Groupes

TD

Proposition de correction

Exercice (*). Les propositions suivantes sont-elles vraies ou fausses ? Justifier votre réponse.

1. La soustraction est un LCI dans $\mathbb{Z}$.
2. 0 est l'élément neutre de la soustraction dans $\mathbb{Z}$.
3. La soustraction dans $\mathbb{Z}$ est associative.
4. 0 est l'élément neutre pour l'addition dans $\mathbb{N}$.
5. L'addition est associative dans $\mathbb{N}$.
6. L'addition est une LCI dans l'ensemble des nombres entiers pairs.
7. L'addition est une LCI dans l'ensemble des nombres entiers impairs.

1. Oui.
2. Non car pas neutre à gauche.
3. Non car $a-(b-c)=a-b+c=(a-b)-(-c)$.
4. Oui.
5. Oui.
6. Oui car la somme de deux entiers pairs est paire.
7. Non car la somme de deux entiers impairs est paire.

Exercice (*). Préciser pour chacune des LCI $\star$ définies ci-dessous si elle est associative, commutative, possède un élément neutre.

1. $\forall x,y\in\mathbb{R},\ x\star y=\sqrt{x^2+y^2}$
2. $\forall x,y\in\mathbb{R},\ x\star y=\sqrt[3]{x^3+y^3}$
3. $\forall x,y\in\mathbb{R},\ x\star y=\ln(\mathrm{e}^x+\mathrm{e}^y)$

1. Elle est clairement commutative. Elle est associative : $(x\star y)\star z=(\sqrt{x^2+y^2})\star z=\sqrt{(\sqrt{x^2+y^2})^2+z^2}=\sqrt{x^2+y^2+z^2}=\sqrt{x^2+(\sqrt{y^2+z^2})^2})=x\star(y\star z)$ (cela provient du fait que $x^2+y^2\geq 0$). Le seul élément neutre qui peut venir à l'esprit est 0, mais il n'est pas neutre pour les nombres négatifs : $x\star 0=\sqrt{x^2}=|x|\neq x$. Si on n'a pas l'intuition, on peut le chercher : soit e un éventuel élément neutre et $x\in\mathbb{R}$. Alors
$$x\star e=x\Leftrightarrow\sqrt{x^2+e^2}=x\Rightarrow x^2+e^2=x^2\Rightarrow e^2=0$$
Le seul élément neutre possible est donc 0, mais cela n'en est pas un.
2. Elle est clairement commutative. Elle est associative : $(x\star y)\star z=(\sqrt[3]{x^3+y^3})\star z=\sqrt[3]{(\sqrt[3]{x^3+y^3})^3+z^3}=\sqrt[3]{x^3+y^3+z^3}=\sqrt[3]{x^3+(\sqrt[3]{y^3+z^3})^3})=x\star(y\star z)$ (les fonctions cube et racine cubique sont bijections réciproques l'une de l'autre). Le seul élément neutre qui peut venir à l'esprit est 0 : $x\star 0=\sqrt[3]{x^3}=x$. Donc 0 est l'élément neutre.
3. Elle est clairement commutative. Elle est associative : $(x\star y)\star z=(\ln(\mathrm{e}^x+\mathrm{e}^y))\star z=\ln\left(\mathrm{e}^{\ln(\mathrm{e}^x+\mathrm{e}^y)}+\mathrm{e}^z\right)=\ln(\mathrm{e}^x+\mathrm{e}^y+\mathrm{e}^z)=\ln\left(\mathrm{e}^x+\mathrm{e}^{\ln(\mathrm{e}^y+\mathrm{e}^z)}\right)=x\star(y\star z)$ (les fonctions exponentielle et logarithme népérien sont bijections réciproques l'une de l'autre). Si y est l'élément neutre alors $x\star y=x\Leftrightarrow\ln(\mathrm{e}^x+\mathrm{e}^y)=x=\ln(\mathrm{e}^x)\Leftrightarrow\mathrm{e}^x+\mathrm{e}^y=\mathrm{e}^x\Leftrightarrow\mathrm{e}^y=0$. Ceci est impossible, donc il n'y a pas d'élément neutre.

Exercice. Pour tout $(x;y)\in[0;1]^2$, on pose :
$$x\star y=x+y-xy$$

1. Montrer que $([0;1];\star)$ est un magma commutatif et associatif.
2. Montrer que $([0;1];\star)$ possède un élément neutre.
3. Quels sont les éléments inversibles de $([0;1];\star)$?

1. **Magma :** Si $0\leq x\leq 1$ et $0\leq y\leq 1$, alors $0\leq 1-x\leq 1$ et $0\leq 1-y\leq 1$. D'où $0\leq(1-x)(1-y)=1-(x+y-x)\leq 1$. Ainsi $-1\leq(-(x+y-xy)\leq 0$ et $0\leq x+y-xy\leq 1$.

   Commutatif : Évident.

   Associatif : $x\star(y\star z)=x+(y\star z)-x(y\star z)=x+(y+z-yz)-x(y+z-yz)=x+y+z-xy-xz-yz+xyz$, et $(x\star y)\star z=(x\star y)+z-(x\star y)z=(x+y-xy)+z-(x+y-xy)z=x+y+z-xy-xz-yz+xyz$.

2. Pour qu'un élément neutre e existe, il doit vérifier que pour tout $x \in [0;1]$, $x \star e = x = x + e - xe$. D'où nécessairement, pour tout x, $e(x-1) = 0$. Donc $e = 0$. On vérifie aisément que 0 est bien un élément neutre.
3. Deux éléments x, y sont inverses l'un de l'autre si et seulement si $x \star y = 0 = x + y - xy$, c'est-à-dire $y(x-1) = x$. Si $x = 1$, ceci est impossible. Si $x \neq 1$, nous avons $y = \frac{x}{x-1} \leq 0$. Le seul élément inversible de $[0;1]$ est donc 0.

Exercice. Soit $\star$ une opération associative sur un ensemble E. Montrer que l'ensemble des éléments réguliers à gauche est stable pour $\star$.

Soit RG l'ensemble des éléments régulier à gauche. C'est-à-dire que pour tout $x \in RG$, pour tout $(y;z) \in E^2$, $x \star y = x \star z \Rightarrow y = z$. Soit x et y deux éléments de RG. Nous avons alors, pour tout $(z;t) \in E^2$,

$$\begin{aligned}(x \star y) \star z = (x \star y) \star t &\Rightarrow x \star (y \star z) = x \star (y \star t) \\ &\Rightarrow y \star z = y \star t \\ &\Rightarrow z = t\end{aligned}$$

Ainsi $x \star y \in RG$.

Exercice (*). Soit E un ensemble muni d'une loi de composition interne associative $\star$ et d'un élément neutre. Un élément de E est dit idempotent si $x \star x = x$.

1. Montrer que si x et y sont idempotents et commutent, alors $x \star y$ est idempotent.
2. Montrer que si x est idempotent et inversible alors x^{-1} est idempotent.

1. $(x \star y) \star (x \star y) = (x \star x) \star (y \star y)$ (associative et commute). C'est égal à $x \star y$. Donc $(x \star y)$ est idempotent.
2. Nous savons que si x et y sont inversibles alors $x \star y$ aussi et l'inverse est $y^{-1} \star x^{-1}$, en prenant $y = x$ et en utilisant le fait que $x \star x = x$, nous avons $x^{-1} = (x \star x)^{-1} = x^{-1} \star x^{-1}$ et l'inverse est bien idempotent.

Exercice (*). Soit E un ensemble muni d'une loi de composition interne $\star$ associative. Pour tout a de E, on définit les applications g_a et d_a de E dans E : $\forall x \in E,\ d_a(x) = x \star a$ et $g_a(x) = a \star x$.

1. Montrer que s'il existe a dans E tel que g_a et d_a soient surjectives, alors E possède un élément neutre pour la loi $\star$.
2. Montrer que si pour tout a de E, les applications g_a et d_a sont surjectives, alors tout élément de E possède un inverse pour la loi $\star$.

1. Puisque g_a et d_a sont surjective, il existe e et f tels que $e \star a = a = a \star f$.
   — Montrer que $e = f$. Toujours par surjectivité, il existe y et z tels que $y \star a = e$ et $a \star z = f$. Nous avons alors

$$\begin{aligned}e \star f &= (y \star a) \star f = y \star (a \star f) = y \star a \\ &= e \\ e \star f &= e \star (a \star z) = (e \star a) \star z = a \star z \\ &= f\end{aligned}$$

   D'où l'égalité.
   — Montrons maintenant que $\forall x \in E, x \star f = f \star x = x$.
   Encore par surjectivité des applications, il existe y et z tels que $y \star a = x = a \star z$. Nous avons alors

$$\begin{aligned}x \star f &= (y \star a) \star f = y \star (a \star f) = y \star a = x \\ f \star x &= f \star (a \star z) = (f \star a) \star z = a \star z = x\end{aligned}$$

   Donc f est bien un élément neutre pour la loi $\star$.
2. Si les applications sont surjectives, pour tout a, alors nous venons de voir qu'il existe un élément neutre f. Ainsi, pour tout a, par surjectivité, il existe a_d et a_g tels que $a_g \star a = f = a \star a_d$. Il ne reste donc plus qu'à montrer que $a_d = a_g$:

$$a_g = a_g \star f = a_g \star (a \star a_d) = (a_g \star a) \star a_d = f \star a_d = a_d$$

Exercice. Sur $G = \mathbb{R}_+^* \times \mathbb{R}$, on définit l'opération $\star$ par :

$$(x;y) \star (x';y') = (xx';xy'+y)$$

Montrer que $(G;\star)$ est un groupe.

— Si $(x;x') \in (\mathbb{R}_+^*)^2$, alors $xx' \in \mathbb{R}_+^*$. Il est évident que pour tout $(x;y)$ et $(x';y')$ de G, $xy'+y \in \mathbb{R}$ Donc la loi $\star$ est bien une loi de composition interne.
— Nous avons $(1;0) \in G$ et pour tout $(x;y) \in G$, $(x;y) \star (1;0) = (x \times 1; x \times 0 + y) = (x;y)$ et $(1;0) \star (x;y) = (1 \times x; 1 \times y + 0) = (x;y)$. Donc $(1;0)$ est un élément neutre pour $\star$.

— Soit $(x;y) \in G$, alors $(x';y') = \left(\frac{1}{x};-\frac{y}{x}\right) \in G$ ($x>0$). Et nous avons $(x;y)\star(x';y') = \left(\frac{x}{x};\frac{-xy+yx}{x}\right) = (1;0)$. De même $(x';y')\star(x;y) = (1;0)$. Donc tout élément de G est inversible.

— Enfin, pour tout $(x;y)$, $(x';y')$, $(x'';y'')$ de G nous avons

$$(x;y)\star\big((x';y')\star(x'';y'')\big) = (x;y)\star(x'y';x'y''+y') = (xx'x'';xx'y''+xy'+y)$$
$$\big((x;y)\star(x';y')\big)\star(x'';y'') = (xx';xy'+y)\star(x'';y'') = (xx'x'';xx'y''+xy'+y)$$

La loi est donc associative.

Exercice. Soit les quatre fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$:

$$f_1(x) = x \quad ; \quad f_2(x) = \frac{1}{x} \quad ; \quad f_3(x) = -x \quad ; \quad ; f_4(x) = -\frac{1}{x}$$

Montrer que $G = \{f_1;f_2;f_3;f_4\}$ muni de la loi $\circ$ est un groupe.

f_1 est l'identité, donc l'ensemble possède déjà un élément neutre. Ensuite, $f_2\circ f_3 = f_3\circ f_2 = f_4 \in G$, $f_2\circ f_4 = f_4\circ f_2 = f_3 \in G$, $f_3\circ f_4 = f_4\circ f_3 = f_4$, $f_2\circ f_2 = f_1 = f_3\circ f_3 = f_4\circ f_4 \in G$. Donc nous avons bien une lci et $(G;\circ)$ est bien un magma.
Nous venons de voir que tout élément était son propre inverse et nous savons déjà que la loi $\circ$ est associative. Donc $(G;\circ)$ est bien un groupe.

Exercice. Quel est le plus petit sous-groupe de $(\mathbb{R};+)$ (respectivement de $(\mathbb{R}^*;\times)$) contenant 1 ? Contenant 2 ?

Un sous-groupe de $(\mathbb{R};+)$ contenant 1 doit nécessairement contenir l'élément neutre 0, mais aussi $1+1=2$, puis 3, etc, donc $\mathbb{N}$, mais aussi tous les opposés, donc $\mathbb{Z}$. Or $\mathbb{Z}$ étant un sous-groupe, on a trouvé le plus petit.
Avec le même raisonnement, on montre que le plus petit sous-groupe contenant 2 est $2\mathbb{Z}$.

Pour les sous-groupes de $(\mathbb{R}^*;\times)$, on doit contenir 1 et son inverse : 1. Donc en fait le groupe réduit à l'élément neutre $\{1\}$ est le plus petit.
Si il contient 2, il contient aussi l'élément neutre $1 = 2^0$, mais aussi $2\times 2 = 4 = 2^2$, $4\times 2 = 2^3$, etc. C'est-à-dire $\{2^k \ / \ k\in\mathbb{N}\}$. Il doit aussi contenir les inverses de tous ces nombres. Finalement le plus petit sous-groupe de $(\mathbb{R}^*;\times)$ est $\{2^k \ / \ k\in\mathbb{Z}\}$ (à condition d'avoir vérifié, bien évidemment, que c'est un sous-groupe).

Exercice (*). Les ensembles suivants, munis de l'addition des réels sont-ils des groupes ? Justifier.

1. $\{a\sqrt{2} \ / \ a\in\mathbb{N}\}$
2. $\{a\sqrt{2}+b\sqrt{3} \ / \ a,b\in\mathbb{Z}\}$
3. $\{a\sqrt{2}+b\sqrt{3} \ / \ a\in\mathbb{Z},\ b\in\mathbb{N}\}$

1. L'élément neutre étant 0, les éléments ne sont pas inversibles (car si $a\in\mathbb{N}^*$, $-a\notin\mathbb{N}$).
2. Si $x = a\sqrt{2}+b\sqrt{3}$ et $y = a'\sqrt{2}+b'\sqrt{3}$, alors $x+y = (a+a')\sqrt{2}+(b+b')\sqrt{3}\in G$. Nous avons donc stabilité par addition qui conserve sa propriété d'associativité. L'élément neutre est $0 = 0\sqrt{2}+0\sqrt{3}$, l'inverse est $-a\sqrt{2}-b\sqrt{3}$. C'est donc bien un groupe.
3. Cette fois ce n'est pas un groupe puisque l'inverse n'est pas dans l'ensemble (si $b\in\mathbb{N}$, alors $-b\notin\mathbb{N}$).

Exercice (*). Les ensembles suivants, munis de la multiplication des réelles sont-ils des groupes ? Justifier.

1. $\{1,-1,\frac{1}{2},2\}$
2. $\{a2^n \ / \ a=\pm1,\ n\in\mathbb{Z}\}$
3. $\{a+b\sqrt{2} \ / \ a,b\in\mathbb{Q}^*\}$

1. La loi n'est pas interne : tout produit entre deux éléments distincts de l'ensemble est bien dans l'ensemble, mais $2\times 2 = 4$ n'est pas dans l'ensemble.
2. La loi est bien interne : $a_1 2^{n_1} a_2 2^{n_2} = (a_1a_2)2^{n_1+n_2}$ avec $a_1a_2 = \pm1$ et $n_1+n_2\in\mathbb{Z}$, elle est associative. L'élément neutre est $1 = 1\times 2^0$. L'inverse de $a2^n$ est $a2^{-n}$ avec $-n\in\mathbb{Z}$. Donc c'est bien un groupe.
3. L'élément neutre n'est pas dans l'ensemble : $1 = 1+0\times\sqrt{2}$ or on doit avoir $b\in\mathbb{Q}^*$ et $1 = a+b\sqrt{2} \Leftrightarrow \sqrt{2} = \frac{1-a}{b}\in\mathbb{Q}$ (b est non nul), ce qui est absurde.

Exercice. Soit S un sous-groupe d'un groupe G et $a\in G$. Montrer que $a^{-1}Sa = \{c = a^{-1}ba \ / \ b\in S\}$ est un sous-groupe de G, dit conjugué de S.

— G étant un groupe, il est clair que $a^{-1}Sa\subset G$.

— Nous avons $1_G = a^{-1}1_G a\in a^{-1}Sa$.

— Si $d = a^{-1}ba$ et $e = a^{-1}ca$ sont deux éléments de $a^{-1}Sa$, alors

$$de^{-1} = a^{-1}ba\left(a^{-1}ca\right)^{-1} = a^{-1}ba\left(a^{-1}c^{-1}a\right) = a^{-1}\left(bc^{-1}\right)a \in a^{-1}Sa$$

Car S étant un sous-groupe, $bc^{-1} \in S$.

Exercice. Soit G un groupe et $A \subset G$, non vide. On pose :

$$N(A) = \left\{x \in G \ / \ x^{-1}Ax = A\right\}$$

Montrer que $N(A)$ est un sous-groupe de G.

Version sûr de ce que l'on fait

— $1^{-1}A1 = 1A1 = A$, donc $1 \in N(A)$.

— Soit x et y deux éléments de $N(A)$. Nous avons $(xy)^{-1} = y^{-1}x^{-1}$, d'où $(xy)^{-1}A(xy) = y^{-1}x^{-1}Axy = y^{-1}Ay = A$. Donc $xy \in N(A)$.

— Si $x \in N(A)$, alors $x^{-1}Ax = A$. En multipliant par x à gauche et x^{-1} à droite, nous avons $A = xAx^{-1} = (x^{-1})^{-1}Ax^{-1}$. Donc $x^{-1} \in N(A)$.

Version on détaille

— Soit $y \in A$, montrons que $y \in 1^{-1}A1$. $y = 1^{-1}y1 \in 1^{-1}A1$.
Soit $y \in 1^{1-}A1$, montrons que $y \in A$. Il existe $x \in A$ tel que $y = 1^{-1}x1 = x \in A$.
Donc $A = 1^{-1}A1$ et $1 \in N(A)$.

— Soit $x \in N(A)$. Montrons que $xAx^{-1} = A$.
Soit $z \in A$. Puisque $A = x^{-1}Ax$, il existe $y \in A$ tel que $z = x^{-1}yx$. D'où $z = xyx^{-1} \in xAx^{-1}$.
Soit $z \in xAx^{-1}$. Il existe $y \in A$ tel que $z = xyx^{-1}$. Or $A = x^{-1}Ax$, donc il existe $t \in A$ tel que $y = x^{-1}tx$. Ainsi, $z = xx^{-1}txx^{-1} = t = \in A$.
Donc $A = xAx^{-1}$ et $x^{-1} \in N(A)$.

— Soit x et y deux éléments de $N(A)$. Nous avons $x^{-1}Ax = a = y^{-1}Ay$. Montrons que $(xy)^{-1}A(xy) = A$.
Soit $z \in (xy)^{-1}Axy$. Il existe $t \in A$ tel que $z = (xy)^{-1}t(xy) = y^{-1}x^{-1}txy$. Or $A = x^{-1}Ax$, donc $x^{-1}tx \in x^{-1}Ax = A$. De même, un posant $u = x^{-1}tx \in A$, nous avons $y^{-1}uy \in y^{-1}Ay = A$. donc finalement $z \in A$.
Soit $z \in A$. Puisque $A = y^{-1}Ay$, il existe $t \in A$ tel que $z = y^{-1}ty$. Mais de même, il existe $u \in A$ tel que $t = x^{-1}ux$. D'où $z = y^{-1}x^{-1}uxy = (xy)^{-1}u(xy)$. Donc $z \in (xy)^{-1}A(xy)$.
Donc $A = (xy)^{-1}A(xy)$ et $xy \in N(A)$.

Donc $N(A)$ est bien un sous-groupe de G.

Exercice. Soit E un ensemble, $(G;\cdot)$ un groupe et f une bijection de E vers F.
Pour $(x;y) \in E^2$, on pose $xy = f^{-1}(f(x)f(y))$. Montrer que la loi de composition interne ainsi définie sur E munit E d'une structure de groupe.

— Soit x, y, z trois éléments de E. Alors $x(yz) = xf^{-1}(f(y)f(z)) = f^{-1}(f(x)f \circ f^{-1}(f(y)f(z))) = f^{-1}(f(x)f(y)f(z)) = f^{-1}(f \circ f^{-1}(f(x)f(y))f(z)) = f^{-1}(f(x)f(y))z = (xy)z$. La loi est associative.

— Si e est un élément neutre alors nécessairement, $x = xe = f-1(f(x)f(e))$. En composant par f, nous avons $f(x) = f(x)f(e)$. Or $f(x) \in G$, groupe, donc est inversible et $1_G = f(e)$. Par bijectivité de f, nous avons $e = f^{-1}(1_G)$. On vérifie alors aisément que $e = f^{-1}(1_G)$ est un élément neutre pour la loi (à droite ET à gauche).

— Soit $x \in E$. Posons alors $x^{-1} = f^{-1}(f(x)^{-}1)$. Ainsi $xx^{-1} = f^{-1}(f(x)f(x^{-1})) = f^{-1}(f(x)f(x)^{-1}) = f^{-1}(1_G) = e$. De même pour $x^{-1}x$. Ainsi tout élément de E est inversible.

Donc E est bien muni d'une structure de groupe.

Exercice (*). Soit $(E;\star)$ et $(F;\cdot)$ deux groupes. On munit l'ensemble produit $E \times F$ de la loi de composition $\otimes$ définie par :

$$\forall (x;y),\ \left(x';y'\right) \in E \times F,\ (x;y) \otimes \left(x';y'\right) = \left(x \star x';y \cdot y'\right)$$

1. Montrer que $(E \times F;\otimes)$ est un groupe.
2. Soit E' un sous-groupe de E et F' un sous-groupe de F. Montrer que $E' \times F'$ est un sous-groupe de $E \times F$, muni de la loi $\otimes$.

1. C'est la loi produit, donc la démonstration est faite dans le cours.
2. Nous avons bien $E' \times F' \subset E \times F$. Puisque E' et F' sont des sous-groupes, ils contiennent respectivement les neutres de E et F, donc $E' \times F'$ contient le neutre de $E \times F$. Enfin, par construction, si $(x;y) \in E' \times F'$ et $(x';y') \in E' \times F'$, alors $(x;y) \otimes \left(x'^{-1};y'^{-1}\right) = \left(x \star x'^{-1};y \cdot y'^{-1}\right) \in E' \times F'$ car E' et F' sont des sous-groupes.
Plus simplement, d'après la question précédente, $E' \times F'$ est un groupe inclu dans $E \times F$, donc c'est un sous-groupe.

Exercice (*). Soit $G =]-1;1[$ muni de la loi $\star$ définie par : $x \star y = \frac{x+y}{1+xy}$. Montrer que $(G;\star)$ est un groupe abélien.

La loi $\star$ est clairement commutative.

LCI Pour tout $y \in G$, la fonction $f : x \mapsto x \star y$ est strictement croissante ($f'(x) = \frac{1-y^2}{(1+xy)^2} > 0$) et $f(-1) = -1$ et $f(1) = 1$, donc pour tout $x \in G$, $f(x) \in G$. La loi est donc bien une lci.
Autre méthode : nous avons $1+xy > 0$, donc $x \star y \in]-1;1[\Leftrightarrow -1-xy < x+y < 1+xy \Leftrightarrow 0 < 1+x+y+xy$ et $1+xy-x-y > 0$. Or $(1+x) > 0$ et $(1+y) > 0$, donc $(1+x)(1+y) > 0$, d'où $1+x+y+xy > 0$. De même avec $(1-x) > 0$ et $1-y > 0$.

Associative Soit $x, y, z \in G$,

$$x \star (y \star z) = x \star \left(\frac{y+z}{1+yz}\right) = \frac{x + \frac{y+z}{1+yz}}{1 + x\left(\frac{y+z}{1+yz}\right)}$$
$$= \frac{x+y+z+xyz}{1+yz+xy+xz}$$

Cette dernière expression est invariante par permutation sur x, y et z, donc $x \star (y \star z) = z \star (y \star x)$. Et par commutativité, cette dernière expression est égale à $(x \star y) \star z$

Élément neutre 0 est clairement l'élément neutre : $x \star 0 = 0 \star x = \frac{x}{1} = x$.

Inversible L'inverse de x est alors tout simplement $-x \in G : x \star (-x) = \frac{x-x}{1-x^2} = 0$.

Exercice (*). Soit G un groupe et H et K deux sous-groupes de G.

1. Montrer que $H \cap K$ est un sous-groupe de G.
2. Montrer que ($H \cup K$ est un sous-groupe de G) $\Leftrightarrow$ ($H \subset K$ ou $K \subset H$).

1. Si H et K sont des sous-groupes, ils contiennent l'élément neutre, donc $H \cap K$ aussi. Si x et y sont dans l'intersection, alors x et y sont dans K, donc $xy^{-1} \in K$; de même $xy^{-1} \in H$. Donc $xy^{-1} \in H \cap K$ et nous avons bien la stabilité par produit et passage à l'inverse.
2. La réciproque est claire : si l'un des deux contient l'autre, l'union est égale à l'autre, donc est un sous-groupe. Démontrons le sens direct par contraposée. Si H n'est pas inclus dans K et K pas inclus dans H, alors $H \cap \overline{K} \neq \emptyset$ et $\overline{H} \cap K \neq \emptyset$. Prenons $x \in H \cap \overline{K}$ et $y \in \overline{H} \cap K$. Ces deux éléments sont dans $H \cup K$. Puisque $x \in H$ et que H est un sous-groupe, alors x^{-1} est aussi dans H. Supposons que $xy \in H$, alors $y = x^{-1}xy \in H$, ce qui est impossible, donc $xy \notin H$. De même $xy \notin K$. Finalement $xy \notin H \cup K$ et $H \cup K$ n'est pas stable pour la loi du groupe, donc n'est pas un sous-groupe de G.

Exercice.

1. Soit $n \in \mathbb{N}$. Montrer que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
2. Montrer que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$.
3. Soit $a, b \in \mathbb{Z}$. On note $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \ / \ u, v \in \mathbb{Z}\}$. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
   En particulier, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ pour un certain $d \in \mathbb{Z}$. Montrer alors que $d = a \wedge b$.

L'ensemble $\mathbb{Z}$ est bien évidemment muni de sa loi $+$ pour devenir un groupe. On rappelle que $n\mathbb{Z} = \{kn \ / \ k \in \mathbb{Z}\}$.

1. L'élément neutre $0 = 0 \times n$ est dans $n\mathbb{Z}$. Si $x = kn$ et $y = k'n$ sont dans $n\mathbb{Z}$, alors $x - y = (k - k')n$ est aussi dans $n\mathbb{Z}$.
2. Soit G un sous groupe de $\mathbb{Z}$. Il contient donc 0. Si $G = \{0\}$, alors $G = 0\mathbb{Z}$. Sinon, il contient un élément $x \neq 0$. Mais puisque c'est un groupe, il contient aussi $-x$. Ainsi $G \cap \mathbb{N}^*$ est une partie de $\mathbb{N}$ non vide et contient donc un plus petit élément que l'on note n. Montrons alors que $G = n\mathbb{Z}$ par double inclusion :
   — Soit $x \in G$. Si $x = 0$, alors $x \in n\mathbb{Z}$. Sinon, comme précédemment, $|x| \in G$. De plus, en effectuant la division euclidienne de $|x|$ par n, nous avons $|x| = nq + r$ avec $0 \leq r < n$. Or $|x| \in G$ et $n \in G$, d'où par stabilité, $nq \in G$ et $r = x - nq \in G$. Or n était le plus petit élément strictement positif de G. Ainsi $r = 0$ et $x = nq \in n\mathbb{Z}$.
   — Soit $x = nk \in n\mathbb{Z}$. Alors par stabilité, puisque $n \in G$, nk et donc x est dans G.

   Nous avons donc montré que tout sous groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$. Or nous avons montré à la question précédente que tous les ensembles $n\mathbb{Z}$ étaient des sous-groupes de $\mathbb{Z}$. Finalement, les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$.
3. Nous avons $0 = a \times 0 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$. Soit $x = ak_1 + bk_2 \in a\mathbb{Z} + b\mathbb{Z}$ et $y = ak'_1 + bk'_2 \in a\mathbb{Z} + b\mathbb{Z}$. Alors $x - y = a(k_1 - k'_1) + b(k_2 - k'_2) \in a\mathbb{Z} + b\mathbb{Z}$.
   Donc $a\mathbb{Z} + b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$, donc s'écrit $d\mathbb{Z}$. On en déduit qu'il existe k et k' tels que $ak + bk' = d$ (car $d \in d\mathbb{Z}$). Donc $a \wedge b | d$.
   De plus, d'après la relation de Bézout, il existe u et v tels que $au + bv = a \wedge b$, donc $a \wedge b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Donc il existe $k \in \mathbb{Z}$ tel que $dk = a \wedge b$. Donc $d | a \wedge b$. Finalement $d = a \wedge b$.

Exercice. Soit H un groupe abélien. Un élément $x \in H$ est dit d'ordre fini lorsqu'il existe $n \in \mathbb{N}$ tel que la somme $x + \cdots + x$ (n fois) soit égale à 0. Montrer que l'ensemble des éléments d'ordre fini est un sous-groupe abélien de H.

Notons G l'ensemble des éléments d'ordre fini de H.

Inclusion : Nous avons clairement $G \subset H$.

Élément neutre : Nous avons 0=0, donc $0 \in G$.

Stabilité par passage à l'inverse : Soit $x \in G$. Il existe n tel que $x+\cdots+x=0$ (n fois). D'où $(-x)+\cdots+(-x)=-(x+\cdots+x)=-0=0$.

Stabilité par somme : Soit x et y dans G. Il existe n_x et n_y tels que $x+\cdots+x=0$ (n_x fois) et $y+\cdots+y=0$ (n_y fois). Alors, par commutativité de $+$ (H est un groupe abélien), nous avons

$$\underbrace{(x+y)+\cdots+(x+y)}_{n_xn_y \text{ fois}}=\underbrace{(x+\cdots+x)}_{n_xn_y \text{ fois}}+\underbrace{(y+\cdots+y)}_{n_xn_y \text{ fois}}=\underbrace{(0+\cdots+0)}_{n_y \text{ fois}}+\underbrace{(0+\cdots+0)}_{n_x \text{ fois}}=0$$

Donc $x+y \in G$.

Donc G est un sous-groupe de H et comme H est commutatif, G aussi.

Exercice. Décrire tous les homomorphismes de groupes de $\mathbb{Z}$ dans $\mathbb{Z}$. Déterminer ceux qui sont injectifs et ceux qui sont surjectifs.

Soit $f:(\mathbb{Z},+)\longrightarrow(\mathbb{Z},+)$ un morphisme de groupe. Comme tout morphisme f vérifie $f(0)=0$. Notons $a=f(1)$. Alors

$$f(2)=f(1+1)=f(1)+f(1)=a+a=2.a.$$

De même, pour $n \geq 0$:

$$f(n)=f(1+\cdots+1)=f(1)+\cdots+f(1)=n.f(1)=n.a.$$

Enfin comme

$$0=f(0)=f(1+(-1))=f(1)+f(-1)=a+f(-1),$$

alors $f(-1)=-a$ et pour tout $n \in \mathbb{Z}$:

$$f(n)=n.a.$$

Donc tous les morphisme sont de la forme $n \mapsto n.a$, avec $a \in \mathbb{Z}$.

Réciproquement, un morphisme $n \mapsto n.a$ est injectif si et seulement si $a \neq 0$, et surjectif si et seulement si $a=\pm 1$.

Exercice. Soit $f:\mathbb{R}\to\mathbb{C}^*$ l'application qui à tout $x \in \mathbb{R}$ associe $e^{ix} \in \mathbb{C}^*$. Montrer que f est un homomorphisme de groupes. Calculer son noyau et son image. f est-elle injective ?

$$\begin{aligned} f:(\mathbb{R},+) &\longrightarrow (\mathbb{C}^*,\times) \\ x &\mapsto e^{ix} \end{aligned}$$

Vérifions que f est un morphisme de groupe. Soit $x,y \in \mathbb{R}$, alors

$$f(x+y)=e^{i(x+y)}=e^{ix}e^{iy}=f(x)\times f(y),$$

et

$$f(x^{-1})=e^{i(-x)}=\frac{1}{e^{ix}}=f(x)^{-1}.$$

Donc f est un morphisme de groupe.

Montrons que f n'est pas injective en prouvant que le noyau n'est pas réduit à 0 :

$$\operatorname{Ker} f=\{x\in\mathbb{R} \text{ tels que } f(x)=1\}=\left\{x\in\mathbb{R} \text{ tels que } e^{ix}=1\right\}=\{x=0+2k\pi,\ \ k\in\mathbb{Z}\}.$$

Enfin

$$\operatorname{Im} f=\left\{y\in\mathbb{C}^*, y=e^{ix}\right\}$$

est l'ensemble des complexes de module 1, c'est-à-dire le cercle de centre 0 et de rayon 1.

Exercice. Traduire en termes d'homomorphisme de groupes les propriétés traditionnelles suivantes :

1. $\ln(xy)=\ln(x)+\ln(y)$
2. $|zz'|=|z||z'|$
3. $(xy)^{\frac{1}{2}}=x^{\frac{1}{2}}y^{\frac{1}{2}}$
4. $e^{z+z'}=e^ze^{z'}$
5. $\overline{z+z'}=\overline{z}+\overline{z'}$

1. La fonction ln réalise un morphisme de groupes entre $\left(\mathbb{R}_+^*,\times\right)$ et $(\mathbb{R},+)$.
2. Morphisme entre $(\mathbb{C}^*,\times)$ et $\left(\mathbb{R}_+^*,\times\right)$
3. Morphisme entre $\left(\mathbb{R}_+^*,\times\right)$ et $\left(\mathbb{R}_+^*,\times\right)$
4. Morphisme entre $(\mathbb{C},+)$ et $(\mathbb{C}^*,\times)$
5. Morphisme entre $(\mathbb{C},+)$ et $(\mathbb{C},+)$

Exercice. Soit G un groupe. Montrer que l'application $x \to x^{-1}$ est un morphisme si et seulement si G est commutatif.

Indication. $(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xy = yx$.

Soit f l'application de G dans G qui à x associe son inverse x^{-1}. Nous avons bien évidemment $f(e) = e^{-1} = e$. De plus pour tout a, b de G, nous avons d'une part $f(ab) = (ab)^{-1} = b^{-1}a^{-1}$, et d'autre part $f(a)f(b) = a^{-1}b^{-1} = (ba)^{-1}$. Donc f est un morphisme si et seulement si $(ab)^{-1} = (ba)^{-1}$, c'est-à-dire $ab = ba$, donc si et seulement si G est commutatif.

Exercice. Montrer que les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes.

Nous cherchons une application f de $\mathbb{R}$ dans $\mathbb{R}_+^*$ telle que $f(0) = 1$ et pour tout réels, $f(x+y) = f(x) \times f(y)$. Nous reconnaissons alors l'exponentielle, qui suffit à conclure (l'exponentielle est bijective).

Exercice (Groupe des automorphismes). Soit G un groupe multiplicatif (associatif). On note $\mathrm{Aut}(G)$ l'ensemble des isomorphismes $\phi : G \to G$.

1. Montrer que $\mathrm{Aut}(G)$ est un groupe pour la loi $\circ$.
2. Déterminer $\mathrm{Aut}(\mathbb{Z})$.
3. Pour $a \in G$ on note $\phi_a : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & axa^{-1} \end{array} \right.$

   Montrer que $\phi_a \in \mathrm{Aut}(G)$, et que l'application : $\left\{ \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ a & \longmapsto & \phi_a \end{array} \right.$ est un morphisme de groupes.

1. L'identité est bien un automorphisme de G. De plus, soit φ_1 et φ_2 deux automorphismes. Alors pour tout $a, b \in G$, $\varphi_1 \circ \varphi_2(ab) = \varphi_1(\varphi_2(a)\varphi_2(b)) = \varphi_1(\varphi_2(a))\varphi_1(\varphi_2(b)) = \varphi_1 \circ \varphi_2(a)\varphi_1 \circ \varphi_2(b)$. Donc stable par $\circ$. Si x_1 et x_2 sont deux éléments de G, en notant $y_1 = \varphi_1^{-1}(x_1)$ et $y = 2\varphi_1^{-1}(x_2)$, alors $\varphi_1(y_1y_2) = \varphi_1(y_1)\varphi_1(y_2) = x_1x_2$. Ainsi $\varphi_1^{-1}(x_1)\varphi_1^{-1}(x_2) = y_1y_2 = \varphi_1^{-1}(x_1x_2)$. Donc φ_1^{-1} est bien un (auto-)morphisme, d'où stabilité par passage à l'inverse.
2. Soit $f \in \mathrm{Aut}(\mathbb{Z})$. Alors nous devons avoir $f(0)$. Posons $f(1) = a \in \mathbb{Z}$. Par morphisme, nous avons nécessairement que pour tout $n \in \mathbb{Z}$, $f(n) = na$. Soit alors $a = pq$ une décomposition de a. Alors, soit $b \in \mathbb{Z}$ tel que $f(b) = p$ et c tel que $f(x) = q$. Nous avons alors $f(bc) = f(b)f(c) = pa = a = f(1)$. L'application f étant une bijection, nous avons $bc = 1$. Or b et c sont des entiers, donc $b = c = 1$ ou $b = c = -1$. Dans les deux cas, nous avons $p = q = f(\pm 1) = \pm f(1) = \pm a$, donc $a = pq = (\pm a)^2 = a^2$. Ainsi $a = 0$ ou 1. Dans le premier cas, f est l'application nulle qui n'est pas bijective. Dans le second cas, f est l'identité. En conclusion, $\mathrm{Aut}(\mathbb{Z}) = \{Id_{\mathbb{Z}}\}$.
3. Nous avons $\phi_a(e) = e$, $\phi_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = \phi_a(x)\phi_a(y)$. C'est donc bien un morphisme. Il est bien bijectif car $axa^{-1} = aya^{-1} \iff x = y$.
   Notons f cette application. Alors pour tout $a, b \in G$ et pour tout $x \in G$, $f(ab)(x) = \phi_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = \phi_a(\phi_b(x)i) = \phi_a \circ \phi_b(x) = f(a) \circ f(b)(x)$. Donc $f(ab) = f(a) \circ f(b)$. De plus $f(e)(x) = \phi_e(x) = exe^{-1} = x$, donc $f(e) = Id_G$. Donc f est bien un morphisme de groupes.

Exercice (Images directes et réciproques). Soit G un groupe additif et $f : G \to G'$ un morphisme de groupes.

1. Montrer que pour tout sous-groupe H de G on a : $f^{-1}(f(H)) = H + \mathrm{Ker}(f)$.
2. Montrer que pour tout sous-groupe H' de G' on a : $f(f^{-1}(H')) = H' \cap \mathrm{Im}(f)$.

1.
$$\begin{aligned} x \in f^{-1}(f(H)) &\iff f(x) \in f(H) \iff \exists h \in H,\ f(x) = f(h) \\ &\iff \exists h \in H,\ f(x-h) = 0 \iff \exists h \in H,\ y = x - h \in \mathrm{Ker}(f) \\ &\iff \exists h \in H, \exists y \in \mathrm{Ker}(f),\ x = h + y \iff x \in H + \mathrm{Ker}\, f \end{aligned}$$

2.
$$y \in f(f^{-1}(H')) \iff \exists x \in f^{-1}(H'), f(x) = y$$

Ainsi, $y \in \mathrm{Im}(f)$. De plus $x \in f^{-1}(H') \iff \exists z \in H',\ f(x) = z$. Donc $y = z \in f(H')$.
Réciproquement, si $y \in H' \cap \mathrm{Im}(f)$, alors il existe $x \in G$ tel que $y = f(x)$. D'où $f(x) \in H'$ et donc $x \in f^{-1}(H')$. Finalement, $y \in f(f^{-1}(H'))$.
Remarque : Ce résultat a déjà été montré dans le cadre général des applications.

Exercice (Morphismes de $\mathbb{Q}$ additif). Déterminer tous les morphismes de

1. $(\mathbb{Q}, +)$ dans $(\mathbb{Q}, +)$.
2. $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
3. $(\mathbb{Q}, +)$ dans $(\mathbb{Q}^*, \times)$.

1. $x \mapsto ax, a \in \mathbb{Q}$.
2. $x \mapsto 0$.
3. $x \mapsto 1$.

Exercice (Loi sur $\mathbb{Z}^2$). On définit l'opération dans $\mathbb{Z}^2$: $(a,b) * (a',b') = (aa', ab'+b)$.

1. Étudier les propriétés de cette opération.
2. Pour $z \in \mathbb{Z}$, on pose $f_{a,b}(z) = az+b$.
   Montrer que $\phi : \left\{ \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^{\mathbb{Z}} \\ (a,b) & \longmapsto & f_{a,b} \end{array} \right.$ est un morphisme pour $*$ et $\circ$.
3. Est-ce un isomorphisme ?

1. Non commutative, associative, $(1,0)$ = élt neutre,
   (a,b) est régulier $\iff a \neq 0$.
   (a,b) est inversible $\iff a = \pm 1$.
2. Soit $a,a',b,b',z \in \mathbb{Z}$. Alors

$$\begin{aligned} \phi((a,b)*(a',b'))(z) = \phi(aa', ab'+b)(z) = f_{aa',ab'+b}(z) = aa'z+ab'+b = a(a'z+b')+b = f_{a,b}(a'z+b') = f_{a,b}(f_{a',b'}(z)) \\ = \phi(a,b) \circ \phi(a',b')(z) \end{aligned}$$

   $\phi(1,0)(z) = z =)Id(z)$.
3.

Exercice ($(\mathbb{Q},+)$ et $(\mathbb{Q}^{+*},\times)$ ne sont pas isomorphes). Montrer que les groupes $(\mathbb{Q},+)$ et $(\mathbb{Q}_+^*,\times)$ ne sont pas isomorphes (penser à $\sqrt{2}$).

Supposons qu'il existe un isomorphisme φ de $(\mathbb{Q},+)$ vers $\left(\mathbb{Q}_+^*,\times\right)$. Alors il existe donc un unique rationnel a tel que $\varphi(a) = 2$. Posons $b = \frac{a}{2}$, alors $2 = \varphi(a) = \varphi(2b) = \varphi(b)^2$. D'où $\varphi(b) = \sqrt{2} \in \mathbb{Q}$, ce qui est absurde.
Deuxième méthode : D'après l'exercice **??**, le seul morphisme possible est $x \mapsto 1$ qui est non injectif.