CORRIGÉ – CHAPITRE 3

GROUPES

Lois de composition interne

EXERCICE 1 ⋆

Le mot *interne* porte toute la définition : il faut que le résultat reste dans l'ensemble de départ, et que l'opération y soit définie pour *tout* couple.

1. La différence de deux entiers naturels peut être négative :

$$\boxed{\text{Non : } 3-5=-2\notin\mathbb{N}.}$$

2. La différence de deux entiers relatifs est un entier relatif : $\boxed{\text{Oui.}}$

3. La loi n'est pas définie partout :

$$\boxed{\text{Non : le quotient } \frac{x}{0} \text{ n'est pas défini.}}$$

4. Si x et y sont des réels non nuls, $\dfrac{x}{y}$ est un réel non nul : $\boxed{\text{Oui.}}$

5. La demi-somme de deux entiers n'est pas toujours entière :

$$\boxed{\text{Non : } 1*2=\frac{3}{2}\notin\mathbb{Z}.}$$

6. La demi-somme de deux rationnels est un rationnel : $\boxed{\text{Oui.}}$

7. Si $x\geqslant 1$ et $y\geqslant 1$, alors $x^y\geqslant 1$ est un entier : $\boxed{\text{Oui.}}$

8. Si $x\geqslant 0$ et $y\geqslant 0$, alors $x+y\geqslant 0$ et $\sqrt{x+y}$ existe et est positif : $\boxed{\text{Oui.}}$

9. La réunion de deux parties de E est une partie de E : $\boxed{\text{Oui.}}$

10. L'ensemble $A\setminus B$ est inclus dans A, donc dans E : $\boxed{\text{Oui.}}$

Piège de la question 3 : l'obstacle n'est pas que le résultat sorte de $\mathbb{R}$, mais que la loi ne soit pas *définie* pour tout couple. Une L.C.I. est une application de $E\times E$ dans E : elle doit exister partout.

EXERCICE 2 ⋆

1. L'expression $x+y+xy$ est inchangée quand on échange x et y : la loi est **commutative**. Pour l'associativité :

$$(x*y)*z=(x+y+xy)+z+(x+y+xy)z=x+y+z+xy+xz+yz+xyz$$

$$x*(y*z)=x+(y+z+yz)+x(y+z+yz)=x+y+z+yz+xy+xz+xyz$$

Ces deux expressions coïncident :

$$\boxed{\text{Commutative et associative.}}$$

2. L'expression $\dfrac{x+y}{2}$ est symétrique : la loi est commutative. En revanche, avec $x=0$, $y=0$ et $z=2$:

$$(0*0)*2=0*2=1 \qquad \text{tandis que} \qquad 0*(0*2)=0*1=\frac{1}{2}$$

$$\boxed{\text{Commutative, non associative.}}$$

3. On a $1 * 2 = 1$ et $2 * 1 = 2$: la loi n'est pas commutative. En revanche :

$$(x * y) * z = x * z = x \qquad \text{et} \qquad x * (y * z) = x$$

Non commutative, associative.

4. On a $1 * 2 = 2$ et $2 * 1 = 4$: la loi n'est pas commutative. De plus :

$$(x * y) * z = (x^2 y)^2 z = x^4 y^2 z \qquad \text{et} \qquad x * (y * z) = x^2 (y^2 z) = x^2 y^2 z$$

qui diffèrent pour $x = 2$, $y = z = 1$: on obtient 16 d'un côté et 4 de l'autre.

Ni commutative, ni associative.

Les questions 3 et 4 montrent que les deux propriétés sont indépendantes : aucune n'entraîne l'autre.

EXERCICE 3 ⋆⋆

1. La loi $x * y = x + y - xy$ sur $\mathbb{R}$.

Internité et commutativité. Le résultat est un réel, et l'expression est symétrique en x et y.

Associativité. On remarque que $1 - x * y = 1 - x - y + xy = (1 - x)(1 - y)$, d'où :

$$1 - (x * y) * z = (1 - x * y)(1 - z) = (1 - x)(1 - y)(1 - z)$$

Cette expression étant symétrique en x, y et z, la loi est associative.

Neutre. On cherche e tel que $x * e = x$ pour tout x, soit $x + e - xe = x$, c'est-à-dire $e(1 - x) = 0$ pour tout x : nécessairement $e = 0$. On vérifie que $x * 0 = 0 * x = x$.

Éléments symétrisables. On résout $x * y = 0$, soit $x + y - xy = 0$, c'est-à-dire $y(1 - x) = -x$. Si $x \neq 1$, on obtient $y = \dfrac{x}{x - 1}$; si $x = 1$, alors $1 * y = 1 + y - y = 1 \neq 0$.

Loi interne, commutative, associative, de neutre 0.
Les éléments symétrisables sont ceux de $\mathbb{R} \setminus \{1\}$, le symétrique de x étant $\dfrac{x}{x - 1}$.

2. La loi $x * y = \sqrt{x^2 + y^2}$ sur $\mathbb{R}_+$.

Le résultat est un réel positif, et l'expression est symétrique. Pour l'associativité :

$$(x * y) * z = \sqrt{\left(\sqrt{x^2 + y^2}\right)^2 + z^2} = \sqrt{x^2 + y^2 + z^2} = x * (y * z)$$

Le neutre vérifie $\sqrt{x^2 + e^2} = x$ pour tout $x \geqslant 0$, donc $e = 0$. Enfin $x * y = 0$ impose $x^2 + y^2 = 0$, donc $x = y = 0$.

Loi interne, commutative, associative, de neutre 0.
Seul 0 est symétrisable.

3. La loi $x * y = x + y - 3$ sur $\mathbb{Z}$.

Le résultat est un entier relatif, et l'expression est symétrique. Pour l'associativité, les deux calculs donnent $x + y + z - 6$. Le neutre vérifie $x + e - 3 = x$, donc $e = 3$. Enfin $x * y = 3$ équivaut à $y = 6 - x$, qui est bien un entier.

Loi interne, commutative, associative, de neutre 3.
Tout élément x est symétrisable, de symétrique $6 - x$.

Remarque. Les quatre axiomes **IANS** sont donc satisfaits : $(\mathbb{Z}\,; *)$ est un groupe abélien, comme on le vérifiera à l'exercice 7. Ce n'est pas un hasard : l'application $\varphi : x \mapsto x - 3$ est une bijection de $\mathbb{Z}$

sur $\mathbb{Z}$ qui vérifie $\varphi(x * y) = \varphi(x) + \varphi(y)$. Cette loi n'est donc que l'addition habituelle, déguisée par un changement de nom des éléments — et le neutre 3 n'a rien de mystérieux : c'est l'ancien 0.

Neutre, symétrique et tables de Cayley

EXERCICE 4 ⋆

1. Le neutre de $(\mathbb{N}\,;\times)$ est 1. Si $xy = 1$ avec x et y entiers naturels, alors $x \geqslant 1$ et $y \geqslant 1$, donc $x = y = 1$.

Neutre 1 ; seul 1 est symétrisable.

2. Le neutre de $(\mathbb{R}\,;\times)$ est 1, et x est inversible si et seulement si $x \neq 0$.

Neutre 1 ; les éléments symétrisables sont ceux de $\mathbb{R}^*$.

3. On a $A \cap E = A$ pour toute partie A, et $A \cap B = E$ impose $A = B = E$.

Neutre E ; seul E est symétrisable.

4. On a $A \cup \varnothing = A$, et $A \cup B = \varnothing$ impose $A = B = \varnothing$.

Neutre $\varnothing$; seul $\varnothing$ est symétrisable.

5. Le neutre est Id_E, d'après la propriété 1 du chapitre 2. Une application f admet un symétrique pour $\circ$ lorsqu'il existe g telle que $f \circ g = g \circ f = \mathrm{Id}_E$, c'est-à-dire lorsque f est bijective.

Neutre Id_E ; les éléments symétrisables sont les bijections de E.

6. On a $A \,\Delta\, \varnothing = A$ et $A \,\Delta\, A = \varnothing$, résultats établis au chapitre 1.

Neutre $\varnothing$; toute partie est symétrisable, et est son propre symétrique.

Commentaire. La différence symétrique fait donc de $\mathcal{P}(E)$ un groupe abélien, alors que $\cap$ et $\cup$ n'en font pas un : sur les mêmes éléments, changer la loi change tout. Ce groupe a de plus une propriété remarquable — tout élément est son propre symétrique — que l'on exploitera à l'exercice 13.

EXERCICE 5 ⋆

1. Les deux tables sont symétriques par rapport à leur diagonale principale : on lit la même valeur en $(x\,;y)$ et en $(y\,;x)$.

Les deux lois sont commutatives.

2. Dans les deux tables, la ligne de e reproduit l'en-tête des colonnes, et la colonne de e reproduit l'en-tête des lignes.

Dans les deux cas, e est l'élément neutre.

3. On cherche le neutre e dans chaque ligne. Pour la loi $*$: $a * a = b * b = c * c = e$. Pour la loi $\perp$: $a \perp a = b \perp b = e$.

Dans les deux cas, tout élément est symétrisable et est son propre symétrique.

4. On calcule dans la seconde table :

$$(a \perp a) \perp b = e \perp b = b \qquad \text{tandis que} \qquad a \perp (a \perp b) = a \perp a = e$$

Comme $b \neq e$, la loi $\perp$ n'est pas associative : l'axiome **A** échoue.

$(F\,;\perp)$ n'est pas un groupe, alors que $(E\,;*)$ en est un.

5. La ligne de a dans la seconde table est $(a\,;e\,;a)$: l'élément a y figure deux fois, et b n'y figure pas. Rien de tel dans la première table, où chaque ligne contient chacun des quatre éléments exactement une fois.

La seconde table n'est pas un *carré latin*.

On démontrera à l'exercice 13 que la table de Cayley d'un groupe fini en est nécessairement un : c'est donc un second argument, plus rapide, pour écarter $(F\,;\perp)$.

Piège : les trois lectures immédiates données par le cours — symétrie, première ligne, présence du neutre dans chaque ligne — ne testent que la commutativité, le neutre et les symétriques. Elles ne disent *rien* de l'associativité, qui est pourtant l'un des quatre axiomes.

EXERCICE 6 ⋆⋆

1. L'ensemble $\mathcal{P}(E)$ compte quatre éléments : $\varnothing$, $\{a\}$, $\{b\}$ et $E=\{a\,;b\}$. On calcule chaque différence symétrique, par exemple $\{a\}\,\Delta\,\{b\}=\{a\,;b\}$ et $\{a\}\,\Delta\,E=\{b\}$.

Δ	$\varnothing$	$\{a\}$	$\{b\}$	E
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	E
$\{a\}$	$\{a\}$	$\varnothing$	E	$\{b\}$
$\{b\}$	$\{b\}$	E	$\varnothing$	$\{a\}$
E	E	$\{b\}$	$\{a\}$	$\varnothing$

2. La table est symétrique, la ligne de $\varnothing$ reproduit l'en-tête, et $\varnothing$ figure une fois dans chaque ligne : la loi est commutative, de neutre $\varnothing$, et tout élément est symétrisable. L'associativité étant admise :

$(\mathcal{P}(E)\,;\Delta)$ est un groupe abélien à quatre éléments.

3. Les deux groupes ont quatre éléments, mais ne se comportent pas de la même façon. Dans $(\mathcal{P}(E)\,;\Delta)$, *tout* élément est son propre symétrique ; dans $\{1\,;\mathrm{i}\,;-1\,;-\mathrm{i}\}$, seuls 1 et -1 le sont, puisque $\mathrm{i}\times\mathrm{i}=-1\neq 1$.

Non : ces deux groupes d'ordre 4 ne sont pas de même nature.

On retrouvera la première table à l'exercice 8, avec des fonctions à la place des parties.

EXERCICE 7 ⋆

On suit l'ordre **IANS** et l'on s'arrête au premier axiome qui échoue.

	Groupe ?	Justification
$(\mathbb{N}\,;+)$	non	**S** échoue : 3 n'a pas d'opposé dans $\mathbb{N}$.
$(\mathbb{N}\,;\times)$	non	**S** échoue : 2 n'a pas d'inverse dans $\mathbb{N}$.
$(\mathbb{Z}\,;+)$	**oui**	Groupe abélien de neutre 0, le symétrique de x étant $-x$.
$(\mathbb{Z}\,;\times)$	non	**S** échoue : 2 n'a pas d'inverse dans $\mathbb{Z}$.
$(n\mathbb{Z}\,;+)$	**oui**	Groupe abélien de neutre 0 ; $nk+nk'=n(k+k')$ et $-nk=n(-k)$.
$(\mathbb{R}\,;+)$	**oui**	Groupe abélien de neutre 0.
$(\mathbb{R}\,;\times)$	non	**S** échoue : 0 n'a pas d'inverse.
$(\mathbb{R}^*\,;\times)$	**oui**	Groupe abélien de neutre 1, le symétrique de x étant $\frac{1}{x}$.
$(\mathbb{R}^{\mathbb{R}}\,;\circ)$	non	**S** échoue : seules les bijections sont symétrisables (exercice 4).
$(\mathbb{R}^{\mathbb{R}}\,;+)$	**oui**	Groupe abélien de neutre la fonction nulle, le symétrique de f étant $-f$.

Les cinq groupes obtenus sont tous abéliens.

Piège : il ne faut pas confondre « $\mathbb{N}$ n'est pas un groupe pour $+$ » avec « l'addition n'est pas associative sur $\mathbb{N}$ ». Les trois premiers axiomes sont satisfaits ; c'est le quatrième, et lui seul, qui fait défaut. C'est précisément ce manque qui motive la construction de $\mathbb{Z}$.

EXERCICE 8 ⋆⋆

1. Notons $f_{a,b} : x \mapsto ax+b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$.

Internité. Pour tous $(a\,;b)$ et $(c\,;d)$ convenables :

$$(f_{a,b} \circ f_{c,d})(x) = a(cx+d)+b = (ac)x + (ad+b)$$

donc $f_{a,b} \circ f_{c,d} = f_{ac,\,ad+b}$, avec $ac \in \mathbb{R}^*$: la loi est interne.

Associativité. C'est celle de la composition des applications.

Neutre. $f_{1,0} = \mathrm{Id}_{\mathbb{R}}$ appartient à G.

Symétrique. On cherche $f_{a',b'}$ telle que $f_{a,b} \circ f_{a',b'} = f_{1,0}$, soit $aa' = 1$ et $ab'+b = 0$, d'où $a' = \dfrac{1}{a}$ et $b' = -\dfrac{b}{a}$. On vérifie que $f_{\frac{1}{a},-\frac{b}{a}}$ convient aussi de l'autre côté.

Enfin $f_{2,0} \circ f_{1,1} = f_{2,2}$ tandis que $f_{1,1} \circ f_{2,0} = f_{2,1}$.

$(G\,;\circ)$ est un groupe non abélien.

2. La somme de deux fonctions croissantes est croissante, l'addition des fonctions est associative, et la fonction nulle est croissante et neutre. En revanche, si f est croissante et non constante, $-f$ est décroissante et n'appartient pas à G : par exemple $f = \mathrm{Id}_{\mathbb{R}}$ n'a pas d'opposé dans G.

Ce n'est pas un groupe : l'axiome **S** échoue.

3. On dresse la table de Cayley, en calculant par exemple $f_2 \circ f_3(x) = f_2\left(\frac{1}{x}\right) = -\frac{1}{x} = f_4(x)$.

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

La table ne fait intervenir que des éléments de G : la loi est interne. Elle est associative comme composition d'applications, admet $f_1 = \mathrm{Id}$ pour neutre, et chaque élément est son propre symétrique.

$(G\,;\circ)$ est un groupe abélien à quatre éléments.

On reconnaît, aux noms près, la table obtenue à l'exercice 6 : ce sont « les mêmes » quatre éléments.

4. Soient x et y dans $]-1\,;1[$. Alors $|xy| < 1$, donc $1 + xy > 0$, et :

$$1 - x \star y = \frac{(1+xy)-(x+y)}{1+xy} = \frac{(1-x)(1-y)}{1+xy} > 0 \qquad 1 + x \star y = \frac{(1+x)(1+y)}{1+xy} > 0$$

Donc $-1 < x \star y < 1$: la loi est interne. Elle est visiblement commutative, et un calcul donne :

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

Le neutre est 0, et le symétrique de x est $-x$, qui appartient bien à $]-1\,;1[$.

$(G\,;\star)$ est un groupe abélien.

5. La loi est interne sur $\mathbb{R}^2$. Un calcul donne, pour les deux parenthésages :

$$y\,\mathrm{e}^{x'+x''} + y'\,\mathrm{e}^{x''-x} + y''\,\mathrm{e}^{-x-x'}$$

en seconde composante, et $x+x'+x''$ en première : la loi est associative. Le neutre est $(0\,;0)$, puisque :

$$(x\,;y) \diamond (0\,;0) = (x\,;\, y\,\mathrm{e}^0 + 0) = (x\,;y) \qquad \text{et} \qquad (0\,;0) \diamond (x\,;y) = (x\,;\, 0 + y\,\mathrm{e}^0) = (x\,;y)$$

Le symétrique de $(x\,;y)$ est $(-x\,;-y)$, car $y\,\mathrm{e}^{-x} + (-y)\,\mathrm{e}^{-x} = 0$. Enfin :

$$(1\,;0) \diamond (0\,;1) = \left(1\,;\,\mathrm{e}^{-1}\right) \qquad \text{tandis que} \qquad (0\,;1) \diamond (1\,;0) = (1\,;\,\mathrm{e})$$

$(G\,;\diamond)$ est un groupe non abélien.

EXERCICE 9 ⋆⋆

1. *Internité.* Si x et x' sont non nuls, xx' l'est aussi, et $xy'+y$ est un réel.
Associativité. Les deux parenthésages donnent la même chose :

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

$$(x\,;y)*((x'\,;y')*(x''\,;y'')) = (x\,;y)*(x'x''\,;x'y''+y') = (xx'x''\,;\,x(x'y''+y')+y)$$

Neutre. On vérifie $(x\,;y)*(1\,;0) = (x\,;\,0+y) = (x\,;y)$ et $(1\,;0)*(x\,;y) = (x\,;\,y+0) = (x\,;y)$.
Symétrique. On résout $(x\,;y)*(x'\,;y') = (1\,;0)$, soit $xx'=1$ et $xy'+y=0$, d'où $x' = \dfrac{1}{x}$ et $y' = -\dfrac{y}{x}$.
On vérifie que ce couple convient aussi à gauche.
Enfin $(2\,;0)*(1\,;1) = (2\,;2)$ alors que $(1\,;1)*(2\,;0) = (2\,;1)$.

$$\boxed{(\mathbb{R}^*\times\mathbb{R}\,;*) \text{ est un groupe non abélien.}}$$

2. On applique la définition de la loi :

$$(x\,;y)^2 = (x\,;y)*(x\,;y) = (x^2\,;\,xy+y) = \boxed{(x^2\,;\,y(x+1))}$$

$$(x\,;y)^3 = (x\,;y)^2*(x\,;y) = (x^3\,;\,x^2y+y(x+1)) = \boxed{(x^3\,;\,y(x^2+x+1))}$$

3. On conjecture, en notant $S_n = 1+x+\cdots+x^{n-1}$:

$$\boxed{\forall n\in\mathbb{N}^*,\quad (x\,;y)^n = (x^n\,;\,y\,S_n)}$$

Démonstration par récurrence. La formule est vraie pour $n=1$, où $S_1=1$. Supposons-la vraie au rang n :

$$(x\,;y)^{n+1} = (x\,;y)^n*(x\,;y) = (x^n\,;\,y\,S_n)*(x\,;y) = (x^{n+1}\,;\,x^ny+y\,S_n) = (x^{n+1}\,;\,y\,S_{n+1})$$

puisque $S_n+x^n = S_{n+1}$. La formule est donc vraie pour tout $n\in\mathbb{N}^*$.

4. La somme S_n est celle des termes d'une suite géométrique de raison x.

$$\boxed{\text{Si } x\neq 1 \ :\ (x\,;y)^n = \left(x^n\,;\,y\,\frac{x^n-1}{x-1}\right) \qquad \text{et si } x=1 \ :\ (1\,;y)^n = (1\,;\,ny)}$$

EXERCICE 10 ⋆⋆

1. On développe :

$$1+x*y = 1+x+y+xy = (1+x)(1+y)$$

Si $x\neq -1$ et $y\neq -1$, alors $1+x\neq 0$ et $1+y\neq 0$, donc $1+x*y\neq 0$, c'est-à-dire $x*y\neq -1$.

$$\boxed{* \text{ est une loi interne sur } G=\mathbb{R}\setminus\{-1\}.}$$

2. *Commutativité.* L'expression $x+y+xy$ est symétrique en x et y.
Associativité. En appliquant deux fois l'identité de la question 1 :

$$1+(x*y)*z = (1+x*y)(1+z) = (1+x)(1+y)(1+z)$$

expression symétrique en x, y et z. Donc $(x*y)*z = x*(y*z)$.
Neutre. On a $x*0 = x+0+0 = x$, et $0\in G$: le neutre est 0.
Symétrique. On cherche $y\in G$ tel que $x*y=0$, c'est-à-dire $(1+x)(1+y)=1$, soit :

$$1+y = \frac{1}{1+x} \qquad \text{donc} \qquad y = \frac{1}{1+x}-1 = \frac{-x}{1+x}$$

Ce réel appartient bien à G : si l'on avait $\dfrac{-x}{1+x} = -1$, il viendrait $-x = -1 - x$, ce qui est absurde.

$$\boxed{(G\,;*) \text{ est un groupe abélien de neutre } 0, \text{ le symétrique de } x \text{ étant } \frac{-x}{1+x}.}$$

3. Posons $\varphi : x \mapsto 1 + x$. C'est une bijection de $G = \mathbb{R} \setminus \{-1\}$ sur $\mathbb{R}^*$, de réciproque $t \mapsto t - 1$, et la question 1 s'écrit :

$$\varphi(x * y) = \varphi(x) \times \varphi(y)$$

La loi $*$ n'est que la multiplication de $\mathbb{R}^*$, transportée sur G par la bijection φ.
Les deux groupes sont « les mêmes », à ce changement de nom près.

C'est le même phénomène qu'à l'exercice 3, question 3, où l'addition de $\mathbb{Z}$ était déguisée par $x \mapsto x - 3$.

EXERCICE 11 ⋆⋆

1. Une bijection de E dans E est déterminée par le triplet $(\sigma(1)\,;\sigma(2)\,;\sigma(3))$, dont les trois coordonnées sont distinctes et prises dans $\{1\,;2\,;3\}$. Il y a 3 choix pour $\sigma(1)$, puis 2, puis 1.

$$\boxed{\mathcal{S}(E) \text{ possède } 3 \times 2 \times 1 = 6 \text{ éléments.}}$$

$$(1\,;2\,;3) \quad (1\,;3\,;2) \quad (2\,;1\,;3) \quad (2\,;3\,;1) \quad (3\,;1\,;2) \quad (3\,;2\,;1)$$

2. On vérifie les quatre axiomes, les trois premiers reposant sur le chapitre 2.

- **I** : la composée de deux bijections est une bijection.
- **A** : la composition des applications est associative.
- **N** : Id_E est bijective et neutre pour $\circ$.
- **S** : si σ est bijective, sa réciproque σ^{-1} l'est aussi et vérifie $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}_E$.

$$\boxed{(\mathcal{S}(E)\,;\circ) \text{ est un groupe.}}$$

3. On calcule image par image, en se souvenant que $\sigma \circ \tau$ applique τ en premier :

$$(\sigma \circ \tau)(1) = \sigma(1) = 2 \qquad (\sigma \circ \tau)(2) = \sigma(3) = 3 \qquad (\sigma \circ \tau)(3) = \sigma(2) = 1$$

$$(\tau \circ \sigma)(1) = \tau(2) = 3 \qquad (\tau \circ \sigma)(2) = \tau(1) = 1 \qquad (\tau \circ \sigma)(3) = \tau(3) = 2$$

$$\boxed{\sigma \circ \tau = (2\,;3\,;1) \qquad \tau \circ \sigma = (3\,;1\,;2) \qquad \text{donc } \mathcal{S}(E) \text{ n'est pas abélien.}}$$

4. Le symétrique de σ est sa bijection réciproque. Les quatre premiers éléments listés ci-dessous vérifient $\sigma \circ \sigma = \mathrm{Id}$, les deux derniers s'échangent.

$$\boxed{\begin{array}{l}(1\,;2\,;3),\ (1\,;3\,;2),\ (2\,;1\,;3) \text{ et } (3\,;2\,;1) \text{ sont leur propre symétrique}\,;\\ (2\,;3\,;1) \text{ et } (3\,;1\,;2) \text{ sont symétriques l'un de l'autre.}\end{array}}$$

Premières propriétés et groupe produit

EXERCICE 12 ⋆

1. Les égalités $x \cdot x^{-1} = x^{-1} \cdot x = e$ montrent que x est un symétrique de x^{-1}. La loi étant associative, la proposition 2 assure l'unicité du symétrique :

$$\boxed{\left(x^{-1}\right)^{-1} = x}$$

2. On applique deux fois la propriété 3, en traitant xyz comme $(xy)z$:

$$(xyz)^{-1} = \left((xy)z\right)^{-1} = z^{-1}(xy)^{-1} = \boxed{z^{-1}y^{-1}x^{-1}}$$

3. En multipliant à gauche par a^{-1}, puis à droite pour la seconde équation :

$$ax = b \iff a^{-1}ax = a^{-1}b \iff \boxed{x = a^{-1}b} \qquad xa = b \iff \boxed{x = ba^{-1}}$$

Ces deux solutions coïncident si G est abélien, mais pas en général.

4. D'après la question 2 et la question 1 :

$$\left(aba^{-1}\right)^{-1} = \left(a^{-1}\right)^{-1}b^{-1}a^{-1} = \boxed{ab^{-1}a^{-1}}$$

Pour la puissance, on remarque que les facteurs intérieurs se simplifient deux à deux :

$$\left(aba^{-1}\right)^2 = ab\underbrace{a^{-1}a}_{=e}ba^{-1} = ab^2a^{-1}$$

et une récurrence immédiate donne :

$$\boxed{\left(aba^{-1}\right)^n = ab^na^{-1}}$$

5. Si G est abélien, alors $y^{-1}x^{-1} = x^{-1}y^{-1}$, et la propriété 3 donne :

$$\boxed{(xy)^{-1} = x^{-1}y^{-1}}$$

Piège : cette égalité est *fausse* en général. C'est bien $y^{-1}x^{-1}$ qu'il faut écrire, l'inversion renversant l'ordre.

EXERCICE 13 ⋆⋆

1. Supposons $ax = ay$. En multipliant à gauche par a^{-1}, qui existe puisque G est un groupe :

$$a^{-1}(ax) = a^{-1}(ay) \implies (a^{-1}a)x = (a^{-1}a)y \implies ex = ey \implies x = y$$

Le raisonnement est symétrique pour $xa = ya$, en multipliant cette fois à droite.

Tout élément d'un groupe est régulier, à gauche comme à droite.

2. La ligne de a dans la table est constituée des éléments ax, pour x parcourant G. Si deux d'entre eux coïncident, disons $ax = ay$, la régularité donne $x = y$: deux cases distinctes ne peuvent donc pas contenir le même élément. Comme la ligne compte exactement autant de cases que G a d'éléments, chacun y figure exactement une fois. Le raisonnement est identique pour les colonnes.

La table de Cayley d'un groupe fini est un carré latin.

3. Dans la seconde table de l'exercice 5, la ligne de a est $(a\,;e\,;a)$: l'élément a y figure deux fois.

Cette table ne peut donc pas être celle d'un groupe.

C'est un critère bien plus rapide que la recherche d'un contre-exemple à l'associativité.

4. Si $x^2 = e$, alors $x \cdot x = e$, donc x est son propre symétrique : $x^{-1} = x$. Soient alors x et y dans G. En appliquant ce résultat à xy, puis la propriété 3 :

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

$$\boxed{G \text{ est abélien.}}$$

5. Deux exemples déjà rencontrés conviennent :

$$\boxed{(\mathcal{P}(E)\,;\Delta) \text{ de l'exercice 6, et le groupe } \{f_1\,;f_2\,;f_3\,;f_4\} \text{ de l'exercice 8.}}$$

On peut ajouter le groupe $(E\,;*)$ de la première table de l'exercice 5 : ces trois groupes ont la même table, aux noms près.

EXERCICE 14 ⋆⋆

1. D'après la proposition 4, le groupe produit de $(G\,;\cdot)$ et $(H\,;*)$ est $G \times H$ muni de la loi $(x\,;y) \perp (x'\,;y') = (x \cdot x'\,;\, y * y')$. Ici, avec $G = H = (\mathbb{Z}\,;+)$:

Internité : la somme de deux entiers est un entier, sur chaque composante. *Associativité* : elle vaut composante par composante, car $+$ est associative sur $\mathbb{Z}$. *Neutre* : $(0\,;0)$. *Symétrique* de $(a\,;b)$: $(-a\,;-b)$.

$$\boxed{(\mathbb{Z} \times \mathbb{Z}\,;+) \text{ est un groupe abélien, de neutre } (0\,;0).}$$

2. C'est le groupe produit de $(\mathbb{R}\,;+)$ et de $(\mathbb{R}^*\,;\times)$, tous deux groupes.

$$\boxed{\text{C'est un groupe, de neutre } (0\,;1),\ \text{le symétrique de } (x\,;y) \text{ étant } \left(-x\,;\,\frac{1}{y}\right).}$$

3. Soient $(x\,;y)$ et $(x'\,;y')$ dans $G \times H$, avec G et H abéliens :

$$(x\,;y) \perp (x'\,;y') = (x \cdot x'\,;\, y * y') = (x' \cdot x\,;\, y' * y) = (x'\,;y') \perp (x\,;y)$$

$$\boxed{\text{Le groupe produit de deux groupes abéliens est abélien.}}$$

4. Dans un groupe produit, chaque composante du résultat ne dépend que des composantes correspondantes. Or la seconde composante de $(x\,;y) * (x'\,;y')$ vaut $xy' + y$: elle fait intervenir x, qui appartient à la *première* composante.

$$\boxed{\text{Non : } * \text{ n'est pas la loi produit.}}$$

Un second argument, décisif : $(\mathbb{R}^*\,;\times)$ et $(\mathbb{R}\,;+)$ étant abéliens, leur groupe produit le serait aussi d'après la question 3, alors que $(\mathbb{R}^* \times \mathbb{R}\,;*)$ ne l'est pas.

Sous-groupes

EXERCICE 15 ⋆

On applique la méthode du cours : inclusion, non-vacuité, puis stabilité par xy^{-1}.

1. On a $H = 2\mathbb{Z} \subset \mathbb{Z}$, et $0 = 2 \times 0 \in H$. Soient $x = 2k$ et $y = 2k'$ dans H. La loi étant additive, le symétrique de y est $-y$, et :

$$x - y = 2k - 2k' = 2(k - k') \qquad \text{avec } k - k' \in \mathbb{Z}$$

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

2. L'entier 0 est pair, donc n'appartient pas à H.

$$\boxed{H \text{ n'est pas un sous-groupe : il ne contient pas le neutre.}}$$

On pouvait aussi invoquer la stabilité : 1 et 3 sont impairs, mais $1-3=-2$ ne l'est pas.

3. On a bien $0 \in H$, mais H n'est pas stable : $0 \in H$ et $5 \in H$, alors que $0-5=-5 \notin H$.

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

4. On a $\mathbb{Q}^* \subset \mathbb{R}^*$, et $1 \in \mathbb{Q}^*$. Soient x et y dans $\mathbb{Q}^*$: le quotient $\dfrac{x}{y}$ est un rationnel non nul.

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

5. On a $H \subset \mathbb{C}^*$, et $1 \in H$ car $1^1=1$. Soient z et w dans H, avec $z^n=1$ et $w^m=1$ pour certains n et m de $\mathbb{N}^*$. Alors $nm \in \mathbb{N}^*$ et :

$$\left(zw^{-1}\right)^{nm} = z^{nm}\left(w^{nm}\right)^{-1} = \left(z^n\right)^m\Big(\left(w^m\right)^n\Big)^{-1} = 1\times 1 = 1$$

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

Cet ensemble est la réunion des $\mathbb{U}_n$ de l'exercice 18 : c'est l'ensemble des *racines de l'unité*.

6. *Inclusion.* Montrons d'abord que $H \subset \mathbb{R}^*$, c'est-à-dire qu'un élément de H n'est jamais nul. Supposons $a+b\sqrt{2}=0$ avec $(a\,;b) \neq (0\,;0)$. Si $b=0$, alors $a=0$: exclu. Donc $b \neq 0$ et $\sqrt{2} = -\dfrac{a}{b} \in \mathbb{Q}$, ce qui contredit l'irrationalité de $\sqrt{2}$.

Non-vacuité. $1 = 1+0\sqrt{2} \in H$.

Stabilité. Soient $x=a+b\sqrt{2}$ et $y=c+d\sqrt{2}$ dans H. Le même argument que ci-dessus montre que $c^2-2d^2 \neq 0$, et l'on calcule :

$$y^{-1} = \frac{1}{c+d\sqrt{2}} = \frac{c-d\sqrt{2}}{c^2-2d^2} = \frac{c}{c^2-2d^2} - \frac{d}{c^2-2d^2}\sqrt{2}$$

qui est de la forme voulue, à coefficients rationnels non tous nuls. Enfin :

$$(a+b\sqrt{2})(p+q\sqrt{2}) = (ap+2bq)+(aq+bp)\sqrt{2}$$

est encore de cette forme, et non nul comme produit de deux réels non nuls.

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

EXERCICE 16 ⋆

1. On a $n\mathbb{Z} \subset \mathbb{Z}$, et $0 = n\times 0 \in n\mathbb{Z}$. Soient $x=nk$ et $y=nk'$ dans $n\mathbb{Z}$:

$$x-y = n(k-k') \in n\mathbb{Z}$$

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

2. On applique la définition avec $n=1$ puis $n=0$:

$$\boxed{1\mathbb{Z}=\mathbb{Z} \qquad \text{et} \qquad 0\mathbb{Z}=\{0\}}$$

Ce sont les deux sous-groupes « extrêmes » : le groupe tout entier et le sous-groupe trivial.

3. *Sens direct.* Supposons $n\mathbb{Z} \subset m\mathbb{Z}$. Comme $n = n\times 1 \in n\mathbb{Z}$, on a $n \in m\mathbb{Z}$: il existe $q \in \mathbb{Z}$ tel que $n=mq$, donc m divise n.

Réciproque. Supposons $n = mq$ avec $q \in \mathbb{Z}$. Tout élément de $n\mathbb{Z}$ s'écrit $nk = m(qk)$ avec $qk \in \mathbb{Z}$, donc appartient à $m\mathbb{Z}$.

$$\boxed{n\mathbb{Z} \subset m\mathbb{Z} \iff m \text{ divise } n}$$

Piège : l'inclusion et la divisibilité vont en sens *inverse*. Plus n est grand au sens de la divisibilité, plus $n\mathbb{Z}$ est petit.

4. Un entier appartient à $4\mathbb{Z} \cap 6\mathbb{Z}$ s'il est à la fois multiple de 4 et de 6, donc multiple de leur plus petit commun multiple 12 ; réciproquement tout multiple de 12 convient.

$$\boxed{4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z} \qquad \text{et} \qquad 4\mathbb{Z} \cap 5\mathbb{Z} = 20\mathbb{Z}}$$

$$\boxed{\text{On conjecture } n\mathbb{Z} \cap m\mathbb{Z} = \text{ppcm}(n\,;m)\,\mathbb{Z}.}$$

EXERCICE 17 ⋆⋆

1. On a $H \cap K \subset G$. De plus $e \in H$ et $e \in K$, donc $e \in H \cap K$, qui n'est pas vide. Soient enfin x et y dans $H \cap K$. Comme H est un sous-groupe, $xy^{-1} \in H$; comme K en est un, $xy^{-1} \in K$. Donc $xy^{-1} \in H \cap K$.

$$\boxed{H \cap K \text{ est un sous-groupe de } G.}$$

2. On a $2 \in 2\mathbb{Z}$ et $3 \in 3\mathbb{Z}$, donc tous deux appartiennent à $2\mathbb{Z} \cup 3\mathbb{Z}$. Pourtant $2 + 3 = 5$ n'est ni pair ni multiple de 3.

$$\boxed{2\mathbb{Z} \cup 3\mathbb{Z} \text{ n'est pas stable, donc n'est pas un sous-groupe de } (\mathbb{Z}\,;+).}$$

3. Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G, et $H = \bigcap_{i\in I} H_i$. Chaque H_i contient e, donc H aussi. Soient x et y dans H : pour tout $i \in I$, on a $x \in H_i$ et $y \in H_i$, donc $xy^{-1} \in H_i$. Ceci valant pour tout i, on obtient $xy^{-1} \in H$.

$$\boxed{\text{Oui : une intersection quelconque de sous-groupes est un sous-groupe.}}$$

L'asymétrie avec la réunion mérite d'être notée : l'intersection se comporte bien, la réunion non. C'est l'objet de l'exercice 22.

EXERCICE 18 ⋆⋆

1. Si $|z| = 1$ alors $z \neq 0$, donc $\mathbb{U} \subset \mathbb{C}^*$. De plus $|1| = 1$, donc $1 \in \mathbb{U}$. Soient z et w dans $\mathbb{U}$:

$$|zw^{-1}| = \frac{|z|}{|w|} = \frac{1}{1} = 1$$

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

2. Si $z^n = 1$ alors $z \neq 0$, donc $\mathbb{U}_n \subset \mathbb{C}^*$, et $1^n = 1$ donne $1 \in \mathbb{U}_n$. Soient z et w dans $\mathbb{U}_n$:

$$(zw^{-1})^n = z^n (w^n)^{-1} = 1$$

Enfin, si $z^n = 1$, alors $|z|^n = 1$; comme $|z|$ est un réel strictement positif, cela impose $|z| = 1$.

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

3. Supposons $m = nq$ avec $q \in \mathbb{N}^*$, et soit $z \in \mathbb{U}_n$. Alors :

$$z^m = z^{nq} = (z^n)^q = 1^q = 1$$

$$\boxed{n \text{ divise } m \implies \mathbb{U}_n \subset \mathbb{U}_m}$$

4. On résout $z^4 = 1$. Les quatre solutions sont :

$$\boxed{\mathbb{U}_4 = \{1\,;\mathrm{i}\,;-1\,;-\mathrm{i}\}}$$

C'est exactement l'ensemble dont le cours dresse la table de Cayley. On retrouve donc, mais cette fois par une démonstration générale, que cette table est bien celle d'un groupe.

EXERCICE 19 ⋆⋆⋆

1. *Le centre.* On a $C(G) \subset G$ par définition, et $e \in C(G)$ puisque $ey = ye = y$ pour tout y.

Soient x et x' dans $C(G)$, et $y \in G$. De l'égalité $x'y = yx'$, on tire en multipliant à gauche et à droite par x'^{-1} :

$$y\,x'^{-1} = x'^{-1}y$$

On calcule alors, en utilisant successivement cette égalité puis celle vérifiée par x :

$$(x\,x'^{-1})y = x(x'^{-1}y) = x(y\,x'^{-1}) = (xy)\,x'^{-1} = (yx)\,x'^{-1} = y(x\,x'^{-1})$$

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

2. *Le conjugué.* On a $aHa^{-1} \subset G$, et $e = aea^{-1} \in aHa^{-1}$ puisque $e \in H$.

Soient aha^{-1} et $ah'a^{-1}$ deux éléments de aHa^{-1}. D'après l'exercice 12, $(ah'a^{-1})^{-1} = a\,h'^{-1}a^{-1}$, d'où :

$$(aha^{-1})(ah'a^{-1})^{-1} = a\,h\,\underbrace{a^{-1}a}_{=e}\,h'^{-1}a^{-1} = a(h\,h'^{-1})a^{-1}$$

Comme H est un sous-groupe, $h\,h'^{-1} \in H$, donc ce produit appartient à aHa^{-1}.

$\boxed{aHa^{-1} \text{ est un sous-groupe de } G.}$

3. *Les éléments de torsion.* On a $T(G) \subset G$, et $e \in T(G)$ car $e^1 = e$ avec $1 \in \mathbb{N}^*$.

Soient x et y dans $T(G)$, avec $x^n = e$ et $y^m = e$ pour certains n et m de $\mathbb{N}^*$. Comme G est abélien, on peut développer la puissance d'un produit :

$$(xy^{-1})^{nm} = x^{nm}(y^{-1})^{nm} = (x^n)^m\Big((y^m)^n\Big)^{-1} = e$$

et $nm \in \mathbb{N}^*$, donc $xy^{-1} \in T(G)$.

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

Où sert la commutativité ? Uniquement à écrire $(xy^{-1})^k = x^k(y^{-1})^k$. Dans un groupe quelconque, $(xy)^2 = xyxy$ ne se simplifie pas en x^2y^2, et $T(G)$ peut alors ne pas être un sous-groupe.

Exercices de synthèse

EXERCICE 20 : VRAI OU FAUX

1. **Fausse** La soustraction sur $\mathbb{Z}$ n'admet pas de neutre : $x - e = x$ impose $e = 0$, mais $0 - x = -x$ n'est égal à x que si $x = 0$. Il faut un neutre *des deux côtés*.

2. **Vraie** C'est la proposition 1 du cours : si e et e' sont neutres, le calcul de $e * e'$ des deux façons donne $e = e'$.

3. **Fausse** L'unicité, énoncée par la proposition 2, exige que la loi soit *associative*. C'est cette hypothèse qui autorise le calcul de $y * x * y'$ sans parenthèses.

4. **Fausse** La proposition 3 donne $(xy)^{-1} = y^{-1}x^{-1}$. L'égalité annoncée n'est vraie que si G est abélien (exercice 12, question 5).

5. **Vraie** La commutativité ne figure pas dans les axiomes **IANS**. Les exercices 8, 9 et 11 en fournissent trois contre-exemples.

6. **Vraie** Les axiomes **I**, **A** et **N** sont satisfaits ; c'est **S** qui échoue, et c'est précisément ce manque qui motive la construction de $\mathbb{Z}$.

7. **Vraie** C'est la première condition de la définition. La caractérisation de la proposition 5 la remplace par la non-vacuité, mais le neutre s'en déduit aussitôt.

8. **Vraie** C'est la question 1 de l'exercice 17.

9. **Fausse** L'ensemble $2\mathbb{Z}\cup 3\mathbb{Z}$ n'est pas stable, puisque $2+3=5$ n'y appartient pas. L'exercice 22 précise exactement quand la réunion est un sous-groupe.

10. **Vraie** C'est la caractérisation de la proposition 5, celle que l'on utilise en pratique.

EXERCICE 21 ⋆⋆⋆

1. Pour tout $x \in G$:

$$(\tau_a \circ \tau_{a^{-1}})(x) = a(a^{-1}x) = (aa^{-1})x = x \qquad (\tau_{a^{-1}} \circ \tau_a)(x) = a^{-1}(ax) = x$$

Les deux composées valent Id_G, ce qui prouve d'après le chapitre 2 que τ_a est bijective.

$$\boxed{\tau_a \text{ est bijective, de bijection réciproque } \tau_{a^{-1}}.}$$

2. Pour tout $x \in G$, l'associativité donne :

$$(\tau_a \circ \tau_b)(x) = a(bx) = (ab)x = \tau_{ab}(x) \qquad \text{donc} \qquad \boxed{\tau_a \circ \tau_b = \tau_{ab}}$$

3. D'après la question 1, chaque τ_a est une bijection de G : on a bien $T \subset \mathcal{S}(G)$. De plus $\tau_e = \mathrm{Id}_G$ appartient à T, qui n'est donc pas vide. Soient enfin τ_a et τ_b dans T. La question 1 donne $\tau_b^{-1} = \tau_{b^{-1}}$, puis la question 2 :

$$\tau_a \circ \tau_b^{-1} = \tau_a \circ \tau_{b^{-1}} = \tau_{ab^{-1}} \in T$$

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

4. Soient a et b dans G tels que $\tau_a = \tau_b$. Ces deux applications prenant la même valeur en tout point, évaluons-les en e :

$$a = ae = \tau_a(e) = \tau_b(e) = be = b$$

$$\boxed{\Phi \text{ est injective.}}$$

5. L'application Φ est injective et son image est exactement T : elle réalise donc une bijection de G sur T. De plus, la question 2 montre qu'elle transporte la loi de G sur la composition : $\Phi(ab) = \Phi(a) \circ \Phi(b)$.

> Tout groupe est « le même » qu'un sous-groupe d'un groupe de bijections.
> C'est le *théorème de Cayley*.

Autrement dit, l'étude des groupes abstraits ne dit rien de plus que celle des groupes de bijections — ce qui justifie *a posteriori* l'importance du groupe symétrique rencontré à l'exercice 11.

EXERCICE 22 ⋆⋆⋆

1. Si $H \subset K$, alors $H \cup K = K$, qui est un sous-groupe de G par hypothèse. Si $K \subset H$, alors $H \cup K = H$, qui en est un également.

$$\boxed{\text{Dans les deux cas, } H \cup K \text{ est un sous-groupe de } G.}$$

2. (a) On a $h \in H \subset H \cup K$ et $k \in K \subset H \cup K$. Comme $H \cup K$ est supposé être un sous-groupe, il est stable par la loi :

$$\boxed{hk \in H \cup K}$$

(b) Supposons par l'absurde que $hk \in K$. Comme K est un sous-groupe et que $k \in K$, on a $k^{-1} \in K$, puis :

$$h = h(kk^{-1}) = (hk)k^{-1} \in K$$

ce qui contredit le choix de h, pris dans H mais pas dans K.

$$\boxed{hk \notin K}$$

(c) D'après (a) et (b), on a nécessairement $hk \in H$. Comme $h \in H$, on a aussi $h^{-1} \in H$, donc :

$$k = (h^{-1}h)k = h^{-1}(hk) \in H$$

Cet argument valant pour tout k de K :

$$\boxed{K \subset H}$$

3. La question 1 donne un sens, la question 2 l'autre : si $H \cup K$ est un sous-groupe et si $H \not\subset K$, alors $K \subset H$.

$$\boxed{H \cup K \text{ est un sous-groupe de } G \iff H \subset K \text{ ou } K \subset H}$$

4. On a $2 \in 2\mathbb{Z}$ mais $2 \notin 3\mathbb{Z}$, donc $2\mathbb{Z} \not\subset 3\mathbb{Z}$; et $3 \in 3\mathbb{Z}$ mais $3 \notin 2\mathbb{Z}$, donc $3\mathbb{Z} \not\subset 2\mathbb{Z}$. Aucune des deux inclusions n'a lieu :

$$\boxed{2\mathbb{Z} \cup 3\mathbb{Z} \text{ n'est pas un sous-groupe de } (\mathbb{Z}\,;+).}$$

On retrouve le résultat de l'exercice 17, sans avoir eu besoin d'exhiber le contre-exemple $2 + 3 = 5$.