](g_i)}{\alpha_1\alpha_2\cdots\alpha_n}$.

(b) Soit i un tel plongement. Pour tout $g \in G$, notons $\binom{g'}{\alpha_g} := i(g)$. Alors la commutativité du diagramme partant d'un $g \in G$ montre $g' = g$. Par ailleurs, puisque i est un morphisme, suivre un produit $gh \in G$ donne $g\alpha_g(h) = gh$, *i. e.* $\alpha_g(h) = h$, d'où $\alpha_g = \mathrm{Id}$, et ce pour tout g. Finalement, on doit avoir $i(g) = \binom{g}{\mathrm{Id}}$.

[8] bien observer que les deux 1 n'ont rien à voir : celui d'en haut est le *neutre* de G (notation multiplicative) celui d'en bas est un *générateur* de $\mathbf{Z}$ (notation additive)

Montrons réciproquement que l'application $i : g \mapsto \begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix}$ est un plongement. Son injectivité étant triviale (lire l'abscisse permet de récupérer l'antécédent), il suffit de montrer que c'est un morphisme. Or pour tous g et h dans G on a bien

$$i(g)\ i(h) = \begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix}\begin{pmatrix} h \\ \mathrm{Id} \end{pmatrix} = \begin{pmatrix} g\ \mathrm{Id}(h) \\ \mathrm{Id} \circ \mathrm{Id} \end{pmatrix} = \begin{pmatrix} gh \\ \mathrm{Id} \end{pmatrix} = i(gh).$$

(c) L'application j prend clairement ses valeurs dans $\mathrm{Int}\, G^\Diamond$. Montrons que j est un morphisme. Soient φ et ψ dans $\mathrm{Aut}\, G$ et $x \in G^\Diamond$. On a alors

$$\begin{aligned}[j(\varphi) \circ j(\psi)](x) &= \underset{(1,\varphi)}{\mathrm{int}} \left(\underset{(1,\psi)}{\mathrm{int}}\ x \right) = \begin{pmatrix} 1 \\ \varphi \end{pmatrix}\begin{pmatrix} 1 \\ \psi \end{pmatrix} x \begin{pmatrix} 1 \\ \psi^{-1} \end{pmatrix}\begin{pmatrix} 1 \\ \varphi^{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ \varphi\psi \end{pmatrix} x \begin{pmatrix} 1 \\ \psi^{-1}\varphi^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 \\ \varphi\psi \end{pmatrix} x \begin{pmatrix} 1 \\ (\varphi\psi)^{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ \varphi\psi \end{pmatrix} x \begin{pmatrix} 1 \\ \varphi\psi \end{pmatrix}^{-1} = \mathrm{int}_{\begin{pmatrix} 1 \\ \varphi\psi \end{pmatrix}}(x),\ \textit{c. q. f. d.}.\end{aligned}$$

Montrons alors que j est injective, *i. e.* que son noyau est trivial. Soit $\varphi \in \mathrm{Ker}\, j$. On a alors pour tout $g \in G$ les égalités

$$\begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix} = \mathrm{Id} \begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix} = j(\varphi) \begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix} = \underset{(1,\varphi)}{\mathrm{int}} \begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix} = \begin{pmatrix} 1 \\ \varphi \end{pmatrix}\begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix}\begin{pmatrix} 1 \\ \varphi^{-1} \end{pmatrix} = \begin{pmatrix} \varphi(g) \\ \mathrm{Id} \end{pmatrix},$$

ce qui montre (en regardant l'abscisse) $\varphi = \mathrm{Id}$, *c. q. f. d.*.

(d) Suivons dans le diagramme donné les images d'un élément partant d'en haut à gauche :

$$\begin{array}{ccccc} (g,\varphi) & \overset{i\times j}{\hookrightarrow} & & & \left(\begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix}, \underset{(1,\varphi)}{\mathrm{int}} \right) \\ \downarrow \textit{ év} & & & & \downarrow \textit{ év} \\ \varphi(g) & \overset{i}{\hookrightarrow} & \begin{pmatrix} \varphi(g) \\ \mathrm{Id} \end{pmatrix} & \overset{?}{=} & \begin{pmatrix} 1 \\ \varphi \end{pmatrix}\begin{pmatrix} g \\ \mathrm{Id} \end{pmatrix}\begin{pmatrix} 1 \\ \varphi^{-1} \end{pmatrix} \end{array}.$$

Le point d'interrogation peut être enlevé en vertu du calcul de $\mathrm{Ker}\, j$ effectué à la question précédente.

Le diagramme nous dit que l'action d'un automorphisme de G, vue comme automorphisme de $G^\Diamond$ grâce d'une part au plongement $G \overset{i}{\hookrightarrow} G^\Diamond$ (utilisé au départ et à l'arrivée) d'autre part au plongement $\mathrm{Aut}\, G \overset{j}{\hookrightarrow} \mathrm{Aut}\, G^\Diamond$, est celle d'une *conjugaison*. Tout automorphisme de G peut ainsi être réalisé comme automorphisme *intérieur* d'un sur-groupe de G et ce indépendamment de l'automorphisme considéré.

Faisons le lien avec les questions précédentes. Soit $\varphi \in \mathrm{Aut}\, G$. Alors $G^\Diamond$ contient $G \times \langle\varphi\rangle$ comme sous-groupe et la conclusion s'applique à ce sous-groupe. En remarquant que ce dernier est isomorphe à $G \times {}^{\mathbf{Z}}\!/_{\omega}$ où l'on a noté ω le générateur positif de $\mathrm{Ker}\,(\mathbf{Z} \longrightarrow \langle\varphi\rangle)$, on retrouve le groupe G_φ *modulo* un *modulo* ω. Le plongement j restreint à $\langle\varphi\rangle$ envoie alors φ sur $\underset{(1,\varphi)}{\mathrm{int}}$; vu dans ${}^{\mathbf{Z}}\!/_{\omega}$, le générateur φ devient $\overline{1}$ et son agent-image $\underset{(1,\overline{1})}{\mathrm{int}}$: on retrouve la conjugaison c considérée auparavant.

Remarques. Remplacer ${}^{\mathbf{Z}}\!/_{\omega}$ par $\mathbf{Z}$ a certes permis de simplifier la présentation mais on perd l'unicité d'un plongement *modulo* commutativité du diagramme $\begin{array}{ccc} G & \hookrightarrow & \\ \| & & G_\varphi \\ G & \twoheadleftarrow & \end{array}$: on montrerait en effet que les tels morphismes sont les $i_\chi : g \mapsto \begin{pmatrix} g \\ \chi(g)\ \omega \end{pmatrix}$ où χ décrit les morphismes de G vers $\mathbf{Z}$. On pourra alors montrer que le diagramme $\begin{array}{ccc} G & \overset{i_\chi}{\hookrightarrow} & G_\varphi \\ \varphi \downarrow \simeq & & \simeq \downarrow \underset{(g,a)}{\mathrm{int}} \\ G & \overset{i_\chi}{\hookrightarrow} & G_\varphi \end{array}$ commute ssi $\begin{cases} \varphi(g) = g \\ \varphi^{a-1} = \mathrm{int}_{g^{-1}} \\ \chi \circ \varphi = \chi \text{ ou } \omega = 0 \end{cases}$ (le cas de l'exercice est celui où $(g, a, \chi) = (1, 1, 0)$).

Par ailleurs, afin de comprendre *tous* les moyens de réaliser "naturellement" $\mathrm{Aut}\, G$ dans $\mathrm{Int}\, G^\Diamond$ (pas seulement celui de l'exercice), on pourrait chercher *tous* les plongements $j : \begin{cases} \mathrm{Aut}\, G & \longrightarrow & \mathrm{Int}\, G^\Diamond \\ \alpha & \longmapsto & \underset{(g_\alpha,\alpha)}{\mathrm{int}} \end{cases}$

qui font commuter le diagramme $\begin{array}{ccc} G\times\operatorname{Aut}G & \overset{i\times j}{\hookrightarrow} & G^{\Diamond}\times\operatorname{Int}G^{\Diamond} \\ \downarrow \acute{e}v & & \downarrow \acute{e}v \\ G & \overset{i}{\hookrightarrow} & G^{\Diamond} \end{array}$. On montre aisément que ce dernier commute ssi $\forall\alpha\in\operatorname{Aut}G,\ \alpha'=\operatorname{int}_{g_\alpha^{-1}}\circ\alpha$. Sous cette hypothèse, et en supposant de plus G abélien, on montrerait facilement que j est un morphisme ssi[9] $\forall\alpha,\beta\in\operatorname{Aut}G,\ g_{\alpha\beta}=\alpha(g_\beta)+g_\alpha$ (le cas de l'exercice est celui où g_α vaut toujours 1).

Quotients. Soit G un groupe.

1. Montrons que les deux réponses sont "non" en général. Vu le cours, il faut chercher des monoïdes qui ne sont pas des groupes, donc il faut utiliser des non inversibles – par exemple des idempotents ou des nilpotents.

   Notons $a:=\begin{pmatrix}\cdot & 1\\ \cdot & \cdot\end{pmatrix}$. Si $M=\{1,a,0\}$ et $N=\{0,1\}$, la divisibilité étudiée tombe en défaut. Le théorème de Lagrange (concernant l'ordre des sous-trucs) est donc faux dans les monoïdes.

   Soient a une matrice et n un naturel tels que $a^{n+1}=a^n\neq a^{n-1}$. Si $M=\left\{1,a,a^2,...,a^n\right\}$ est le monoïde engendré par a et si N est le sous-monoïde $\{1,a^n\}$, alors les classes *modulo* N sont $\{1,a^n\}$, $\{a,a^n\}$, $\left\{a^2,a^n\right\}$, ..., $\{a^n,a^n\}$. On en déduit $\left|{}^{M}\!/_{N}\right|=|M|=\left|{}_{N}\backslash^{M}\right|$ alors que $|N|=2$. (La même idée s'adapterait en imposant $a^{n+1}=0\neq a^n$ et en supposant $M=\langle a\rangle$ et $N=\{0,1\}$.) Dans les deux cas, on a $\left|{}^{M}\!/_{N}\right||N|=2\,|M|=|N|\left|{}_{N}\backslash^{M}\right|$ qui ne peut valoir $|M|$ puisque ce dernier est non nul.

2. Supposons que A soit le translaté d'un sous-groupe. Soit $\alpha\in G$ tel que $B:=\alpha A$ soit un sous-groupe : vu les égalités $\{gA\}_{g\in G}=\left\{g\alpha^{-1}B\right\}_{g\in G}\overset{g\leftarrow h\alpha}{=}\{hB\}_{h\in G}$, on est ramené au cas où A est un sous-groupe. Alors les Ag sont les orbites de l'action du groupe A sur G, donc ces orbites partitionnent l'ensemble agi G. En appliquant l'inversion de G, on en déduit que ce dernier est également partitionné par les $(Ag)^{-1}=g^{-1}A^{-1}=g^{-1}A$ lorsque g décrit G, donc par les hA lorsque h décrit $G^{-1}=G$.

   Supposons que $\{gA\ ;\ g\in G\}$ partitionne G. Déjà, A ne peut être vide, sinon tous les gA le seraient et leur réunion G aussi. Soit $a\in A$. Montrons que $B:=a^{-1}A$ est un sous-groupe. Il contient déjà $a^{-1}a=1$. Observons pour la suite le fait suivant : puisque deux classes gA et hA se rencontrant sont égales, si B rencontre un translaté gB alors il contient ce dernier. Soit $b\in B$. Alors d'une part bB et B contiennent tous deux $b1=b$, d'où l'inclusion $bB\subset B$ qui montre (en faisant varier b) la stabilité de B par translation, d'autre part $b^{-1}B$ et B contiennent tous deux $b^{-1}b=1$, d'où l'appartenance $b^{-1}\in b^{-1}B\subset B$ qui montre la stabilité de B par inversion.

   L'exercice essaie en fait de donner sens à l'égalité ${}^{G}\!/_{A}=\{gA\ ;\ g\in G\}$, valide pour tout sous-groupe A, lorsque A n'est plus forcément un sous-groupe. Si notre exigence est que les éléments du quotient doivent partitionner l'ensemble quotienté (agi), alors l'exercice montre que A doit être le translaté d'un sous-groupe B et que dans ce cas le quotient "généralisé" est un quotient "standard", à savoir celui ${}^{G}\!/_{B}$ de l'action (à droite) du groupe B par composition sur G.

3. Soit $\overline{\varphi}:\ {}^{G}\!/_{\operatorname{Ker}\varphi}\longrightarrow\operatorname{Im}\varphi$ un morphisme faisant le diagramme. Notons π la projection *modulo* $\operatorname{Ker}\varphi$ et i l'injection $\operatorname{Im}\varphi\subset H$. On a alors pour tout $g\in G$ les égalités

   $$\overline{\varphi}(\overline{g})=\overline{\varphi}(\pi(g))=[\overline{\varphi}\circ\pi](g)=[i\circ\varphi](g)=i(\varphi(g))=\varphi(g),\text{ ce qui montre l'unicité de }\overline{\varphi}.$$

   Par ailleurs, le cours montre que l'application $\overline{\varphi}$ définie comme imposé par l'analyse ci-dessus est bien un isomorphisme de groupes.

4. Supposons que ${}^{G}\!/_{H}$ est un groupe pour la loi $\ \overline{a}\overline{b}:=\overline{ab}$. Soient $a\in G$ et $h\in H$. Vu les égalités $\begin{cases}\overline{1}=1H=H=\overline{h}\\ \overline{ah}=ahH=aH=\overline{a}\end{cases}$, on peut écrire $\overline{ha}=\overline{h}\ \overline{a}=\overline{1}\ \overline{ah}=\overline{1ah}=\overline{ah}$, d'où $ha\in\overline{ha}=\overline{ah}=ahH=aH$. Ceci montre l'inclusion $Ha\subset aH$, *i. e.* $a^{-1}H\subset Ha^{-1}$. Faire varier a dans tout G donne $bH\subset Hb$ pour tout $b\in G^{-1}=G$, ce qui montre l'égalité $Ha=aH$, d'où l'on tire $aHa^{-1}=Haa^{-1}=H$.

   Supposons réciproquement $\forall a\in G,\ aHa^{-1}=H$. On a alors (pour tous $a,b\in G$) les égalités

   $$\overline{a}\overline{b}=(aH)(bH)=a(Hb)H=a(bH)H=(ab)(HH)=abH=\overline{ab},$$

   ce qui montre que la projection canonique $G\twoheadrightarrow{}^{G}\!/_{H}$ est un morphisme de magmas (où la loi de ${}^{G}\!/_{H}$ est la composition des parties). La structure du groupe G se transfère alors sur ${}^{G}\!/_{H}$.

[9] Lorsque l'application $\alpha\mapsto g_\alpha$ vérifie cette dernière égalité, on dit que c'est un ***cocycle*** de G d'ordre 1. On effleure ici la ***cohomologie*** des groupes (qui sort complètement du cadre du cours).

La condition s'énonce "H est invariant par conjugaison" (on pourrait même remplacer "invariant" par "stable"). Le travail ci-dessus pourrait s'effectuer pour les classes à droite : dans les deux cas, on arriverait à la condition équivalente $\forall a \in G,\ aH = Ha$, montrant l'égalité des deux quotients ${}^{G}\!/_{H} = {}_{H}\!\backslash^{G}$.

Soit φ un morphisme de groupes de source G. Supposons $H = \operatorname{Ker}\varphi$. Montrons qu'il est stable par conjugaison. Soient $h \in H$ et $a \in G$. On a alors $\varphi\left(aha^{-1}\right) = \varphi(a)\,\varphi(h)\,\varphi\left(a^{-1}\right) = \varphi(a)\,1\varphi(a)^{-1} = 1$, d'où $aha^{-1} \in \operatorname{Ker}\varphi = H$, *c. q. f. d.*

5. Montrons que H est est un sous-groupe de G stable par conjugaison. Puisque $1 \in 1A = \overline{1} \in \mathcal{H}$, on a l'appartenance $1 \in \cup\mathcal{H} = H$. Soit $h \in H$, soit $g \in G$ tel que $h \in gA$: on alors les appartenances $h^{-1} \in A^{-1}g^{-1} \overset{A^{-1}=A}{=} g^{-1}gAg^{-1} \overset{A \text{ est invariant par conjugaison}}{=} g^{-1}A \in \mathcal{H}$, d'où $h^{-1} \in \cup\mathcal{H} = H$. Soit de plus $i \in H$: on a alors les appartenances $hi \in \overline{hi} = \overline{hi} \in \mathcal{H}$, d'où $hi \in \cup\mathcal{H} = H$. Soit enfin $x \in G$. On a alors les appartenances $xhx^{-1} \in xgAx^{-1} = xgx^{-1}A \in \mathcal{H}$, ce qui conclut.

   On se convaincra avant de poursuivre que $\mathcal{H}$ et ${}^{H}\!/_{A}$ sont tous deux des ensembles de classes *modulo* A, *i. e.* des parties de ${}^{G}\!/_{A}$. Montrons qu'elles sont égales. Soit $C \in \mathcal{H}$. Puisque $\mathcal{H} \subset {}^{G}\!/_{A}$, on peut invoquer un $g \in G$ tel que $C = gA$. Alors $g \in C \in \mathcal{H}$, donc $g \in H$ et $C = \overline{g} \in {}^{H}\!/_{A}$. Soit réciproquement $\Gamma \in {}^{H}\!/_{A}$. Soit $h \in H$ tel que $\Gamma = hA$. Soit $C \in \mathcal{H}$ tel que $h \in C$. Alors les deux classes C et Γ se rencontrent (en h), donc sont égales, d'où l'appartenance $\Gamma = C \in \mathcal{H}$.

6. Appelons ***rétraction*** du sous-groupe H toute endomorphisme ρ de G tel que $\begin{cases} \rho_{|H} = \mathrm{Id}_H \\ \operatorname{Im}\rho \subset H \end{cases}$. Ce qui suit est plus prétexte à digressions qu'une réponse succincte aux questions posées.

   (a) Par exemple, lorsque G et H sont des espaces vectoriels, ces conditions équivalent à ce que ρ soit un projecteur sur[10] H. Plaçons-nous dans ce cadre vectoriel. Puisque la loi du groupe G est alors commutative, toutes les conjugaisons sont triviales et H est bien stable par conjugaison. Soit S un supplémentaire de H. Est alors un isomorphisme $\begin{cases} S \times H & \widetilde{\longrightarrow} & G \\ (s,h) & \longmapsto & s+h \end{cases}$. Notons π la projection *modulo* H. Ses noyau et image étant H et S, elle induit un isomorphisme ${}^{G}\!/_{H} \widetilde{\longrightarrow} S$, d'où l'on déduit un isomorphisme $\begin{cases} {}^{G}\!/_{H} \times H & \widetilde{\longrightarrow} & G \\ (\pi(s), h) & \longmapsto & s+h \end{cases}$ dont la réciproque est le produit $\begin{cases} G & \widetilde{\longrightarrow} & {}^{G}\!/_{H} \times H \\ g & \longmapsto & (\pi(g), p(g)) \end{cases}$ des applications linéaires π et p (où l'on noté p le projecteur sur H parallèlement à S).

   Tout ce que l'on a fait, c'est remplacer dans le couple $(\mathrm{Id} - p, p)$ réalisant un isomorphisme $G = S \oplus H \underset{p}{\overset{\mathrm{Id}-p}{\widetilde{\longrightarrow}}} S \times H$ le projecteur $\mathrm{Id} - p : G \twoheadrightarrow S$ par la projection $\pi : G \twoheadrightarrow {}^{G}\!/_{H}$.

   (b) Soit $\rho : G \twoheadrightarrow H$ une rétraction de H. Notons encore π la projection *modulo* H. Montrons (inspiré par le cas vectoriel ci-dessus) que le morphisme produit $\varphi : \begin{cases} G & \longrightarrow & {}^{G}\!/_{H} \times H \\ g & \longmapsto & (\pi(g), \rho(g)) \end{cases}$ est un isomorphisme. Soit $g \in \operatorname{Ker}\varphi$: l'égalité $\pi(g) = \overline{1}$ signifie $g \in H$, d'où l'on tire $g = \rho(g) = 1$. Ainsi φ est-il injectif. Pour la surjectivité, il suffit de montrer que φ atteint toute partie génératrice de ${}^{G}\!/_{H} \times H$, par exemple $\left\{\overline{1}\right\} \times H$ et ${}^{G}\!/_{H} \times \{1\}$. Pour la première, on observera pour tout $h \in H$ les égalités $\left(\overline{1}, h\right) = \left(\overline{h}, \rho(h)\right) = \varphi(h)$. Pour la seconde, on observera pour tout $g \in G$ (en abrégeant $\gamma := \rho(g)^{-1}$) les égalités $(\overline{g}, 1) \overset{\gamma \in H}{=} (\overline{g}\ \overline{\gamma}, \rho(g)\,\gamma) \overset{\rho_{|H}=\mathrm{Id}}{=} (\overline{g\gamma}, \rho(g\gamma)) = \varphi(g\gamma)$.

   Compléments. Comme pour les espaces vectoriels, en notant $\begin{cases} H' := \operatorname{Ker}\rho \text{ et} \\ \rho' : x \mapsto \rho(x)^{-1}\,x \end{cases}$, on montrerait (penser en termes de projecteurs) les égalités $\begin{cases} \operatorname{Fix}\rho = H = \operatorname{Ker}\rho' = \operatorname{Im}\rho \\ \operatorname{Fix}\rho' = H' = \operatorname{Ker}\rho = \operatorname{Im}\rho' \end{cases}$, que ρ' est une rétraction de H' telle que $\rho\rho' = \mathrm{Id}$, que le couple (ρ, ρ') réalise un isomorphisme $G \widetilde{\longrightarrow} H \times H'$ de réciproque $(h, h') \mapsto hh'$, que $G = H \odot H'$ est composé direct de H et H' et que π induit un isomorphisme ${}^{G}\!/_{H} \simeq H'$ de réciproque induite par ρ'. Réciproquement, si l'on a une telle décomposition $G = H \odot H'$, alors les morphismes $\begin{matrix} \rho : hh' \mapsto h \\ \rho' : hh' \mapsto h' \end{matrix}$ sont des rétractions de H et H' de produit Id_G et dont le couple réalise un isomorphisme $G \widetilde{\longrightarrow} H \times H'$.

   Généralisation. On observera que l'isomorphisme (π, ρ) trouvé utilise la projection *modulo* H pour définir son abscisse (quoi de plus "naturel" pour définir une image dans ${}^{G}\!/_{H}$?) et la

[10] et il y en existe : l'axiome du choix permet en toute dimension d'invoquer un supplémentaire de H, ce qui permet définir le projecteur sur H parallèlement à ce supplémentaire

rétraction ρ pour son ordonnée. C'est affirmer la commutativité du diagramme

$$\begin{array}{ccccc} & \overset{\pi}{\twoheadleftarrow} & G & \overset{\rho}{\twoheadrightarrow} & \\ {}^{G}\!/_{H} & & \downarrow\simeq & & H \\ & \twoheadleftarrow & {}^{G}\!/_{H} \times H & \twoheadrightarrow & \end{array}$$

où les flèches du bas sont les projections sur les coordonnées.

Remarquer également que l'on aurait pu composer π et ρ à gauche respectivement par tout isomorphisme $i : A \simeq {}^{G}\!/_{H}$ et $\sigma : B \simeq H$, ce qui aurait fournit d'autres isomorphismes $G \xrightarrow{\sim} {}^{G}\!/_{H} \times H$ faisant chacun commuter un diagramme $\begin{array}{ccccc} {}^{G}\!/_{H} & \overset{\pi}{\twoheadleftarrow} & G & \overset{\rho}{\twoheadrightarrow} & H \\ \simeq\downarrow i & & \downarrow\simeq & & \simeq\downarrow \sigma \\ A & \twoheadleftarrow & A \times B & \twoheadrightarrow & B \end{array}$.

(c) Supposons réciproquement (et un peu plus généralement) que G est isomorphe à un produit $A \times B$ de sorte à faire commuter le diagramme $\begin{array}{ccc} {}^{G}\!/_{H} & \overset{\pi}{\twoheadleftarrow} & G \\ \downarrow i & & \downarrow\simeq \\ A & \twoheadleftarrow & A \times B \end{array}$ où i est injectif (on avait $(A, B) = \left({}^{G}\!/_{H}, H\right)$ et $i = \mathrm{Id}$ dans le cas ci-dessus). Montrons alors que les groupes A et B doivent être isomorphes respectivement à ${}^{G}\!/_{H}$ et à H et que ce dernier admet une rétraction. Mieux (les diagrammes vont permettre d'avoir une unicité) : *montrons qu'il y a un unique isomorphisme* $H \overset{\sigma}{\simeq} B$ *et une unique rétraction* $G \overset{\rho}{\twoheadrightarrow} H$ *faisant commuter le diagramme* $\begin{array}{ccccc} {}^{G}\!/_{H} & \overset{\pi}{\twoheadleftarrow} & G & \overset{\rho}{\twoheadrightarrow} & H \\ \simeq\downarrow i & & \downarrow\simeq & & \simeq\downarrow \sigma \\ A & \twoheadleftarrow & A \times B & \twoheadrightarrow & B \end{array}$ *(où les flèches du bas sont les projections sur les coordonnées).*

Appelons φ l'isomorphisme $G \xrightarrow{\sim} A \times B$ invoqué.

Analyse. Notons $\beta : G \twoheadrightarrow B$ la composée de φ par $\twoheadrightarrow$, qui doit valoir $\sigma \circ \rho$. Restreindre à H donne $\beta_{|H} = [\sigma \circ \rho]_{|H} = \sigma \circ \rho_{|H} = \sigma \circ \mathrm{Id}_H = \sigma$, ce qui impose σ, d'où l'on déduit $\rho = \sigma^{-1} \circ \beta$.

Synthèse. Montrons que $\sigma := \beta_{|H} : H \longrightarrow B$ est un isomorphisme. Soit $h \in H$ tel que $\sigma(h) = 1$. On a alors $\varphi(h) = \left(i\left(\overline{h}\right), \beta(h)\right) = \left(i\left(\overline{1}\right), \beta_{|H}(h)\right) = \left(\overline{1}, \sigma(h)\right) = \left(\overline{1}, 1\right)$, d'où $h = 1$ par injectivité de φ. Soit $b \in B$. Par surjectivité de φ, on peut invoquer un $g \in G$ tel que $\varphi(g) = \left(\overline{1}, b\right)$. L'abscisse donne $i(\overline{g}) = \overline{1}$, *i. e.* (par injectivité de i) $\overline{g} = \overline{1}$, *i. e.* $g \in H$, donc l'ordonnée donne $b = \beta(g) = \beta_{|H}(g) = \sigma(g)$. L'analyse nous suggère alors très fortement de définir $\rho := \sigma^{-1} \circ \beta$. Les morphismes σ et ρ font par définition commuter le diagramme précédent. Il reste à montrer que ρ est une rétraction de H, ce qui vient d'une part des inclusions $\mathrm{Im}\,\rho = \mathrm{Im}\left(\sigma^{-1} \circ \beta\right) \subset \mathrm{Im}\left(\sigma^{-1}\right) \subset H$, d'autre part des égalités $\rho_{|H} = \left[\sigma^{-1} \circ \beta\right]_{|H} = \sigma^{-1} \circ \left[\beta_{|H}\right] = \left[\beta_{|H}\right]^{-1} \circ \beta_{|H} = \mathrm{Id}_H$.

(d) Montrons enfin (afin de motiver l'introduction des diagrammes dans les hypothèses) que la donnée d'un isomorphisme $\varphi : \left\{ \begin{array}{ccc} G & \xrightarrow{\sim} & {}^{G}\!/_{H} \times H \\ g & \longmapsto & (\Gamma(g), \beta(g)) \end{array} \right.$ *ne permet pas toujours* de récupérer une rétraction de H *via* l'ordonnée. On pourra même supposer Γ d'une forme sympathique où π apparaît : pas $g \mapsto i(\overline{g})$ (vu la démonstration ci-dessus), plutôt $g \mapsto \overline{\gamma(g)}$ pour un certain $\gamma \in \mathrm{Aut}\, G$. Toutes ces hypothèses se résument en un diagramme commutatif $\begin{array}{ccccc} G & \overset{\gamma}{\xleftarrow{\sim}} & G & \overset{\beta}{\twoheadrightarrow} & \\ \downarrow\pi & & \simeq\downarrow\varphi & & H \\ {}^{G}\!/_{H} & \twoheadleftarrow & {}^{G}\!/_{H} \times H & \twoheadrightarrow & \end{array}$

Idée. L'application β est candidate mais il se pourrait très bien que $\sigma := \beta_{|H}$ ne fixe pas H ; ce (faux-)problème est pallié en remplaçant le candidat β par $\sigma^{-1} \circ \beta$, lequel va alors fixer H et d'être image $\subset H$, donc sera une rétraction de H. Mais tout cela ne fera sens que si l'on peut parler de σ^{-1}, *i. e.* si l'on montre que $\sigma \in \mathrm{Aut}\, H$ – et c'est là que le bât blesse.

Mise en œuvre.

• Essayons de montrer la surjectivité de σ. Soit $h \in H$. [Micro analyse : si a est un antécédent de h par σ, alors $\varphi(a) = (\Gamma(a), h)$ et donc h vaut $\varphi^{-1}(\overline{x}, h)$ pour un certain $x \in G$.] Soit $x \in G$ à choisir convenablement. La surjectivité de φ nous permet d'invoquer un $a \in G$ tel que $\varphi(a) = (\overline{x}, h)$. L'abscisse donne $\overline{\gamma(a)} = \overline{x}$, *i. e.* $\gamma(a) \in xH$ ou encore $a \in \gamma^{-1}(xH)$. On aimerait alors choisir x tel que $\gamma^{-1}(xH) \subset H$ pour avoir $a \in H$ et que l'égalité $\sigma(a) = h$ fasse sens.

• Cependant, si l'on pense en termes affines, les translatés $x + H$ gardent la même direction et n'ont aucun raison de rester inclus dans $\gamma(H)$ si γ fait "tourner" les directions, par exemple si $(G, H) = (\mathbf{C}, \mathbf{R})$ et si $\gamma = i\,\mathrm{Id}$ est la rotation d'un quart de tour. Cette idée va en fait engendrer toute une classe de contre-exemples.

• Essayons cette fois de montrer l'injectivité de σ : vu (à $h \in \operatorname{Ker}\sigma$ fixé) les équivalences

$$h = 1 \iff \begin{pmatrix}\overline{1}\\ 1\end{pmatrix} = \varphi(h) = \begin{pmatrix}\overline{\gamma(h)}\\ \beta(h)\end{pmatrix} = \begin{pmatrix}\overline{\gamma(h)}\\ 1\end{pmatrix} \iff \overline{\gamma(h)} = \overline{1} \iff \gamma(h) \in H,$$

l 'injectivité de σ équivaut à l'inclusion $\gamma(\operatorname{Ker}\sigma) \subset H$ et découlerait donc de celle $\gamma(H) \subset H$. Or on va carrément réaliser un σ nul (donc de noyau H) et faire tourner les directions pour que $\gamma(H)$ et H soient en somme directe (orthogonaux dans notre exemple complexe).

Contre-exemples. On suppose que G et H sont des espaces vectoriels non nuls tels que $\dim H = \operatorname{codim} H$. Soient S un supplémentaire de H et $\gamma \in \operatorname{Aut} G$ tel que $\begin{pmatrix}\gamma(S)\\ \gamma(H)\end{pmatrix} = \begin{pmatrix}H\\ S\end{pmatrix}$. (Par exemple, $(S,H) = (i\mathbf{R},\mathbf{R})$ et $\gamma = i\operatorname{Id}$.) Notons p et q les projecteurs sur H et sur S parallèlement à l'autre. La composées des isomorphismes $G \underset{q}{\overset{p}{\xrightarrow{\sim}}} H \times S \underset{\gamma_{|S}}{\overset{\gamma_{|H}}{\xrightarrow{\sim}}} S \times H \underset{\mathrm{Id}_{|H}}{\overset{\pi_{|S}}{\xrightarrow{\sim}}} {}^{G}\!/_{H} \times H$ réalise alors un isomorphisme

$$\left\{\begin{array}{ccc} G & \xrightarrow{\sim} & {}^{G}\!/_{H} \times H \\ \underset{S}{\Uparrow} + \underset{H}{\Uparrow} & \longmapsto & \begin{pmatrix}\overline{\gamma(h)}\\ \gamma(s)\end{pmatrix} \end{array}\right. \qquad \left(\begin{array}{c}\text{observer les égalités } \pi(\gamma(s+h)) \\ = \underbrace{\overline{\gamma(s)}}_{\in H} + \overline{\gamma(h)} = \overline{0} + \gamma(h) = \overline{\gamma(h)}\end{array}\right)$$

faisant commuter le diagramme $\begin{array}{ccccc} G & \overset{\gamma}{\xrightarrow{\sim}} & G & \overset{q}{\twoheadrightarrow} & S \\ \downarrow \pi & & \simeq\downarrow \varphi & & \simeq\downarrow \gamma \\ {}^{G}\!/_{H} & \twoheadleftarrow & {}^{G}\!/_{H} \times H & \twoheadrightarrow & H \end{array}$. Mais le morphisme ordonnée $\gamma \circ q : G \twoheadrightarrow H$ ne peut induire un automorphisme de H puisque son noyau contient $\operatorname{Ker} q = H$ (et que H est non nul).

Actions.

1.

(a) Soit $f \in F$. Vu que $\mathbf{F}_p$ est engendré par $\overline{1}$, on a les équivalences

$$f \in \Phi \iff [\forall a \in \mathbf{F}_p,\ a \cdot f = f] \iff \overline{1} \cdot f = f \iff \forall n \in \mathbf{Z},\ f(\overline{n}) = f\left(\overline{n+1}\right) \iff f \text{ constante.}$$

Par ailleurs, pour tout $c \in G^{\mathbf{F}_p}$ constante, on a les équivalences

$$c \in F \iff \prod_{a \in \mathbf{F}_p} c(a) = 1 \iff c^p = 1 \iff c \text{ vaut constamment une racine } p\text{-ième de } 1,$$

d'où suit l'équivalence f constante$\iff f$ vaut constamment une racine p-ième de 1.

Supposons que p divise $|\Phi|$. Alors Φ n'est pas réduit au groupe trivial : soit $c \neq 1_F$ dedans. La valeur constante de c ne vaut 1 et est d'après ce qui précède d'ordre au plus p, donc est d'ordre p exactement, ce qui conclut.

(b) Soit $f \in F$. L'égalité $\#\operatorname{Orb} f\ \#\operatorname{Fix} f = \#\mathbf{F}_p = p$ et la primalité de p montrent que $\begin{pmatrix}\#\operatorname{Fix} f\\ \#\operatorname{Orb} f\end{pmatrix}$ ne peut prendre que deux valeurs. Ces deux cas disjoints sont décrits par les équivalences

$$\begin{array}{rcl} \begin{pmatrix}\#\operatorname{Fix} f\\ \#\operatorname{Orb} f\end{pmatrix} & = & \begin{pmatrix}1\\ p\end{pmatrix} \iff |\operatorname{Orb} f| = p \overset{\#\operatorname{Orb} f \mid \#\mathbf{F}_p}{\iff} p \mid \#\operatorname{Orb} f \quad \text{et} \\ \begin{pmatrix}\#\operatorname{Fix} f\\ \#\operatorname{Orb} f\end{pmatrix} & = & \begin{pmatrix}p\\ 1\end{pmatrix} \iff |\operatorname{Fix} f| = |\mathbf{F}_p| \overset{\operatorname{Fix} f \subset \mathbf{F}_p}{\iff} \operatorname{Fix} f = \mathbf{F}_p \iff f \in \Phi. \end{array}$$

(c) Une fonction de F est définie par $p-1$ valeurs, la dernière étant fixée par l'égalité $\prod_{a \in \mathbf{F}_p} f(a) = 1$. Proprement, on a une bijection $\left\{\begin{array}{ccc} F & \longrightarrow & G^{p-1} \\ f & \longmapsto & (f(\overline{a}))_{1 \leq a < p} \\ \left\{\begin{array}{l} 0 \mapsto \left(\prod g_i\right)^{-1} \\ i \in [1,p[\mapsto g_i \end{array}\right. & \longleftarrow & (g_i)_{1 \leq i < p} \end{array}\right.$, d'où l'égalité des cardinaux $|F| = \left|G^{p-1}\right| = |G|^{p-1}$. Puisque $p \mid \#G$, on en déduit que $|F|$ est nul *modulo* p.

L'équation aux classes s'écrit $|F| = \sum_{f \in T} |\operatorname{Orb} f|$ pour une certaine transversale $T \subset F$. Cette dernière contient d'une part tous les élément seuls dans leur orbite, *i. e.* les éléments de Φ (contribution à la somme : $|\Phi|$), d'autre part des éléments dont l'orbite a p éléments (contribution à la somme : un multiple de p). *Modulo* p, cela s'écrit $0 = |\Phi| + 0$, *i. e.* $p \mid \#\Phi$, ce qui conclut.

2. L'équation aux classes s'écrit $\left|{}^{G}\!/_{S}\right| = \sum_{\overline{g}\in T} |\mathrm{Orb}\,\overline{g}|$ pour une certaine transversale $T \subset {}^{G}\!/_{S}$. Cette dernière contient d'une part tous les élément seuls dans leur orbite, *i. e.* les éléments de $\{\overline{g}\ ;\ \mathrm{Fix}\,\overline{g} = H\}$, d'autre part des éléments dont l'orbite a pour cardinal un diviseur de $|H|$ autre que 1, en particulier (vu que H est un p-groupe) une puissance non triviale de p. Puisque S est un p-Sylow, le cardinal $\left|{}^{G}\!/_{S}\right| = \frac{|G|}{|S|}$ n'est pas multiple de p. Finalement, *modulo* p, l'équation aux classes implique $0 \neq \left|{}^{G}\!/_{S}\right| = \#\{\overline{g}\ ;\ \mathrm{Fix}\,\overline{g} = H\} + 0$, d'où la non-nullité de $\#\{\overline{g}\ ;\ \mathrm{Fix}\,\overline{g} = H\}$ et la non-vacuité cherchée.

Soit $g \in G$ tel que $\mathrm{Fix}\,\overline{g} = H$. Soit $h \in H$. Puisque $h \cdot \overline{g} = \overline{g}$, on a l'appartenance $hg \in hgS = gS$, d'où $h \in gSg^{-1}$, ce qui montre l'inclusion $H \subset gSg^{-1}$ et la conclusion (si de plus H est un p-Sylow, l'égalité des cardinaux implique l'égalité ensembliste $H = gSg^{-1}$, montrant que H est conjugué à S).