CORRIGÉ – CHAPITRE 4

MORPHISMES

Morphismes de groupes

EXERCICE 1 ⋆

Il s'agit à chaque fois de comparer $f(x \cdot y)$ et $f(x) * f(y)$, en prenant garde aux deux lois, qui ne sont pas toujours les mêmes au départ et à l'arrivée.

1. Pour tous réels x et y : $3(x+y) = 3x+3y$. Morphisme.

2. On a $f(x+y) = x+y+1$ alors que $f(x)+f(y) = x+y+2$. Non : prendre $x = y = 0$.

3. On a $f(1+1) = 4$ alors que $f(1)+f(1) = 2$. Non.

4. Pour tous réels non nuls : $(xy)^2 = x^2y^2$. Morphisme.

5. La conjugaison vérifie $\overline{z+z'} = \overline{z}+\overline{z'}$. Morphisme.

6. Le module vérifie $|zz'| = |z|\,|z'|$, et $|z| > 0$ pour $z \neq 0$. Morphisme.

7. Le logarithme vérifie $\ln(xy) = \ln(x)+\ln(y)$ sur $\mathbb{R}_+^*$. Morphisme.

8. Pour tous entiers : $5(k+k') = 5k+5k'$. Morphisme.

9. On a $f(0+0) = 5$ alors que $f(0)+f(0) = 10$. Non.

10. L'exponentielle vérifie $\mathrm{e}^{x+y} = \mathrm{e}^x\,\mathrm{e}^y$. Morphisme.

11. Pour tous réels non nuls : $\dfrac{1}{xy} = \dfrac{1}{x} \times \dfrac{1}{y}$. Morphisme.

12. Pour tous réels non nuls : $\ln|xy| = \ln\left(|x|\,|y|\right) = \ln|x| + \ln|y|$. Morphisme.

Piège des questions 3 et 4 : c'est la même formule $x \mapsto x^2$, mais pas les mêmes lois. Elle respecte la multiplication, pas l'addition : la propriété dépend des *trois* composantes de l'application, comme au chapitre 2.

EXERCICE 2 ⋆

Un *endomorphisme* va d'un groupe dans lui-même, un *isomorphisme* est un morphisme bijectif, un *automorphisme* est les deux à la fois.

	Nature	**Justification**
1. $x \mapsto 3x$	automorphisme	Même groupe au départ et à l'arrivée, bijectif de réciproque $y \mapsto \frac{y}{3}$.
4. $x \mapsto x^2$ sur $\mathbb{R}^*$	endomorphisme seul	$f(-1) = f(1) = 1$: non injectif.
5. $z \mapsto \overline{z}$	automorphisme	Bijectif, de réciproque lui-même.
6. $z \mapsto \lvert z\rvert$	aucun des trois	Groupes différents, et non injectif.
7. $x \mapsto \ln(x)$	isomorphisme	Bijectif, de réciproque exp ; groupes différents.
8. $k \mapsto 5k$	endomorphisme seul	Injectif, mais 1 n'a pas d'antécédent.
10. $x \mapsto \mathrm{e}^x$	isomorphisme	Bijectif, de réciproque ln ; groupes différents.
11. $x \mapsto \frac{1}{x}$	automorphisme	Bijectif, de réciproque lui-même.
12. $x \mapsto \ln\lvert x\rvert$	aucun des trois	Groupes différents, et $f(-1) = f(1) = 0$.

Piège : les questions 7 et 10 fournissent des isomorphismes, mais *pas* des automorphismes : les groupes de départ et d'arrivée sont différents, même s'ils sont isomorphes.

EXERCICE 3 ⋆⋆

1. D'après la propriété 3 du chapitre 3, on a toujours $\iota(xy) = (xy)^{-1} = y^{-1}x^{-1}$, tandis que $\iota(x)\,\iota(y) = x^{-1}y^{-1}$. Ainsi :

$$\iota \text{ est un morphisme } \iff \forall (x\,;y) \in G^2,\ y^{-1}x^{-1} = x^{-1}y^{-1}$$

Or, lorsque x et y parcourent G, les éléments $a = x^{-1}$ et $b = y^{-1}$ parcourent également G tout entier. La condition s'écrit donc $ba = ab$ pour tous a et b de G.

$$\boxed{\iota \text{ est un morphisme si et seulement si } G \text{ est abélien.}}$$

2. On compare de même :

$$c(xy) = (xy)^2 = xyxy \qquad \text{et} \qquad c(x)\,c(y) = x^2y^2 = xxyy$$

L'égalité $xyxy = xxyy$ équivaut, par régularité à gauche par x puis à droite par y, à $yx = xy$.

$$\boxed{c \text{ est un morphisme si et seulement si } G \text{ est abélien.}}$$

3. Le groupe $\mathcal{S}(\{1\,;2\,;3\})$ n'est pas abélien : l'exercice 11 du chapitre 3 exhibe deux permutations σ et τ telles que $\sigma \circ \tau \neq \tau \circ \sigma$.

$$\boxed{\text{Ni } \sigma \mapsto \sigma^{-1},\ \text{ni } \sigma \mapsto \sigma \circ \sigma \text{ n'est un morphisme de ce groupe.}}$$

Propriétés élémentaires et isomorphismes

EXERCICE 4 ⋆

1. Montrons par récurrence que $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{N}$.
Initialisation. Pour $n = 0$, on a $x^0 = e_G$ et $f(e_G) = e_H = f(x)^0$ d'après la propriété 1.
Hérédité. Supposons la formule vraie au rang n. Alors :

$$f(x^{n+1}) = f(x^n \cdot x) = f(x^n) * f(x) = f(x)^n * f(x) = f(x)^{n+1}$$

Extension à $\mathbb{Z}$. Soit $n < 0$, et posons $m = -n > 0$. La propriété 1 donne :

$$f(x^n) = f\Big((x^m)^{-1}\Big) = f(x^m)^{-1} = \Big(f(x)^m\Big)^{-1} = f(x)^{-m} = f(x)^n$$

$$\boxed{\forall n \in \mathbb{Z},\quad f(x^n) = f(x)^n}$$

2. Un morphisme envoie le neutre sur le neutre : il suffit donc de calculer l'image du neutre de départ.

$$\boxed{\begin{array}{ll} \textbf{(a)}\ f(0) = 1 \neq 0 & \textbf{(b)}\ f(1) = 2 \neq 1 \\ \textbf{(c)}\ f(0) = \mathrm{i} \neq 0 & \textbf{(d)}\ f(0) = -3 \neq 0 \end{array}}$$

$$\boxed{\text{Aucune de ces quatre applications n'est un morphisme.}}$$

Remarque : ce test est instantané et doit devenir un réflexe. Il ne prouve rien lorsqu'il est concluant — une application peut envoyer le neutre sur le neutre sans être un morphisme, comme $x \mapsto x^2$ sur $(\mathbb{R}\,;+)$ — mais il élimine immédiatement un mauvais candidat.

3. La loi étant notée additivement des deux côtés, la question 1 s'écrit ici $g(nx) = n\,g(x)$. Appliquée à $x = 1$:

$$\boxed{\forall n \in \mathbb{Z}, \quad g(n) = n\,g(1)}$$

Soit maintenant $q \in \mathbb{N}^*$. En appliquant ce qui précède à $x = \dfrac{1}{q}$ et $n = q$:

$$g(1) = g\left(q \times \frac{1}{q}\right) = q\,g\left(\frac{1}{q}\right) \qquad \text{donc} \qquad g\left(\frac{1}{q}\right) = \frac{g(1)}{q}$$

Enfin, pour $r = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$:

$$g(r) = g\left(p \times \frac{1}{q}\right) = p\,g\left(\frac{1}{q}\right) = \frac{p}{q}\,g(1)$$

$$\boxed{\forall r \in \mathbb{Q}, \quad g(r) = r\,g(1)}$$

Un morphisme de $(\mathbb{R}\,;+)$ dans lui-même est donc entièrement déterminé sur $\mathbb{Q}$ par la seule valeur $g(1)$.

EXERCICE 5 ⋆⋆

1. Pour tout réel x, $\ln\left(\mathrm{e}^x\right) = x$, et pour tout réel $x > 0$, $\mathrm{e}^{\ln(x)} = x$.

$$\boxed{g \circ f = \mathrm{Id}_{\mathbb{R}} \qquad \text{et} \qquad f \circ g = \mathrm{Id}_{\mathbb{R}_+^*}}$$

Les applications f et g sont donc réciproques l'une de l'autre : ce sont deux isomorphismes.

2. La composée $g \circ f$ est un morphisme d'après la propriété 2 du cours, et elle est bijective comme composée de deux bijections (chapitre 2).

$$\boxed{g \circ f \text{ est un isomorphisme de } G \text{ sur } K.}$$

3. Un automorphisme de G étant en particulier une bijection de G dans G, on a $\mathrm{Aut}(G) \subset \mathcal{S}(G)$.

L'application Id_G est bijective, et c'est un morphisme puisque $\mathrm{Id}_G(xy) = xy = \mathrm{Id}_G(x)\,\mathrm{Id}_G(y)$: elle appartient à $\mathrm{Aut}(G)$, qui n'est donc pas vide.

Soient enfin f et h dans $\mathrm{Aut}(G)$. D'après la propriété 2, h^{-1} est un morphisme, et c'est une bijection : $h^{-1} \in \mathrm{Aut}(G)$. La question 2 donne alors que $f \circ h^{-1}$ est un automorphisme.

$$\boxed{\mathrm{Aut}(G) \text{ est un sous-groupe de } \mathcal{S}(G).}$$

EXERCICE 6 ⋆⋆

1. Soient h et h' dans G. En intercalant $g^{-1}g = e$:

$$\varphi_g(hh') = g\,hh'\,g^{-1} = g\,h\,\underbrace{g^{-1}g}_{=e}\,h'\,g^{-1} = (ghg^{-1})(gh'g^{-1}) = \varphi_g(h)\,\varphi_g(h')$$

$$\boxed{\varphi_g \text{ est un morphisme de } G \text{ dans } G.}$$

2. Pour tout $h \in G$:

$$(\varphi_g \circ \varphi_{g^{-1}})(h) = g(g^{-1}hg)g^{-1} = h \qquad (\varphi_{g^{-1}} \circ \varphi_g)(h) = g^{-1}(ghg^{-1})g = h$$

Les deux composées valent Id_G :

$$\boxed{\varphi_g \text{ est bijective, et } \varphi_g^{-1} = \varphi_{g^{-1}}.}$$

3. Les deux questions précédentes se combinent :

$$\boxed{\varphi_g \text{ est un endomorphisme bijectif de } G \text{ : c'est un automorphisme.}}$$

4. On enchaîne les équivalences :

$$\varphi_g = \mathrm{Id}_G \iff \forall h \in G,\ ghg^{-1} = h \iff \forall h \in G,\ gh = hg$$

la dernière équivalence s'obtenant en multipliant à droite par g.

$$\boxed{\varphi_g = \mathrm{Id}_G \iff g \in C(G)}$$

5. Pour tous g, g' et h de G :

$$(\varphi_g \circ \varphi_{g'})(h) = g(g'hg'^{-1})g^{-1} = (gg')\,h\,(g'^{-1}g^{-1}) = (gg')\,h\,(gg')^{-1} = \varphi_{gg'}(h)$$

en utilisant la propriété 3 du chapitre 3 pour l'inverse d'un produit.

$$\boxed{\varphi_g \circ \varphi_{g'} = \varphi_{gg'},\ \text{donc } \Phi : g \mapsto \varphi_g \text{ est un morphisme de } (G\,;\cdot) \text{ dans } (\mathrm{Aut}(G)\,;\circ).}$$

D'après la question 4, le noyau de Φ est exactement le centre $C(G)$. On retrouve ainsi, par la proposition 3, que $C(G)$ est un sous-groupe de G — résultat établi à la main au chapitre 3.

EXERCICE 7 ⋆⋆

1. L'exponentielle vérifie $\mathrm{e}^{x+y} = \mathrm{e}^x\mathrm{e}^y$ et réalise une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$, de réciproque ln.

$$\boxed{x \mapsto \mathrm{e}^x \text{ est un isomorphisme de } (\mathbb{R}\,;+) \text{ sur } (\mathbb{R}_+^*\,;\times).}$$

2. Posons $f : k \mapsto nk$, de $\mathbb{Z}$ dans $n\mathbb{Z}$. C'est un morphisme, car $n(k+k') = nk + nk'$. Son noyau est $\{k \in \mathbb{Z} \mid nk = 0\} = \{0\}$ puisque $n \neq 0$, donc f est injectif ; et tout élément de $n\mathbb{Z}$ s'écrit nk par définition, donc f est surjectif.

$$\boxed{k \mapsto nk \text{ est un isomorphisme de } (\mathbb{Z}\,;+) \text{ sur } (n\mathbb{Z}\,;+).}$$

3. Posons $\varphi : x \mapsto 1 + x$. L'identité établie au chapitre 3 donne, pour tous x et y de $\mathbb{R} \setminus \{-1\}$:

$$\varphi(x * y) = 1 + x + y + xy = (1+x)(1+y) = \varphi(x) \times \varphi(y)$$

De plus φ est une bijection de $\mathbb{R} \setminus \{-1\}$ sur $\mathbb{R}^*$, de réciproque $t \mapsto t - 1$.

$$\boxed{\varphi \text{ est un isomorphisme de } (\mathbb{R} \setminus \{-1\}\,;*) \text{ sur } (\mathbb{R}^*\,;\times).}$$

4. Posons $\psi : x \mapsto x - 3$. Pour tous entiers x et y :

$$\psi(x \perp y) = (x + y - 3) - 3 = (x-3) + (y-3) = \psi(x) + \psi(y)$$

et ψ est bijective de $\mathbb{Z}$ sur $\mathbb{Z}$, de réciproque $t \mapsto t + 3$.

$$\boxed{\psi \text{ est un isomorphisme de } (\mathbb{Z}\,;\perp) \text{ sur } (\mathbb{Z}\,;+).}$$

Les questions 3 et 4 confirment ce que le chapitre 3 laissait pressentir : ces lois inhabituelles ne sont que des lois connues, transportées par un changement de nom des éléments.

EXERCICE 8 ⋆⋆

1. Si $x + x = 0$, alors $2x = 0$, et comme $2 \neq 0$ dans $\mathbb{R}$, il vient $x = 0$.

$$\boxed{\text{Le seul réel vérifiant } x + x = 0 \text{ est } 0.}$$

2. Un tel réel existe :

$$\boxed{y = -1 \text{ convient, car } (-1) \times (-1) = 1 \text{ et } -1 \neq 1.}$$

3. Supposons qu'un tel isomorphisme f existe. Comme f est un morphisme :

$$f(-1) + f(-1) = f\big((-1) \times (-1)\big) = f(1) = 0$$

la dernière égalité venant de la propriété 1, le neutre de $(\mathbb{R}^* ; \times)$ étant 1 et celui de $(\mathbb{R} ; +)$ étant 0. D'après la question 1, on en déduit $f(-1) = 0 = f(1)$. Or f est injectif, donc $-1 = 1$: c'est absurde.

$$\boxed{(\mathbb{R}^* ; \times) \text{ et } (\mathbb{R} ; +) \text{ ne sont pas isomorphes.}}$$

4. L'argument repose entièrement sur l'existence, dans $\mathbb{R}^*$, d'un élément différent du neutre et égal à son propre inverse. Or dans $\mathbb{R}_+^*$, l'équation $y^2 = 1$ avec $y > 0$ n'a que la solution $y = 1$: l'argument tombe.

$$\boxed{\text{Non : et de fait, } (\mathbb{R}_+^* ; \times) \text{ et } (\mathbb{R} ; +) \text{ sont isomorphes par l'exponentielle.}}$$

Méthode à retenir : pour montrer que deux groupes ne sont *pas* isomorphes, on cherche une propriété préservée par tout isomorphisme — ici le nombre d'éléments égaux à leur propre symétrique — et vraie dans l'un, fausse dans l'autre.

Noyau et image

EXERCICE 9 ⋆

1. On a $H \subset G$, et $1 \in H$. De plus, pour z et z' dans $H = \{1 ; -1\}$, le produit zz'^{-1} vaut 1 ou -1 : H est bien un sous-groupe de G. Enfin :

$$1^2 = 1 \qquad \mathrm{i}^2 = -1 \qquad (-1)^2 = 1 \qquad (-\mathrm{i})^2 = -1$$

$$\boxed{H \text{ est un sous-groupe de } G, \text{ et } f \text{ est bien à valeurs dans } H.}$$

2. La multiplication des complexes étant commutative, pour tous z et z' de G :

$$f(zz') = (zz')^2 = z^2 z'^2 = f(z)\, f(z')$$

$$\boxed{f \text{ est un morphisme de } G \text{ dans } H.}$$

3. Sur le diagramme, deux flèches arrivent sur 1 et deux sur -1. Le noyau est l'ensemble des éléments envoyés sur le neutre 1 de H, et l'image l'ensemble des éléments atteints.

$$\boxed{\operatorname{Ker} f = \{1 ; -1\} \qquad \text{et} \qquad \operatorname{Im} f = \{1 ; -1\} = H}$$

On le retrouve par le calcul : $z^2 = 1$ équivaut à $z \in \{1 ; -1\}$, et le tableau des quatre carrés montre que les deux valeurs 1 et -1 sont atteintes.

4. Le noyau contient deux éléments, donc n'est pas réduit au neutre ; l'image est l'ensemble d'arrivée tout entier.

$$\boxed{f \text{ n'est pas injectif, mais il est surjectif.}}$$

EXERCICE 10 ⋆

1. Pour tous complexes non nuls, $|zz'| = |z|\,|z'|$: f_1 est un morphisme. Son image est l'ensemble des modules de complexes non nuls, c'est-à-dire les réels strictement positifs ; son noyau est l'ensemble des complexes de module 1.

$$\boxed{f_1 \text{ est un morphisme, } \operatorname{Im} f_1 = \mathbb{R}_+^* \text{ et } \operatorname{Ker} f_1 = \mathbb{U}.}$$

L'ensemble d'arrivée étant $\mathbb{R}^*$, ce morphisme n'est pas surjectif ; il n'est pas injectif non plus.

2. Pour tous $(a\,;b)$ et $(a'\,;b')$ de $\mathbb{Z}^2$:

$$f_2((a\,;b)+(a'\,;b')) = (a+a')-(b+b') = (a-b)+(a'-b') = f_2(a\,;b)+f_2(a'\,;b')$$

Tout entier a est atteint, par exemple par $(a\,;0)$, et $a-b=0$ équivaut à $a=b$.

$$\boxed{f_2 \text{ est un morphisme, } \operatorname{Im} f_2 = \mathbb{Z} \text{ et } \operatorname{Ker} f_2 = \{(a\,;a) \mid a \in \mathbb{Z}\}.}$$

3. Le logarithme vérifie $\ln(xy) = \ln(x) + \ln(y)$, atteint tout réel, et ne s'annule qu'en 1.

$$\boxed{f_3 \text{ est un morphisme, } \operatorname{Im} f_3 = \mathbb{R} \text{ et } \operatorname{Ker} f_3 = \{1\} \text{ : c'est un isomorphisme.}}$$

EXERCICE 11 ⋆

On cherche à chaque fois les antécédents du neutre d'arrivée, puis l'ensemble des valeurs atteintes.

1. $\boxed{\operatorname{Ker} = \{0\} \quad ; \quad \operatorname{Im} = \mathbb{R}}$ **2.** $\boxed{\operatorname{Ker} = \{-1\,;1\} \quad ; \quad \operatorname{Im} = \mathbb{R}_+^*}$

3. $\boxed{\operatorname{Ker} = \{0\} \quad ; \quad \operatorname{Im} = \mathbb{C}}$ **4.** $\boxed{\operatorname{Ker} = \{0\} \quad ; \quad \operatorname{Im} = 5\mathbb{Z}}$

5. $\boxed{\operatorname{Ker} = \{1\} \quad ; \quad \operatorname{Im} = \mathbb{R}^*}$ **6.** $\boxed{\operatorname{Ker} = \{-1\,;1\} \quad ; \quad \operatorname{Im} = \mathbb{R}}$

Piège : le noyau est l'ensemble des antécédents du neutre *d'arrivée*, qui vaut 0 pour une loi additive et 1 pour une loi multiplicative. Aux questions 2 et 5, chercher les x tels que $x^2 = 0$ ou $\frac{1}{x} = 0$ n'aurait aucun sens.

EXERCICE 12 ⋆⋆

Dans chaque cas, il suffit d'exhiber le bon morphisme : la proposition 3 fait le reste.

1. L'application $z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*\,;\times)$ dans $(\mathbb{R}_+^*\,;\times)$, dont le noyau est $\mathbb{U}$.

$$\boxed{\mathbb{U} \text{ est un sous-groupe de } (\mathbb{C}^*\,;\times).}$$

2. L'application $k \mapsto nk$ est un endomorphisme de $(\mathbb{Z}\,;+)$, d'image $n\mathbb{Z}$.

$$\boxed{n\mathbb{Z} \text{ est un sous-groupe de } (\mathbb{Z}\,;+).}$$

3. L'application $f_2 : (a\,;b) \mapsto a-b$ de l'exercice 10 est un morphisme de $(\mathbb{Z}^2\,;+)$ dans $(\mathbb{Z}\,;+)$, de noyau $\{(a\,;a) \mid a \in \mathbb{Z}\}$.

$$\boxed{\{(a\,;a) \mid a \in \mathbb{Z}\} \text{ est un sous-groupe de } (\mathbb{Z}^2\,;+).}$$

4. L'application $x \mapsto x^2$ est un endomorphisme de $(\mathbb{R}^*\,;\times)$, d'image $\mathbb{R}_+^*$.

$$\boxed{\mathbb{R}_+^* \text{ est un sous-groupe de } (\mathbb{R}^*\,;\times).}$$

Ces quatre résultats avaient demandé, au chapitre 3, autant de vérifications séparées. Un seul théorème les remplace toutes : c'est exactement le gain annoncé par le cours.

EXERCICE 13 ⋆⋆

1. *Sens réciproque.* Si $f(x) = ax$, alors $f(x+y) = a(x+y) = ax + ay = f(x) + f(y)$.

Sens direct. Supposons f morphisme et posons $a = f(1)$. La question 1 de l'exercice 4, écrite additivement, donne $f(n \times 1) = n\,f(1)$ pour tout $n \in \mathbb{Z}$, c'est-à-dire $f(n) = an$.

$$\boxed{f \text{ est un morphisme de } (\mathbb{Z}\,;+) \iff \exists a \in \mathbb{Z},\ \forall x \in \mathbb{Z},\ f(x) = ax}$$

(a) Le noyau est $\{x \in \mathbb{Z} \mid ax = 0\}$ et l'image l'ensemble des multiples de a.

$$\boxed{\text{Si } a \neq 0 \ :\ \operatorname{Ker} f = \{0\} \text{ et } \operatorname{Im} f = a\mathbb{Z} \qquad \text{si } a = 0 \ :\ \operatorname{Ker} f = \mathbb{Z} \text{ et } \operatorname{Im} f = \{0\}}$$

(b) Le morphisme est injectif si et seulement si $a \neq 0$, et surjectif si et seulement si $a\mathbb{Z} = \mathbb{Z}$, c'est-à-dire si a divise 1.

$$\boxed{f \text{ est un isomorphisme si et seulement si } a = 1 \text{ ou } a = -1.}$$

(c)

$$\boxed{\operatorname{Aut}(\mathbb{Z}\,;+) = \{\mathrm{Id}_{\mathbb{Z}}\ ;\ x \mapsto -x\}}$$

C'est donc un groupe à deux éléments, dans lequel chaque élément est son propre symétrique.

2. *Sens réciproque.* Si $f(x\,;y) = (ax+cy\,;\,bx+dy)$, un calcul direct sur chaque composante montre que f est un morphisme.

Sens direct. Supposons f morphisme, et posons $f(1\,;0) = (a\,;b)$ et $f(0\,;1) = (c\,;d)$. Comme $(x\,;y) = x\,(1\,;0) + y\,(0\,;1)$, la question 1 de l'exercice 4 donne :

$$f(x\,;y) = x\,f(1\,;0) + y\,f(0\,;1) = (ax\,;\,bx) + (cy\,;\,dy) = (ax+cy\,;\,bx+dy)$$

(a)

$$\boxed{\operatorname{Ker} f = \{(x\,;y) \in \mathbb{Z}^2 \mid ax + cy = 0 \text{ et } bx + dy = 0\}}$$

(b) *Supposons* $ad - bc \neq 0$, et soit $(x\,;y) \in \operatorname{Ker} f$. En combinant les deux équations :

$$d(ax+cy) - c(bx+dy) = (ad-bc)\,x = 0 \qquad \text{et} \qquad a(bx+dy) - b(ax+cy) = (ad-bc)\,y = 0$$

Comme $ad - bc \neq 0$, il vient $x = y = 0$, donc $\operatorname{Ker} f = \{(0\,;0)\}$ et f est injectif.

Supposons $ad - bc = 0$. Si $(c\,;a) \neq (0\,;0)$, le couple non nul $(-c\,;\,a)$ vérifie :

$$a(-c) + ca = 0 \qquad \text{et} \qquad b(-c) + da = ad - bc = 0$$

donc appartient au noyau. Si $(c\,;a) = (0\,;0)$, on vérifie de même que $(-d\,;\,b)$ convient ; et si de plus $(d\,;b) = (0\,;0)$, alors f est l'application nulle et $\operatorname{Ker} f = \mathbb{Z}^2$. Dans tous les cas, le noyau n'est pas réduit à $\{(0\,;0)\}$.

$$\boxed{f \text{ est injectif si et seulement si } ad - bc \neq 0.}$$

EXERCICE 14 ⋆⋆

1. On a $H \subset \mathbb{Z}^2$, et $(0\,;0) \in H$ puisque $0 - 0 = 0$ est pair. Soient $(a\,;b)$ et $(a'\,;b')$ dans H. Alors :

$$(a\,;b) - (a'\,;b') = (a-a'\,;\,b-b') \qquad \text{et} \qquad (a-a') - (b-b') = (a-b) - (a'-b')$$

qui est une différence de deux entiers pairs, donc un entier pair.

$$\boxed{H \text{ est un sous-groupe de } (\mathbb{Z}^2\,;+).}$$

2. *f est bien à valeurs dans H.* Pour tout $(u\,;v) \in \mathbb{Z}^2$: $(2u+v) - v = 2u$, qui est pair.

Morphisme. Pour tous $(u\,;v)$ et $(u'\,;v')$:

$$f\big((u\,;v)+(u'\,;v')\big)=\big(2(u+u')+(v+v')\,;\,v+v'\big)=(2u+v\,;\,v)+(2u'+v'\,;\,v')$$

Injectivité. Soit $(u\,;v)\in\operatorname{Ker} f$, c'est-à-dire $2u+v=0$ et $v=0$. La seconde équation donne $v=0$, puis la première $u=0$. Donc $\operatorname{Ker} f=\{(0\,;0)\}$.

Surjectivité. Soit $(a\,;b)\in H$. Comme $a-b$ est pair, l'entier $u=\dfrac{a-b}{2}$ est bien dans $\mathbb{Z}$. En posant $v=b$:

$$f(u\,;v)=(2u+v\,;\,v)=\big((a-b)+b\,;\,b\big)=(a\,;b)$$

$$\boxed{f \text{ est un isomorphisme de } (\mathbb{Z}^2\,;+) \text{ sur } (H\,;+).}$$

3. L'isomorphisme construit à la question précédente donne :

$$\boxed{H \text{ et } \mathbb{Z}^2 \text{ sont isomorphes, bien que } H \text{ soit une partie } \textit{stricte} \text{ de } \mathbb{Z}^2.}$$

En effet $(1\,;0)\notin H$. On retrouve le phénomène signalé par le cours à propos de $\mathbb{Z}$ et $n\mathbb{Z}$, et repris à l'exercice 17.

Injectivité et surjectivité

EXERCICE 15 ⋆

1. Le neutre d'arrivée est 1, et $\mathrm{e}^x=1$ équivaut à $x=0$. Par ailleurs tout réel strictement positif y s'écrit $\mathrm{e}^{\ln(y)}$.

$$\boxed{\operatorname{Ker} f=\{0\} \text{ et } \operatorname{Im} f=\mathbb{R}_+^* : f \text{ est un isomorphisme.}}$$

2. Le neutre d'arrivée est 1, et $|z|=1$ définit $\mathbb{U}$. Tout réel $r>0$ est le module du complexe r.

$$\boxed{\operatorname{Ker} g=\mathbb{U} \text{ et } \operatorname{Im} g=\mathbb{R}_+^* : g \text{ est surjectif, non injectif.}}$$

3. Le neutre d'arrivée est 0, et $3k=0$ équivaut à $k=0$. L'image est l'ensemble des multiples de 3.

$$\boxed{\operatorname{Ker} h=\{0\} \text{ et } \operatorname{Im} h=3\mathbb{Z}\neq\mathbb{Z} : h \text{ est injectif, non surjectif.}}$$

4. On a $x+y=0$ si et seulement si $y=-x$. Et tout réel z s'écrit $z+0$.

$$\boxed{\operatorname{Ker} u=\{(x\,;-x)\mid x\in\mathbb{R}\} \text{ et } \operatorname{Im} u=\mathbb{R} : u \text{ est surjectif, non injectif.}}$$

5. On a $(x\,;2x)=(0\,;0)$ si et seulement si $x=0$. L'image est la droite d'équation $y=2x$.

$$\boxed{\operatorname{Ker} v=\{0\} \text{ et } \operatorname{Im} v=\{(x\,;2x)\mid x\in\mathbb{R}\}\neq\mathbb{R}^2 : v \text{ est injectif, non surjectif.}}$$

Le point $(1\,;0)$, par exemple, n'a pas d'antécédent.

EXERCICE 16 ⋆⋆

1. On a $f(G')\subset H$. De plus $e_G\in G'$ et $f(e_G)=e_H$, donc $e_H\in f(G')$, qui n'est pas vide.

Soient y et y' dans $f(G')$: il existe x et x' dans G' tels que $y=f(x)$ et $y'=f(x')$. Alors, en utilisant la propriété 1 puis la définition d'un morphisme :

$$y*y'^{-1}=f(x)*f(x')^{-1}=f(x)*f(x'^{-1})=f(x\cdot x'^{-1})$$

et $x\cdot x'^{-1}$ appartient à G', qui est un sous-groupe.

$$\boxed{f(G') \text{ est un sous-groupe de } H.}$$

2. On a $f^{-1}(H') \subset G$. De plus $f(e_G) = e_H \in H'$, donc $e_G \in f^{-1}(H')$.
Soient x et x' dans $f^{-1}(H')$, c'est-à-dire $f(x) \in H'$ et $f(x') \in H'$. Alors :

$$f(x \cdot x'^{-1}) = f(x) * f(x')^{-1} \in H'$$

puisque H' est un sous-groupe. Donc $x \cdot x'^{-1} \in f^{-1}(H')$.

$$\boxed{f^{-1}(H') \text{ est un sous-groupe de } G.}$$

3. Soit $x \in \operatorname{Ker} f$. Alors $f(x) = e_H$, et $e_H \in H'$ puisque H' est un sous-groupe de H. Donc $x \in f^{-1}(H')$.

$$\boxed{\operatorname{Ker} f \subset f^{-1}(H')}$$

4. Il suffit de particulariser :

$$\boxed{\operatorname{Im} f = f(G) \text{ (question 1 avec } G' = G) \qquad \operatorname{Ker} f = f^{-1}(\{e_H\}) \text{ (question 2 avec } H' = \{e_H\})}$$

L'ensemble $\{e_H\}$ est bien un sous-groupe de H, et G est un sous-groupe de lui-même : la proposition 3 est donc un cas particulier des deux premières questions.

EXERCICE 17 ⋆⋆

1. L'application $k \mapsto 2k$ vérifie $2(k+k') = 2k+2k'$: c'est un endomorphisme de $(\mathbb{Z}\,;+)$. Son noyau est $\{k \in \mathbb{Z} \mid 2k = 0\} = \{0\}$, donc elle est injective ; son image est $2\mathbb{Z}$, et l'entier 1 n'a pas d'antécédent.

$$\boxed{\text{C'est un endomorphisme injectif et non surjectif de } (\mathbb{Z}\,;+).}$$

2. En restreignant l'ensemble d'arrivée à $2\mathbb{Z}$, l'application devient surjective sans cesser d'être injective ni d'être un morphisme.

$$\boxed{(\mathbb{Z}\,;+) \text{ et } (2\mathbb{Z}\,;+) \text{ sont isomorphes.}}$$

Pourtant $2\mathbb{Z}$ est une partie stricte de $\mathbb{Z}$, puisque $1 \notin 2\mathbb{Z}$.

3. Au chapitre 2, on avait construit une *bijection* de $\mathbb{N}$ sur l'ensemble des entiers naturels pairs : les deux ensembles avaient donc « autant » d'éléments. Ici on obtient davantage : un *isomorphisme*, qui respecte en outre la loi de groupe.

$$\boxed{\begin{array}{l}\text{Un ensemble infini peut être en bijection avec une de ses parties strictes ;}\\ \text{un groupe infini peut être isomorphe à l'un de ses sous-groupes stricts.}\end{array}}$$

4. Si G est fini et f injectif, alors f réalise une bijection de G sur $\operatorname{Im} f$, qui possède donc autant d'éléments que G. Comme $\operatorname{Im} f \subset G$ et que G est fini, il vient $\operatorname{Im} f = G$.

$$\boxed{\text{Non : pour un groupe fini, tout endomorphisme injectif est surjectif.}}$$

C'est précisément la finitude qui interdit à un ensemble d'être en bijection avec une partie stricte.

Exercices de synthèse

EXERCICE 18 : VRAI OU FAUX

1. **Vraie** C'est la propriété 1 du cours, démontrée en appliquant f à l'égalité $e_G \cdot e_G = e_G$.

2. **Fausse** L'application $x \mapsto x^2$ de $(\mathbb{R}\,;+)$ dans $(\mathbb{R}\,;+)$ envoie 0 sur 0, sans être un morphisme (exercice 1). Le test du neutre élimine, il ne valide pas.

3. **Vraie** C'est la proposition 3.

4. **Fausse** L'image est un sous-groupe de H, l'ensemble d'*arrivée*. Elle n'est en général même pas incluse dans G.

5. **Vraie** C'est le théorème 1, et c'est lui que l'on utilise en pratique.

6. **Vraie** C'est le premier point de la propriété 2.

7. **Vraie** C'est le second point de la propriété 2.

8. **Vraie** L'exponentielle en est un, de réciproque le logarithme (exercice 7).

9. **Fausse** Ce n'est vrai que si G est abélien, comme l'établit l'exercice 3. Dans $\mathcal{S}(\{1\,;2\,;3\})$, c'est faux.

10. **Fausse** Les groupes $(\mathbb{Z}\,;+)$ et $(2\mathbb{Z}\,;+)$ sont isomorphes (exercice 17), et $2\mathbb{Z}$ est une partie stricte de $\mathbb{Z}$.

EXERCICE 19 ⋆⋆⋆

1. On développe les deux carrés :

$$\begin{aligned}(xx'-yy')^2+(xy'+x'y)^2 &= x^2x'^2-2xx'yy'+y^2y'^2+x^2y'^2+2xy'x'y+x'^2y^2\\ &= x^2x'^2+x^2y'^2+y^2x'^2+y^2y'^2\\ &= x^2(x'^2+y'^2)+y^2(x'^2+y'^2)=(x^2+y^2)(x'^2+y'^2)\end{aligned}$$

les deux doubles produits se compensant.

2. *Internité.* Si $(x\,;y)$ et $(x'\,;y')$ sont non nuls, alors $x^2+y^2>0$ et $x'^2+y'^2>0$, donc leur produit est strictement positif. D'après la question 1, il en va de même de la somme des carrés des deux coordonnées du résultat, qui n'est donc pas le couple nul.

Commutativité. Les deux expressions $xx'-yy'$ et $xy'+x'y$ sont inchangées lorsqu'on échange $(x\,;y)$ et $(x'\,;y')$.

Associativité. Un calcul direct montre que les deux parenthésages donnent tous deux :

$$(xx'x''-xy'y''-yx'y''-yy'x''\;;\;xx'y''+xy'x''+yx'x''-yy'y'')$$

Neutre. $(x\,;y)*(1\,;0)=(x\times1-y\times0\,;\,x\times0+1\times y)=(x\,;y)$, et de même à gauche.

Symétrique. En posant $N=x^2+y^2>0$, on vérifie que $\left(\dfrac{x}{N}\,;\,\dfrac{-y}{N}\right)$ convient :

$$(x\,;y)*\left(\frac{x}{N}\,;\,\frac{-y}{N}\right)=\left(\frac{x^2+y^2}{N}\,;\,\frac{-xy+xy}{N}\right)=(1\,;0)$$

$$\boxed{(\mathbb{R}^2\setminus\{(0\,;0)\}\,;*)\text{ est un groupe abélien.}}$$

3. On a $\mathcal{C}\subset\mathbb{R}^2\setminus\{(0\,;0)\}$, et $(1\,;0)\in\mathcal{C}$. Soient $(x\,;y)$ et $(x'\,;y')$ dans $\mathcal{C}$. Le symétrique de $(x'\,;y')$ est $(x'\,;-y')$, puisque $N=1$, et il appartient à $\mathcal{C}$. Enfin, d'après la question 1, la somme des carrés des coordonnées du produit vaut $1\times1=1$.

$$\boxed{\mathcal{C}\text{ est un sous-groupe de }(\mathbb{R}^2\setminus\{(0\,;0)\}\,;*).}$$

4. Pour tous $(x\,;y)$ et $(x'\,;y')$ non nuls :

$$f\big((x\,;y)*(x'\,;y')\big)=(xx'-yy')+\mathrm{i}(xy'+x'y)=(x+\mathrm{i}y)(x'+\mathrm{i}y')=f(x\,;y)\times f(x'\,;y')$$

De plus f est bijective, de réciproque $z\mapsto(\mathcal{R}e(z)\,;\,\mathcal{I}m(z))$.

$$\boxed{f\text{ est un isomorphisme de }(\mathbb{R}^2\setminus\{(0\,;0)\}\,;*)\text{ sur }(\mathbb{C}^*\,;\times).}$$

5. La restriction de f à $\mathcal{C}$ reste un morphisme et reste injective. Son image est :

$$f(\mathcal{C})=\{x+\mathrm{i}y\mid x^2+y^2=1\}=\{z\in\mathbb{C}\mid|z|=1\}=\mathbb{U}$$

$$\boxed{f \text{ induit un isomorphisme de } (\mathcal{C}\,;*) \text{ sur } (\mathbb{U}\,;\times).}$$

6. *Morphisme.* Pour tous réels a et b, les formules d'addition donnent :

$$\varphi(a+b) = \big(\cos(a+b)\,;\,\sin(a+b)\big) = \big(\cos a\cos b - \sin a\sin b\,;\,\cos a\sin b + \cos b\sin a\big)$$

ce qui est exactement $\big(\cos a\,;\,\sin a\big) * \big(\cos b\,;\,\sin b\big) = \varphi(a) * \varphi(b)$.

Surjectivité. Soit $(x\,;y) \in \mathcal{C}$, c'est-à-dire $x^2+y^2=1$. Il existe alors un réel θ tel que $x=\cos\theta$ et $y=\sin\theta$: le point appartient au cercle trigonométrique.

Noyau. Le neutre de $(\mathcal{C}\,;*)$ est $(1\,;0)$, et :

$$\begin{aligned}\varphi(\theta) = (1\,;0) &\iff \cos\theta = 1 \quad\text{et}\quad \sin\theta = 0\\ &\iff \theta \in 2\pi\mathbb{Z}\end{aligned}$$

$$\boxed{\varphi \text{ est un morphisme surjectif, de noyau } \operatorname{Ker}\varphi = 2\pi\mathbb{Z}.}$$

Le noyau n'est pas réduit au neutre : d'après le théorème 1, l'application φ n'est donc pas injective. On lit ainsi la périodicité du sinus et du cosinus.

EXERCICE 20 ⋆⋆⋆

1. Pour tous entiers relatifs m et n, la relation admise donne :

$$\varphi_a(m+n) = a^{m+n} = a^m \cdot a^n = \varphi_a(m)\cdot\varphi_a(n)$$

$$\boxed{\varphi_a \text{ est un morphisme de } (\mathbb{Z}\,;+) \text{ dans } (G\,;\cdot).}$$

2. L'ensemble $\{a^n \mid n\in\mathbb{Z}\}$ n'est autre que $\operatorname{Im}\varphi_a$, et la proposition 3 s'applique.

$$\boxed{\{a^n \mid n\in\mathbb{Z}\} \text{ est un sous-groupe de } G.}$$

3. D'après la proposition 3, $\operatorname{Ker}\varphi_a$ est un sous-groupe de $(\mathbb{Z}\,;+)$. Le résultat admis au chapitre 3 donne alors :

$$\boxed{\text{Il existe un unique } d\in\mathbb{N} \text{ tel que } \operatorname{Ker}\varphi_a = d\mathbb{Z}.}$$

4. On distingue les deux cas.

- Si $d=0$, alors $\operatorname{Ker}\varphi_a = \{0\}$: d'après le théorème 1, φ_a est injectif. Les puissances a^n sont donc deux à deux distinctes, et le sous-groupe engendré par a est infini.
- Si $d>0$, alors $a^d = e$, et les entiers n vérifiant $a^n = e$ sont exactement les multiples de d. En particulier d est le plus petit entier strictement positif tel que $a^d = e$.

$$\boxed{\text{Dans le second cas, } d \text{ est appelé l'}\textit{ordre}\text{ de } a.}$$

5. On a $\mathrm{i}^1 = \mathrm{i}$, $\mathrm{i}^2 = -1$, $\mathrm{i}^3 = -\mathrm{i}$ et $\mathrm{i}^4 = 1$. Ainsi $\mathrm{i}^n = 1$ si et seulement si n est un multiple de 4.

$$\boxed{\operatorname{Ker}\varphi_{\mathrm{i}} = 4\mathbb{Z} \quad ; \quad \operatorname{Im}\varphi_{\mathrm{i}} = \mathbb{U}_4 \quad ; \quad \mathrm{i} \text{ est d'ordre } 4.}$$

6. Dans $(\mathbb{R}^*\,;\times)$, le neutre est 1. On a $(-1)^n = 1$ si et seulement si n est pair, tandis que $2^n = 1$ si et seulement si $n=0$.

$$\boxed{\operatorname{Ker}\varphi_{-1} = 2\mathbb{Z} : \text{l'élément } -1 \text{ est d'ordre } 2.}$$

$$\boxed{\operatorname{Ker}\varphi_2 = \{0\} = 0\mathbb{Z} : \text{l'élément } 2 \text{ n'est pas d'ordre fini.}}$$

Ce dernier cas fournit d'ailleurs un isomorphisme de $(\mathbb{Z}\,;+)$ sur le sous-groupe $\{2^n \mid n\in\mathbb{Z}\}$ de $(\mathbb{R}^*\,;\times)$, et l'on retrouve une fois de plus qu'un groupe infini peut être isomorphe à un sous-groupe strict.