

# Feuille d'exercices 1

**Exercice 1.** Soit  $E = \{a, b\}$  un ensemble à deux éléments.

- On considère sur  $E$  la loi de composition interne  $*$  définie par  $a * a = a$ ,  $a * b = a$ ,  $b * a = b$ ,  $b * b = b$ . Cette loi est-elle commutative ? associative ?
- Mêmes questions pour la loi  $*$  définie par  $a * a = b$ ,  $a * b = a$ ,  $b * a = a$ ,  $b * b = a$ .
- Construire sur  $E$  une loi de composition interne  $*$  telle que  $(E, *)$  soit un groupe.

## Solution

(a) Rappelons les définitions d'après les suivantes

Déf: Soit  $E$  un ensemble muni d'une loi de composition interne  $*$ .

On dit que:

- la loi est commutative si,  $\forall a, b \in E$ , on a  $a * b = b * a$ .
- la loi est associative si,  $\forall a, b, c \in E$ , on a  $(a * b) * c = a * (b * c)$ .

Dans notre cas :

- On a que  $a * b = a$  et  $b * a = b$ . Comme  $a \neq b$  (car  $E$  a 2 éléments) la loi  $*$  n'est pas commutative.
- Nous avons différents cas à analyser:
  - $(a * b) * a = a * a = a$  et  $a * (b * a) = a * b = a$
  - $(a * b) * b = a * b = a$  et  $a * (b * b) = a * b = a$
  - $(a * a) * a = a * a = a$  et  $a * (a * a) = a * a = a$
  - $(a * a) * b = a * b = a$  et  $a * (a * b) = a * a = a$
  - $(b * a) * a = b * a = b$  et  $b * (a * a) = b * a = b$
  - $(b * a) * b = b * b = b$  et  $b * (a * b) = b * a = b$
  - $(b * b) * a = b * a = b$  et  $b * (b * a) = b * b = b$
  - $(b * b) * b = b * b = b$  et  $b * (b * b) = b * b = b$

Dans tous les cas on a égalité, donc la loi  $*$  est associative.

(2) Nous avons que  $a+b = b+a$  donc la loi est commutative.  
Par contre elle n'est pas associative car, par exemple nous avons  
 $(b+a)+a = a+a=b$  mais  $b+(a+a)=b+b=a$

(3) Rappelons la définition suivante:

Déf: On appelle groupe un ensemble  $G$  muni d'une loi de composition interne  $*$  possédant les propriétés suivantes:

- 1) La loi est associative:  $\forall a,b,c \in G, a*(b*c)=(a*b)*c$
- 2) Il existe un élément neutre  $e \in G$ :  $\forall a \in G, a*e=e*a=a$
- 3) Tout élément  $a \in G$  possède un élément symétrique  $a' \in G$  tel que  
 $a*a'=a'*a=e$

On doit donc trouver une loi  $*$  sur l'ensemble  $E=\{a,b\}$  satisfaisant les propriétés précédentes.

La propriété (2) en particulier donne l'existence d'un élément neutre.  
A' moins d'échanger le rôle de  $a$  et  $b$ , on peut supposer que  $a$  soit l'élément neutre. On doit donc avoir:

$$a+a=a, a+b=b, b+a=b.$$

Il nous reste à décider à quoi est égale le produit  $b+b$ .

D'après (3), chaque élément de  $E$  doit avoir un symétrique.

On a que  $a$  est le symétrique de lui même.

Comme  $b$  doit aussi avoir un symétrique (et il ne peut pas être  $a$  car  $b+a=a+b=b$  qui n'est pas l'élément neutre) forcément  $b$  est aussi le symétrique de lui même, donc  $b+b=a$ .

Vérifions que la loi  $*$  si définie est associative.

Nous avons que :

- $(a * b) * a = b * a = b$  et  $a * (b * a) = a * b = b$
- $(a * b) * b = b * b = a$  et  $a * (b * b) = a * a = a$
- $(a * a) * a = a * a = a$  et  $a * (a * a) = a * a = a$
- $(a * a) * b = a * b = b$  et  $a * (a * b) = a * b = b$
- $(b * a) * a = b * a = b$  et  $b * (a * a) = b * a = b$
- $(b * a) * b = b * b = a$  et  $b * (a * b) = b * b = a$
- $(b * b) * a = a * a = a$  et  $b * (b * a) = b * b = a$
- $(b * b) * b = a * b = b$  et  $b * (b * b) = b * a = b$

Réu Nous pouvons aussi observer que la loi que l'on vient de définir est commutative car  $a * b = b = b * a$ .

Nous avons démontré que :

- (1) Un ensemble de deux éléments admet une seule structure de groupe (à moins d'échanger les éléments entre eux).
  - (2) Un groupe à deux éléments est forcément abélien c.à.d. la loi de groupe est forcément commutative.
- 

**Exercice 2.** On munit l'ensemble  $\mathbb{R}$  d'une loi de composition  $*$  définie par  $a * b = a + b - ab$  pour tous les  $a, b \in \mathbb{R}$ .

- Vérifier que la loi  $*$  est associative, et admet un élément neutre que l'on identifiera.
- Déterminer tous les éléments  $a \in \mathbb{R}$  admettant un symétrique  $a'$  pour la loi  $*$ .
- Vérifier que  $\mathbb{R} \setminus \{1\}$ , muni de la loi  $*$ , est un groupe abélien.

## Solution

(a) Soient  $a, b, c \in \mathbb{R}$ . On doit vérifier que  $(a * b) * c = a * (b * c)$ .

- Nous avons que d'une part

$$\begin{aligned}
 (a * b) * c &= (a + b - ab) * c = (a + b - ab) + c - (a + b - ab) \cdot c = \\
 &= a + b + c - ab - ac - bc + abc
 \end{aligned}$$

D'autre part

$$\begin{aligned} a * (b * c) &= a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = \\ &= a + b + c - bc - ab - ac + abc \end{aligned}$$

On a donc l'égalité souhaitée.

- Pour l'élément neutre : rappelons la définition d'après

On dit que  $e \in E$  est un élément neutre pour la loi  $*$  si

$$\forall a \in E \text{ on a : } a * e = e * a = a.$$

Dans notre exemple, on a que  $e \in \mathbb{R}$  est l'élément neutre pour la loi  $*$  si et seulement si  $\forall b \in \mathbb{R}$  on a  $e + b - e \cdot b = b + e - b \cdot e = b$ .

Ceci est équivalent à  $e - be = 0$ , donc  $e - e = 0$ .

Finalement,  $e = 0$  est l'élément neutre.

- (b) Rappelons d'abord la définition d'après :

Tout élément  $a \in G$  possède un élément symétrique  $a' \in G$  tel que

$$a * a' = a' * a = e$$

Dans notre cas on a que  $a \in \mathbb{R}$  a un symétrique  $a' \iff$

$$a * a' = a' * a = a + a' - a \cdot a' = 0.$$

Ceci équivaut à  $a'(a-1) = 0$ . Donc :

- si  $a \neq 1$ ,  $a' = \frac{a}{a-1}$  est le symétrique de  $a$ .

- si  $a = 1$  on a :

$$a'(a-1) = 0 \neq 1 = 1.$$

Donc les éléments de  $\mathbb{R}$  qui ont un symétrique sont les éléments de l'ensemble  $\mathbb{R} \setminus \{1\}$ .

- (c) Soit  $E = \mathbb{R} \setminus \{1\}$ . On veut montrer que  $(E, *)$  est un groupe abélien.

- Montrons que  $\star$  est stable par la loi  $\star$ .  
 Soient  $a, b \in \mathbb{R} \setminus \{1\}$ . Supposons par l'absurde  $a \star b = 1$ .  
 Alors  $a \star b = a + b - ab = 1$ , donc  $b(1-a) = 1-a$ .  
 En divisant par  $1-a$  (qui est différent de 0 car  $a \neq 1$  par hypothèse), on a  $b = 1$ , ce qui est absurde - car  $b \in \mathbb{R} \setminus \{1\}$ .  
 On a donc que  $\star$  est stable par la loi  $\star$ .
- On a déjà montré que la loi  $\star$  est associative sur  $\mathbb{R}$  (et donc sur son sous ensemble  $E$ ) (point (a)).
- On a que l'élément neutre  $e = 0$  appartient à  $\mathbb{R} \setminus \{1\}$ .
- On a montré (point (b)) que tout élément de  $E$  a un symétrique.
- Enfin, la loi  $\star$  est commutative car  

$$a \star b = a + b - ab = b + a - ba = b \star a$$

Donc  $E = \mathbb{R} \setminus \{1\}$  muni de  $\star$  est un groupe abélien.

---

**Exercice 4.** Montrer que les structures suivantes sont des groupes :

- $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ .
- $(\{-1, 1\}, \cdot)$ ,  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{C}^*, \cdot)$ .

c)  $(S(E), \circ)$ , où  $E$  est un ensemble fini et  $S(E)$  l'ensemble des bijections de  $E$  dans  $E$ .

Remarque : si  $E = \{1, \dots, n\}$ , on note  $S_n$  le groupe  $S(E)$ .

Solution Montrons que les structures suivantes sont des groupes.

Pour chaque structure  $(E, \star)$  il faudra vérifier que :

- la loi  $\star$  est interne
- la loi  $\star$  est associative
- il existe un élément neutre pour  $\star$ ,  $e \in E$
- chaque  $a \in E$  a un symétrique pour  $\star$   $a' \in E$

- (a) (i) Il est clair que la loi " $+$ " est interne pour tous les ensembles  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ .
- (ii) Comme la loi " $+$ " est interne et  $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$  il suffit de montrer que (ii) est vrai pour  $E = \mathbb{C}$  c.à.d. que  $\forall a, b, c \in \mathbb{C}$  on a  $(a+b)+c = a+(b+c)$  qui est vrai par définition de l'addition.
- (iii) On remarque que  $0 = 0$  est l'élément neutre pour la loi " $+$ " et il appartient à tous les ensembles.
- (iv) On remarque que pour tout ensemble  $E \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ , si  $a \in E$  alors  $-a \in E$ . Donc chaque élément de  $E$  possède un symétrique.

- (b) (i) Il est clair que la loi " $\cdot$ " est interne pour  $E = \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ . On remarquera que si  $E = \{1, -1\}$  et  $a, b \in E \Rightarrow a \cdot b \in \{1, -1\} \Rightarrow a \cdot b \in E$ . Donc " $\cdot$ " est interne aussi pour l'ensemble  $E = \{-1, 1\}$ .
- (ii) Comme la loi est interne et  $\{1, -1\} \subseteq \mathbb{Q}^* \subseteq \mathbb{R}^* \subseteq \mathbb{C}^*$  il suffit de remarquer que " $\cdot$ " est associative pour  $\mathbb{C}^*$  c.à.d. que  $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall a, b, c \in \mathbb{C}$ .
- (iii) On remarque que  $1 = 1$  est l'élément neutre pour la loi " $\cdot$ " et il appartient à tous les ensembles.
- (iv) On remarque que pour chaque ensemble  $E$  de l'exercice, si  $a \in E$  alors  $1/a \in E$ . Donc chaque élément de  $E$  a un symétrique pour la loi " $\cdot$ ".

- (c) Soit  $E$  un ensemble fini et  $S(E)$  l'ensemble des bijections de  $E$  dans  $E$ , muni de la loi " $\circ$ " (composition de fonctions). Montrons que (i), (ii), (iii) et (iv) sont vérifiés.

(i) Soient  $f, g \in S(E)$  deux bijections de  $E$  dans  $E$ .

Alors  $f \circ g$  est aussi une application de  $E$  dans  $E$ .

- \* De plus  $f \circ g$  est injective : supposons  $f \circ g(a) = f \circ g(a')$  pour  $a, a' \in E$ . Comme  $f$  est injective, cela implique  $g(a) = g(a')$ . Comme  $g$  est injective, cela implique  $a = a'$ .  
Donc  $f \circ g$  est injective.

- \* Autre,  $f \circ g$  est surjective : Soit  $a' \in E$ . Comme  $f$  est surjective,  $\exists a'' \in E$  tel que  $f(a'') = a'$ .  
Comme  $g$  est surjective,  $\exists a \in E$  tel que  $g(a) = a''$ .  
Donc  $f \circ g(a) = a'$  et  $f \circ g$  est surjective.

On a donc montré que  $f \circ g \in S(E)$ , donc la loi " $\circ$ " est interne à  $S(E)$ .

(ii) Associativité : Soient  $f, g, h \in S(E)$ . On a que  $\forall a \in E$ ,

$$((f \circ g) \circ h)(a) = f \circ g \circ h(a) = f(g(h(a))) = (f \circ (g \circ h))(a)$$

Donc la loi est associative.

(iii) Soit  $\epsilon : E \rightarrow E$  l'application identité t.q.  $\epsilon(a) = a \quad \forall a \in E$ .

Clairement  $\epsilon \in S(E)$  et  $\epsilon$  est l'élément neutre pour  $\circ$   
car  $\forall f \in S(E)$ ,  $f \circ \epsilon(a) = f(a) = \epsilon \circ f(a)$ .

Donc  $f \circ \epsilon = \epsilon \circ f = f$ .

(iv) Soit  $f \in S(E)$  et soit  $f^{-1} : E \rightarrow E$  l'application  
définie par  $f^{-1}(a) = b$  si  $f(b) = a$ .

Cette application est bien définie car  $f$  est une  
bijection. De plus  $f^{-1} \in S(E)$  et  $f \circ f^{-1} = f^{-1} \circ f = \epsilon$ .

Donc chaque  $f \in S(E)$  a un symétrique pour la loi " $\circ$ ".

**Exercice 5.** Les ensembles suivants muni des lois considérées sont-ils des groupes ?

- a)  $G = \{f_1, f_2, f_3, f_4\}$  muni de la composition  $\circ$ , où  $f_1, f_2, f_3, f_4$  sont les applications de  $\mathbb{R}^*$  dans  $\mathbb{R}^*$  définies par  $f_1(x) = x$ ,  $f_2(x) = -x$ ,  $f_3(x) = 1/x$ ,  $f_4(x) = -1/x$ .
- b)  $H = \{f_{a,b}; (a, b) \in \mathbb{R}^* \times \mathbb{R}\}$  muni de la composition  $\circ$ , où  $f_{a,b}$  est l'application de  $\mathbb{R}$  dans  $\mathbb{R}$  définie par  $f_{a,b}(x) = ax + b$ .
- c) L'ensemble  $E$  des fonctions croissantes de  $\mathbb{R}$  dans  $\mathbb{R}$ , muni de l'addition.

## Solutions

(a) (i) Remarquons que la loi est interne car

$$f_1 \circ f_1 = f_1, f_1 \circ f_2 = f_2, f_1 \circ f_3 = f_3, f_1 \circ f_4 = f_4$$

$$f_2 \circ f_1 = f_2, f_2 \circ f_2 = f_1, f_2 \circ f_3 = f_4, f_2 \circ f_4 = f_3$$

$$f_3 \circ f_1 = f_3, f_3 \circ f_2 = f_4, f_3 \circ f_3 = f_1, f_3 \circ f_4 = f_2$$

$$f_4 \circ f_1 = f_4, f_4 \circ f_2 = f_1, f_4 \circ f_3 = f_2, f_4 \circ f_4 = f_1$$

(ii) La loi est associative car la composition de fonctions est associative. (voir correction exo 4 point (c) aussi).

(iii)  $f_1$  est l'élément neutre pour la loi " $\circ$ ", comme montré dans (i).

(iv) Comme montré dans (i) chaque élément de  $G$  est symétrique de lui-même.

Donc  $(G, \circ)$  est un groupe.

(b) (i) La loi  $\circ$  est interne à  $H$  car si  $f_{a,b}$  et  $f_{c,d} \in H$

avec  $a, c \in \mathbb{R}^*, b, d \in \mathbb{R} \Rightarrow$

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

et  $ac \in \mathbb{R}^*, ad+b \in \mathbb{R}$ . Donc  $f_{a,b} \circ f_{c,d} = f_{ac, ad+b} \in H$ .

(ii) La loi est associative car la composition de fonctions l'est.

(iii) L'élément neutre est  $f_{1,0}$  car  $f_{1,0}(x) = x \forall x \in \mathbb{R}$

donc  $f_{1,0} \circ f_{a,b} = f_{a,b} \circ f_{1,0} = f_{a,b} \quad \forall a \in \mathbb{R}^*, b \in \mathbb{R}$ .

(iv) Remarquons que si  $f_{a,b} \in H$  avec  $a \in \mathbb{R}^*, b \in \mathbb{R}$  alors

$$(f_{\frac{1}{a}, -\frac{b}{a}} \circ f_{a,b})(x) = \frac{1}{a}(ax + b) - \frac{b}{a} = x = f_{1,0}(x)$$

$$(f_{a,b} \circ f_{\frac{1}{a}, -\frac{b}{a}})(x) = a\left(\frac{1}{a}x - \frac{b}{a}\right) + b = x = f_{1,0}(x)$$

Donc  $f_{\frac{1}{a}, -\frac{b}{a}}$  est le symétrique de  $f_{a,b} \in H$ .

Donc  $(H, \circ)$  est un groupe.

(c) Soit  $E = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f(x') \geq f(x), \forall x' \geq x\}$  muni de l'addition de fonctions : si  $f, g \in E$ ,  $(f+g)(x) := f(x) + g(x) \quad \forall x \in \mathbb{R}$ .

Remarquons que si  $(E, +)$  était un groupe, son élément neutre devrait être la fonction  $\ell(x) = 0 \quad \forall x \in \mathbb{R}$ .

Mais alors le symétrique de la fonction  $f(x) = x$  devrait être  $g(x) = -x$ , qui n'est pas croissante. Donc il n'est pas vrai que chaque élément de  $E$  a un symétrique dans  $E$ .

Donc  $(E, +)$  n'est pas un groupe.

**Exercice 9.** On considère le groupe  $\mathbb{Z}$  des entiers relatifs muni de l'addition.

- a) Si  $m \in \mathbb{N}$ , on note  $m\mathbb{Z} = \{mn ; n \in \mathbb{Z}\}$ . Vérifier que  $m\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .  
b) Soit  $G$  un sous-groupe de  $\mathbb{Z}$ . Montrer qu'il existe  $m \in \mathbb{N}$  tel que  $G = m\mathbb{Z}$ .

Indication : Si  $G \neq \{0\}$ , on pourra définir  $m \in \mathbb{N}^*$  comme le plus petit entier naturel non nul contenu dans  $G$ . Pour tout élément  $n$  de  $G$ , on considérera alors le reste de la division euclidienne de  $n$  par  $m$ .

## Solution

(a) Rappelons la définition d'amphi :

Déf : Soit  $(G, *)$  un groupe. Une partie  $H \subset G$  est un sous-groupe de  $G$  si elle possède les propriétés suivantes :

- i)  $e \in H$
- ii)  $\forall a, b \in H \text{ on a } a * b \in H \quad (H \text{ est stable par } *)$
- iii)  $\forall a \in H$ , l'élément symétrique  $a'$  appartient à  $H$ .

Véifions que (i), (ii) et (iii) sont satisfaites quand  $H = m \cdot \mathbb{Z}$ .

(i) On a que l'élément neutre de  $\mathbb{Z}$  pour + est  $e=0$ . Or  $e=m \cdot 0$  pour tout  $m \in \mathbb{N}$ , donc  $e=0 \in m\mathbb{Z} \quad \forall m \in \mathbb{N}$ .

(ii) Soient  $a, b \in m \cdot \mathbb{Z}$ . Alors  $a=m \cdot n$  et  $b=m \cdot n'$  pour  $n, n' \in \mathbb{Z}$ .

Donc  $a+b=m \cdot n+m \cdot n'=m(n+n') \in m \cdot \mathbb{Z}$  car  $n+n' \in \mathbb{Z}$ .

(iii) Si  $a \in m\mathbb{Z}$  et  $a=m \cdot n$ , alors  $-a=m \cdot (-n) \in m\mathbb{Z}$ .

On a donc vérifié que  $m\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ .

(b) Soit  $G$  un sous-groupe de  $\mathbb{Z}$ .

Si  $G=\{0\}$  alors  $G=m\mathbb{Z}$  avec  $m=0$ .

Supposons donc maintenant  $G \neq \{0\}$ .

En suivant l'indication, posons  $m$  égale au plus petit entier naturel non nul contenu dans  $G$ .

Comme  $G$  est un sous-groupe nous avons que  $-m$  est aussi dans  $G$  et que  $m+m+\dots+m \in G$  et aussi  $-m-m-\dots-m \in G$ .

Donc  $m\mathbb{Z} \subseteq G$ . Nous voulons montrer que  $G \subseteq m\mathbb{Z}$ .

Soit  $n \in G$ . Nous pouvons écrire

$n=m \cdot a+b$  où  $a \in \mathbb{Z}$  et  $0 \leq b < m$  est le reste de la division euclidienne de  $n$  par  $m$ .

Comme  $G$  est un sous-groupe,  $n \in G$  et  $-m \cdot a \in G$  (d'après la remarque précédente), alors  $n - m \cdot a = b \in G$

Mais forcément alors  $b=0$  car  $m$  est le plus petit entier  $\geq 1$  contenu dans  $G$  et  $b < m$ .

Donc nous avons montré que  $\forall n \in G, n = m \cdot a$  pour un certain  $a \in \mathbb{Z}$ . Donc  $G \subseteq m\mathbb{Z}$ .

Ceci termine la preuve car  $G \subseteq m\mathbb{Z}$  et  $m\mathbb{Z} \subseteq G$  si et seulement si  $G = m\mathbb{Z}$ .

**Exercice 12.** On considère les éléments suivants du groupe  $S_5$ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}, \quad \varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

- a) Écrire sous la même forme l'élément  $\sigma \circ \varrho$ .
- b) Calculer les puissances successives de l'élément  $\sigma$ , au sens de l'exercice 8, et déterminer le plus petit entier  $m \in \mathbb{N}^*$  tel que  $\sigma^m$  soit la permutation triviale.
- c) Répéter l'opération avec les éléments  $\varrho$  et  $\sigma \circ \varrho$ .

## Solution

(a) Nous avons que

- $\sigma \circ \varrho(1) = \sigma(5) = 1$
- $\sigma \circ \varrho(2) = \sigma(4) = 5$
- $\sigma \circ \varrho(3) = \sigma(1) = 3$
- $\sigma \circ \varrho(4) = \sigma(2) = 4$
- $\sigma \circ \varrho(5) = \sigma(3) = 2$

Donc  $\sigma \circ \varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$

(b) Calculons  $\sigma^n = \underbrace{\sigma \circ \sigma \circ \dots \circ \sigma}_{n \text{ fois}}$  pour tout  $n \in \mathbb{N}$ .

En procédant comme dans (a) nous avons que :

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}, \quad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \text{permutation triviale}$$

Donc le plus petit entier  $m \in \mathbb{N}^*$  tel que  $\sigma^m$  soit la permutation triviale est  $m=5$ .

On a donc  $\sigma^n = \sigma^k$  où  $k \in \{0, 1, 2, 3, 4\}$  est le reste de la division de  $n$  par 5.

$$\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$

(c) · Calculons d'abord les puissances de  $\rho$ .

Nous avons que :

$$\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}, \quad \rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}, \quad \rho^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}. \quad \rho^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \text{permutation triviale.}$$

Donc le plus petit entier  $m \geq 1$  tel que  $\rho^m$  est la permutation triviale est  $m=6$ . De plus  $\rho^m = \rho^k$  où  $k \in \{0, 1, 2, 3, 4, 5\}$  et  $K$  est le reste de la division de  $m$  par 6.

· Calculons maintenant les puissances de  $\sigma \circ \rho$ . Nous avons

$$\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}, \text{ donc } (\sigma \circ \rho)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \text{perm. triviale.}$$

Réu On aurait pu s'attendre à ce résultat, ou que la seule action de  $\sigma \circ \rho$  sur l'ensemble  $\{1, 2, 3, 4, 5\}$  est d'échanger entre eux 2 et 5. Donc en l'appliquant deux fois on "retombe" sur l'ordre de départ.

Dans ce cas donc  $m=2$  et  $\sigma^n = \begin{cases} \sigma & \text{si } n \text{ impair} \\ \text{perm. triviale} & \text{si } n \text{ est pair} \end{cases}$ .

**Exercice 14.** Les applications suivantes sont-elles des morphismes de groupe ?

- a)  $f : x \mapsto 2x$  de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}, +)$ , puis de  $(\mathbb{R}^*, \cdot)$  dans  $(\mathbb{R}^*, \cdot)$ .
- b)  $f : x \mapsto x^2$  de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}, +)$ , puis de  $(\mathbb{R}^*, \cdot)$  dans  $(\mathbb{R}^*, \cdot)$ .
- c)  $f : x \mapsto \ln x$  de  $(\mathbb{R}_+^*, \cdot)$  dans  $(\mathbb{R}, +)$ .
- d)  $f : x \mapsto \exp(x)$  de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}, +)$ .
- e)  $f : x \mapsto \exp(x)$  de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}_+^*, \cdot)$ .
- f)  $f : z \mapsto \bar{z}$  de  $(\mathbb{C}^*, \cdot)$  dans  $(\mathbb{C}^*, \cdot)$ .

Solution Rappelons, avant de procéder, la définition d'un morphisme :

Déf: Soient  $(G, *)$  et  $(\tilde{G}, \times)$  deux groupes. On dit qu'une application  $f: G \rightarrow \tilde{G}$  est un morphisme de groupes si

$$\forall a, b \in G: f(a * b) = f(a) \times f(b).$$

$\uparrow$  loi de  $G$        $\uparrow$  loi de  $\tilde{G}$

Rappelons aussi le résultat suivant :

Proposition: Si  $f: G \rightarrow \tilde{G}$  est un morphisme de groupes, alors

- i)  $f(e) = \tilde{e}$  ( $e$  neutre de  $G$ ,  $\tilde{e}$  neutre de  $\tilde{G}$ )
- ii)  $\forall a \in G: (f(a))' = f(a')$ .  
 $\uparrow$  symétrique       $\uparrow$  symétrique dans  $G$   
dans  $\tilde{G}$ .

Nous pouvons maintenant procéder avec les différentes questions.

(a)  $f: \mathbb{R} \longrightarrow \mathbb{R}$  est un morphisme du groupe  $(\mathbb{R}, +)$  dans  $x \mapsto 2x$  lui-même car

$$\text{si } a, b \in \mathbb{R}, f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$$

Par contre  $f: \mathbb{R}^{\neq} \rightarrow \mathbb{R}^{\neq}$  n'est pas un morphisme du groupe  $(\mathbb{R}^{\neq}, \cdot)$  dans lui-même car

par exemple  $f(3 \cdot 5) = 2 \cdot 15 = 30 \neq f(3) \cdot f(5) = 6 \cdot 10 = 60$ .

Rem Autre, on peut utiliser le point (i) de la proposition et remarquer que si  $f$  était un morphisme de groupes on devrait avoir  $f(1) = 1$ , ce qui n'est pas le cas.

(b)  $f: \mathbb{R} \rightarrow \mathbb{R}$  n'est pas un morphisme de  $(\mathbb{R}, +)$   
 $x \mapsto x^2$  dans lui-même car, par exemple :

$$f(3+2) = f(5) = 5^2 = 25 \neq f(3) + f(2) = 3^2 + 2^2 = 13$$

$f: \mathbb{R} \rightarrow \mathbb{R}$  est un morphisme de  $(\mathbb{R}^*, \cdot)$  dans lui-même, car si  $a, b \in \mathbb{R}^*$  on a que

$$f(a \cdot b) = (ab)^2 = a^2 \cdot b^2 = f(a) \cdot f(b).$$

(c)  $f: \mathbb{R}_+^* \rightarrow \mathbb{R}$  est un morphisme de  $(\mathbb{R}_+^*, \cdot)$   
 $x \mapsto \ln(x)$  dans  $(\mathbb{R}, +)$  car si  $a, b \in \mathbb{R}_+^*$  on a que  $\ln(a \cdot b) = \ln(a) + \ln(b)$

(d)  $f: \mathbb{R} \rightarrow \mathbb{R}$  n'est pas un morphisme de  $(\mathbb{R}, +)$   
 $x \mapsto \exp(x)$  dans lui-même car, par exemple  $f(0) = 1 \neq 0$  qui est l'élément neutre de  $(\mathbb{R}, +)$ .

(e)  $f: \mathbb{R} \rightarrow \mathbb{R}_+^*$  est un morphisme de  $(\mathbb{R}, +)$  dans  $(\mathbb{R}_+^*, \cdot)$  car si  $a, b \in \mathbb{R}$  on a que

$$f(a+b) = \exp(a+b) = \exp(a) \cdot \exp(b).$$

(f)  $f: \mathbb{C}^* \rightarrow \mathbb{C}^*$  est un morphisme du groupe  $(\mathbb{C}^*, \cdot)$   
 $z \mapsto \bar{z}$  dans lui-même car si  $z_1, z_2 \in \mathbb{C}^*$  on a  $f(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2 = f(z_1) \cdot f(z_2)$

### Exercice 16.

- a) Munir l'ensemble  $F_2 = \{0, 1\}$  d'une addition et d'une multiplication de façon que  $F_2$  soit un corps.
- b) Munir l'ensemble  $F_3 = \{-1, 0, 1\}$  d'une addition et d'une multiplication de façon que  $F_3$  soit un corps.
- c) Plus généralement, si  $p \in \mathbb{N}^*$  est un entier premier, montrer qu'il existe un corps  $F_p$  possédant exactement  $p$  éléments.

Solution Rappelons les définitions d'après suivantes :

Déf: On appelle anneau un ensemble  $A$  muni de deux lois de composition internes, notées  $+$  et  $\cdot$ , telles que :

- i)  $(A, +)$  est un groupe abélien, dont l'élément neutre est noté  $0$  ;
- ii) La loi  $\cdot$  est associative et possède un élément neutre, noté  $1$  ;
- iii) La loi  $\cdot$  est distributive par rapport à la loi  $+$  :  $\forall a, b, c \in A$  on a  $a \cdot (b+c) = a \cdot b + a \cdot c$ , et  $(b+c) \cdot a = b \cdot a + c \cdot a$ .

On dit que l'anneau est commutatif si, de plus, la loi  $\cdot$  est commutative.

Déf: Soit  $(A, +, \cdot)$  un anneau. On dit qu'un élément  $a \in A$  est inversible s'il existe un élément  $b \in A$  t.q.  $a \cdot b = b \cdot a = 1$ .  
On dit que  $b$  est l'inverse de  $a$ , et on note  $b = a^{-1}$ .

Déf: Un anneau commutatif  $(A, +, \cdot)$  est appelé un corps si  $A \neq \{0\}$  et si tout élément de  $A \setminus \{0\}$  est inversible.

On a aussi :

Proposition: Si  $(A, +, \cdot)$  corps  $\Rightarrow 1_A + 0_A$ .

B Supposons  $1_A = 0_A$ . Alors t.a=t on aurait :

$$a = a \cdot 1_A = a \cdot 0_A = a(0_A + 0_A) = a(1_A + 1_A) = a + a$$

Donc si  $a'$  est le symétrique de  $a$  pour la loi  $+$ :  $a' + a = a' + a + a$

Donc  $0_A = a$  t.a=t. Absurd, car  $A \neq \{0_A\}$ .  $\square$

(a) Définition de la loi + sur  $F_2 = \{0, 1\}$

Soit  $F_2 = \{0, 1\}$ . Comme  $F_2$  a deux éléments on a montré dans l'exercice 1, point (c), qu'il y a une seule façon (à moins d'échanger les deux éléments entre eux) de munir  $F_2$  d'une loi "+" qui le rend un groupe abélien.

Il s'agit de la loi définie par :  $0+0=0$ ,  $0+1=1+0=1$ ,  $1+1=0$ . avec 0 comme élément neutre.

Définition de la loi  $\circ$  sur  $F_2 = \{0, 1\}$

Définissons maintenant la loi interne  $\circ$ . Soit  $1_{F_2}$  l'élément neutre pour cette loi, c.i.d.  $a \cdot 1_F = 1_F \cdot a = a$  pour tout  $a \in F_2$ .

- D'après la Proposition on a  $1_{F_2} \neq 0$ . Donc  $1_{F_2} = 1$ .

Ceci implique  $1 \cdot 0 = 0$ ,  $0 \cdot 1 = 0$ ,  $1 \cdot 1 = 1$

De plus  $0 \cdot 0 = 0 \cdot (1+1) = (\text{la loi est distributive}) = 0 \cdot 1 + 0 \cdot 1 = 0 + 0 = 0$

- Avec les lois + et  $\circ$  ainsi définies,  $(F_2, +, \circ)$  est un corps. (on pourra vérifier que  $\circ$  est distributive sur +).

(b) Définissons sur  $F_3 = \{0, 1, -1\}$  les lois + et  $\circ$ .

- Définition de +: On doit avoir que  $(F_3, +)$  est un groupe abélien. Supposons que  $0_{F_3} = 0$  soit l'élément neutre de + Alors on a la table de groupe

	0	1	-1
0	0	1	-1
1	1		
-1	-1		

Chaque élément doit avoir une symétrie. Donc

Il existe  $a \in F_3$  tel que

$$a+1 = 1+a = 0$$

- Si  $a=1$  on obtient que  $-1+1+a = -1+1+1 = 0$

- (i) Supposons que  $1+1=1$ . Si  $b$  symétrique de  $1$ , alors on a  
 $b+1+1=b+1 \Rightarrow 1=0$  ce qui est absurde.
- (ii) Supposons que  $1+1=0 \Rightarrow 1$  est le symétrique de  $1$  et, par unicité du symétrique,  $-1$  est le symétrique de  $-1$ .  
 Donc  $1+(-1)\neq 0$ , ce qui implique  $1+(-1)\in\{1,-1\}$ .
- \* Si  $1+(-1)=1 \Rightarrow 1+(1+(-1))=1+1 \Rightarrow -1=0$ : Absurde
  - \* Si  $1+(-1)=-1 \Rightarrow (1+(-1))+(-1)=-1+(-1) \Rightarrow 1=0$ : Abs.
  - Donc si  $1+1\in\{0,1\}$  on trouve un absurd  $\Rightarrow 1+1=-1$ .
  - De la même façon on peut montrer que  $-1+(-1)=1$
  - On a aussi montré dans (ii) que le symétrique de  $1$  doit être  $-1$  et vice versa.

La table du groupe abélien  $(F_3, +)$  est donc

	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

- Définition de  $\cdot$  : Rappelons que  $\cdot$  doit être associative, avoir un élément neutre et être distributive par rapport à  $+$ .  
 Commençons par l'élément neutre,  $1_{F_3}$ .  
 Clairement  $1_{F_3}\neq 0_{F_3}$  (d'après la Proposition).  
 On peut donc supposer  $1_{F_3}=1$  (à moins d'échanger les rôles de  $1$  et  $-1$ ). Nous avons donc
- $0=0\cdot 1=0$ ,  $1\cdot 1=1$ ,  $1\cdot -1=-1\cdot 1=-1$ .

Comme la loi est distributive nous avons aussi :

$$0\cdot -1 = (1+1+1)\cdot -1 = -1 + (-1) + (-1) = 0 = -1\cdot 0$$

$$0\cdot 0 = (1+1+1)\cdot 0 = 0$$

$$-1\cdot -1 = -1\cdot (1+1) = -1 + (-1) = 1.$$

On a la table suivante :

•	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

On pourra vérifier que les axiomes de corps sont satisfaits, c.à.d. que la loi  $\cdot$  définie est associative, à 1 comme élément neutre, que chaque élément de  $F_3 \setminus \{0\}$  a un inverse et que la loi  $\cdot$  est distributive sur  $+$ .

(c) Soit  $p$  un nombre premier.

- On considère l'ensemble  $F_p = \mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, \dots, [p-1]_p\}$
- Pour un entier  $x \in \mathbb{Z}$ , on définit  $[x]_p := [r]_p \in F_p$  si  $r \in \{0, 1, \dots, p-1\}$  est le reste de la division de  $x$  par  $p$ .
- On définit une addition  $\oplus$  et une multiplication  $*$  sur  $F_p$

$$[a]_p \oplus [b]_p = [a+b]_p \quad (\text{le } + \text{ est dans } \mathbb{Z})$$

$$[a]_p * [b]_p = [a \cdot b]_p \quad (\text{le } \cdot \text{ est dans } \mathbb{Z})$$

Ces deux lois sont clairement internes.

- Vérifions que  $(F_p, \oplus, *)$  est un anneau commutatif.

(i)  $(F_p, \oplus)$  est un groupe abélien

- La loi  $\oplus$  est clairement commutative (car la somme est commutative dans  $\mathbb{Z}$ ). L'élément neutre est  $[0]_p$  car  $\forall [a]_p \in F_p$  on a  $[a]_p \oplus [0]_p = [a+0]_p = [a]_p = [0]_p \oplus [a]_p$ .

- La loi  $\oplus$  est aussi associative car

$$([a]_p \oplus [b]_p) \oplus [c]_p = [a+b]_p \oplus [c]_p = [a+b+c]_p = ([a]_p \oplus [b+c]_p) \oplus [c]_p$$

$\begin{matrix} (+ \text{ est} \\ \text{associatif}) \\ \text{sur } \mathbb{Z} \end{matrix}$

Donc on a montré que  $(\mathbb{F}_p, \star)$  est un groupe abélien.

(ii) la loi  $\star$  est associative car

$$\begin{aligned} ([a]_p \star [b]_p) \star [c]_p &= [ab]_p \star [c]_p = [(ab) \cdot c]_p = \stackrel{\text{est}}{\underset{\text{associative}}{}} \\ &= [a(bc)]_p = [a]_p \star [bc]_p = \quad \text{dans } \mathbb{Z} \\ &\stackrel{1}{=} [a]_p \star ([b]_p \star [c]_p) \end{aligned}$$

L'élément neutre de  $\star$  est  $[1]_p$  car

$$[a]_p \star [1]_p = [a \cdot 1]_p = [a]_p \text{ pour tout } [a]_p \in \mathbb{F}_p.$$

(iii) La loi  $\star$  est distributive par rapport à  $\oplus$ :

$$\begin{aligned} [a]_p \star ([b]_p \oplus [c]_p) &= [a]_p \star ([b+c]_p) = \\ &= [a(b+c)]_p = \left( \begin{array}{l} \text{la loi } \star \text{ est distributive} \\ \text{par rapport à } + \text{ sur } \mathbb{Z} \end{array} \right) = \\ &= [ab+ac]_p = [ab]_p \oplus [ac]_p = [a]_p \star [b]_p \oplus [a]_p \star [c]_p \end{aligned}$$

Pour montrer que  $\mathbb{F}_p$  est un corps il nous reste à prouver que tous les éléments différents de  $[0]_p$  ont un inverse pour  $\star$ . Soit  $[a]_p \in \mathbb{F}_p$ ,  $[a]_p \neq [0]_p$ . c.à.d.  $a \in \{1, \dots, p-1\}$ .

Comme  $p$  est un nombre premier,  $\text{Pgcd}(a, p) = 1$

Par le théorème de Bézout, il existe  $x, y \in \mathbb{Z}$  tels que  $x \cdot a + y \cdot p = 1$ . Donc

$$\begin{aligned} [x a + y p]_p &= [1]_p = [x a]_p + [y p]_p = [x a]_p + [0]_p \\ &= [x]_p \star [a]_p \Rightarrow [x]_p \text{ est l'inverse de } [a]_p. \end{aligned}$$