

## 1 Groupes et sous-groupes

### Exercice 1 ★★ Un exemple de groupes –

On définit, pour  $(x, y)$  et  $(x', y')$  dans  $\mathbb{R}^* \times \mathbb{R}$ ,

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

1. Démontrer que  $(\mathbb{R}^* \times \mathbb{R}, \star)$  est un groupe. Est-il commutatif ?
2. Simplifier  $(x, y)^n$  pour tout  $(x, y) \in \mathbb{R}^* \times \mathbb{R}$  et tout  $n \in \mathbb{N}^*$ .

[Indication ▼](#) [Correction ▼](#)

[3213]

### Exercice 2 ★★★ Quelques sous-groupes usuels –

Soit  $(G, \cdot)$  un groupe. Démontrer que les parties suivantes sont des sous-groupes de  $G$  :

1.  $C(G) = \{x \in G; \forall y \in G, xy = yx\}$  ( $C(G)$  s'appelle le centre de  $G$ ) ;
2.  $aHa^{-1} = \{aha^{-1}; h \in H\}$  où  $a \in G$  et  $H$  est un sous-groupe de  $G$ .
3. On suppose de plus que  $G$  est commutatif. On dit que  $x$  est un élément de torsion de  $G$  s'il existe  $n \in \mathbb{N}^*$  tel que  $x^n = e$ . Démontrer que l'ensemble des éléments de torsion de  $G$  est un sous-groupe de  $G$ .

[Indication ▼](#) [Correction ▼](#)

[1302]

### Exercice 3 ★★★ Inversibles à coefficients dans $\mathbb{Z}$ . –

On note  $GL_n(\mathbb{Z})$  l'ensemble des matrices de  $\mathcal{M}_n(\mathbb{R})$ , à coefficients dans  $\mathbb{Z}$ , qui sont inversibles et dont l'inverse est à coefficients dans  $\mathbb{Z}$ .

1. Démontrer que si  $M$  est à coefficients dans  $\mathbb{Z}$ , alors  $M \in GL_n(\mathbb{Z})$  si et seulement si  $\det(M) = \pm 1$ .
2. En déduire que  $GL_n(\mathbb{Z})$  est un sous-groupe de  $GL_n(\mathbb{R})$ .

[Indication ▼](#) [Correction ▼](#)

[1303]

### Exercice 4 ★★★★★ Sous-groupe engendré par le complémentaire d'un sous-groupe –

Soit  $H$  un sous-groupe strict d'un groupe  $(G, \cdot)$ . Déterminer le sous-groupe engendré par le complémentaire de  $H$ .

[Indication ▼](#) [Correction ▼](#)

[1308]

### Exercice 5 ★★★★★ Théorème de Lagrange –

Soit  $(G, \cdot)$  un groupe fini et  $H$  un sous-groupe de  $G$ .

1. Montrer que pour tout  $a \in G$ ,  $H$  et  $aH = \{ah; h \in H\}$  ont le même nombre d'éléments.
2. Soient  $a, b \in G$ . Démontrer que  $aH = bH$  ou  $aH \cap bH = \emptyset$ .
3. En déduire que le cardinal de  $H$  divise le cardinal de  $G$ .

[Indication ▼](#) [Correction ▼](#)

[1309]

### Exercice 6 ★★★★★ Produit de deux sous-groupes –

Soit  $(G, \cdot)$  un groupe et  $A, B$  deux sous-groupes de  $G$ . On note  $AB = \{ab; a \in A, b \in B\}$ . Montrer que  $AB$  est un sous-groupe de  $G$  si et seulement si  $AB = BA$ .

[Indication ▼](#) [Correction ▼](#)

[1307]

## 2 Morphismes de groupe

### Exercice 7 ★ Exemples ou contre-exemples de morphismes de groupes –

Les applications  $\phi : G \rightarrow H$  définies ci-dessous sont-elles des morphismes de groupes ?

1.  $G = (GL_n(\mathbb{R}), \times)$ ,  $H = (\mathbb{R}, +)$ ,  $\phi(A) = \text{tr}(A)$ .
2.  $G = (M_n(\mathbb{R}), +)$ ,  $H = (\mathbb{R}, +)$ ,  $\phi(A) = \text{tr}(A)$ .
3.  $G = (\mathbb{R}^*, \times)$ ,  $H = (\mathbb{R}^*, \times)$ ,  $\phi(x) = |x|$ .
4.  $G = (\mathbb{R}^*, \times)$ ,  $H = (\mathbb{R}^*, \times)$ ,  $\phi(x) = 2x$ .
5.  $G = (\mathbb{R}, +)$ ,  $H = (GL_2(\mathbb{R}), \times)$ ,  $\phi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ .

[Indication ▼](#) [Correction ▼](#)

[2580]

### Exercice 8 ★★★★★ Automorphisme intérieur –

Soit  $(G, \cdot)$  un groupe. Pour  $a \in G$ , on note  $\tau_a : G \rightarrow G$  défini par  $\tau_a(x) = axa^{-1}$ .

1. Démontrer que  $\tau_a$  est un endomorphisme de  $G$ .
2. Vérifier que, pour tous  $a, b \in G$ ,  $\tau_a \circ \tau_b = \tau_{ab}$ .
3. Montrer que  $\tau_a$  est bijective et déterminer son inverse.
4. En déduire que  $\Theta = \{\tau_a; a \in G\}$  muni du produit de composition est un groupe.

[Indication ▼](#) [Correction ▼](#)

[1314]

### Exercice 9 ★★★★★ Somme des valeurs –

Soit  $f$  un morphisme non constant d'un groupe fini  $(G, \cdot)$  dans  $(\mathbb{C}^*, \cdot)$ . Calculer  $\sum_{x \in G} f(x)$ .

[Indication ▼](#) [Correction ▼](#)

[1315]

### Exercice 10 ★★ Morphismes de $\mathbb{Z}$ dans $\mathbb{Z}$ –

Déterminer tous les morphismes de  $(\mathbb{Z}, +)$  dans lui-même. Lesquels sont injectifs ? surjectifs ?

[Indication ▼](#) [Correction ▼](#)

[1311]

### Exercice 11 ★★ Morphismes que $(\mathbb{Q} - -$

Déterminer tous les morphismes de groupes de  $(\mathbb{Q}, +)$  dans  $(\mathbb{Z}, +)$ .

[Indication ▼](#) [Correction ▼](#)

[2638]

### Exercice 12 ★★ Morphisme entre groupes de torsion et groupes sans torsion –

Dans un groupe  $(G, \cdot)$ , un élément  $x$  est dit de torsion s'il existe  $n \geq 1$  tel que  $x^n = e$ . On dit que  $G$  est de torsion si tous ses éléments sont de torsion. On dit que  $G$  est sans torsion si son seul élément de torsion est l'élément neutre. Soit  $G_1$  un groupe de torsion et  $G_2$  un groupe sans torsion. Déterminer tous les morphismes de groupe de  $G_1$  dans  $G_2$ .

[Indication ▼](#) [Correction ▼](#)

[2640]

### Exercice 13 ★★★★★ Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ –

1. Déterminer tous les morphismes de  $\mathbb{Z}/3\mathbb{Z}$  dans  $\mathbb{Z}/4\mathbb{Z}$ .
2. Déterminer tous les morphismes de  $\mathbb{Z}/6\mathbb{Z}$  dans  $\mathbb{Z}/8\mathbb{Z}$ .

[Indication ▼](#) [Correction ▼](#)

[1321]

## 3 Ordre d'un élément, groupes cycliques

### Exercice 14 ★ Pour commencer... –

Quel est l'ordre de  $\bar{9}$  dans  $(\mathbb{Z}/12\mathbb{Z}, +)$  ?

[Indication ▼](#) [Correction ▼](#)

[1324]

---

**Exercice 15** ★★ **Ordre du carré –**

Soit  $G$  un groupe (noté multiplicativement) et  $x \in G$  d'ordre  $n$ . Quel est l'ordre de  $x^2$  ?

[Indication ▼](#) [Correction ▼](#)

[1325]

---

**Exercice 16** ★★ **Tous les éléments sont d'ordre deux –**

Soit  $G$  un groupe dont tous les éléments (sauf l'élément neutre) sont d'ordre au plus deux. Démontrer que  $G$  est abélien.

[Indication ▼](#) [Correction ▼](#)

[1327]

---

**Exercice 17** ★★ **Un groupe infini dont tous les éléments sont d'ordre fini –**

Soit  $G = [0, 1[ \cap \mathbb{Q}$ . On munit  $G$  de la loi de composition interne suivante : pour  $x, y \in G$ ,

$$x \star y = \begin{cases} x + y & \text{si } x + y < 1 \\ x + y - 1 & \text{si } x + y \geq 1. \end{cases}$$

1. Démontrer que  $(G, \star)$  est un groupe commutatif.
2. Démontrer que tous les éléments de  $G$  sont d'ordre fini.

[Indication ▼](#) [Correction ▼](#)

[3327]

---

**Exercice 18** ★★ **Groupe admettant un nombre fini de sous-groupes –**

Soit  $G$  un groupe admettant un nombre fini de sous-groupes.

1. Démontrer que tout élément de  $G$  est d'ordre fini.
2. En déduire que  $G$  est fini.

[Indication ▼](#) [Correction ▼](#)

[2637]

---

**Exercice 19** ★★ **Groupes d'ordre 4 –**

Soit  $G$  un groupe d'ordre 4. Démontrer que  $G$  est isomorphe ou à  $\mathbb{Z}/4\mathbb{Z}$ , ou à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

[Indication ▼](#) [Correction ▼](#)

[3330]

---

**Exercice 20** ★★★ **Sous-groupes de  $(\mathbb{Z}/20\mathbb{Z})^*$  –**

Soit  $G = (\mathbb{Z}/20\mathbb{Z})^*$  le groupe des éléments inversibles de  $\mathbb{Z}/20\mathbb{Z}$ .

1. Donner la liste de tous les éléments de  $G$ .
2. Pour tout  $a \in G$ , déterminer le sous groupe  $\langle a \rangle$  engendré par  $a$ .
3. Déterminer un ensemble minimal de générateurs de  $(G, \cdot)$ .
4.  $(G, \cdot)$  est-il un groupe cyclique ?
5. Déterminer tous les sous-groupes de  $G$  et, pour chaque sous-groupe, préciser un ensemble de générateurs.
6. Parmi les sous-groupes de  $(G, \cdot)$ , lesquels sont isomorphes à un groupe additif  $(\mathbb{Z}/m\mathbb{Z}, +)$  ?

[Indication ▼](#) [Correction ▼](#)

[2193]

---

**Exercice 21** ★★★ **Groupe de cardinal pair –**

Soit  $G$  un groupe de cardinal  $2n$ .

1. Démontrer que la relation  $\mathcal{R}$  définie sur  $G$  par

$$x \mathcal{R} y \iff x = y \text{ ou } x = y^{-1}$$

est une relation d'équivalence sur  $G$ .

## 2. En déduire que $G$ admet des éléments d'ordre deux.

[Indication ▼](#) [Correction ▼](#)

[1328]

### Exercice 22 ★★★★★ Ordre du produit de deux éléments –

Soit  $G$  un groupe abélien,  $x$  et  $y$  deux éléments de  $G$  d'ordres respectifs  $p$  et  $q$ .

1. On suppose que  $p$  et  $q$  sont premiers entre eux. Démontrer que  $xy$  est d'ordre  $pq$ .

2. Importance des hypothèses - 1 : Si  $H = GL_2(\mathbb{R})$ ,  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ , vérifier que  $A$  et  $B$  sont d'ordre fini, mais que  $AB$  n'est pas d'ordre fini.

3. Importance des hypothèses - 2 : Si  $p$  et  $q$  ne sont pas supposés premiers entre eux, démontrer que le produit  $xy$  n'est pas nécessairement d'ordre  $pq$ , ou d'ordre  $\text{ppcm}(p, q)$ .

4. Une application :

Soit  $d$  un diviseur de  $p$ . Démontrer qu'il existe un élément d'ordre  $d$  dans  $G$ . En déduire que  $G$  admet des éléments d'ordre  $\text{ppcm}(p, q)$ . On suppose de plus que  $G$  est fini. Démontrer que  $G$  admet un élément dont l'ordre est le  $\text{ppcm}$  de l'ordre des éléments de  $G$ .

5. Soit  $d$  un diviseur de  $p$ . Démontrer qu'il existe un élément d'ordre  $d$  dans  $G$ .

6. En déduire que  $G$  admet des éléments d'ordre  $\text{ppcm}(p, q)$ .

7. On suppose de plus que  $G$  est fini. Démontrer que  $G$  admet un élément dont l'ordre est le  $\text{ppcm}$  de l'ordre des éléments de  $G$ .

[Indication ▼](#) [Correction ▼](#)

[1326]

### Exercice 23 ★★★★★ Produit de groupes cycliques –

Soient  $G$  et  $H$  deux groupes.

1. Montrer que si  $g$  est un élément d'ordre  $p$  de  $G$  et  $h$  un élément d'ordre  $q$  de  $H$ , alors  $(g, h)$  est d'ordre  $\text{ppcm}(p, q)$  dans  $G \times H$ .

2. On suppose que  $G$  et  $H$  sont cycliques. Démontrer que  $G \times H$  est cyclique si et seulement si les ordres de  $G$  et  $H$  sont premiers entre eux.

[Indication ▼](#) [Correction ▼](#)

[1329]

### Exercice 24 ★★★★★ Sous-groupe d'un groupe cyclique –

Soit  $G$  un groupe cyclique et soit  $H$  un sous-groupe de  $G$ . Démontrer que  $H$  est cyclique.

[Indication ▼](#) [Correction ▼](#)

[1330]

---

**Indication pour l'exercice 1 ▲**

1. Il faut vérifier les trois propriétés de la définition d'un groupe.
  2. Calculer ce que cela vaut pour  $n = 2, n = 3$ , puis faire une récurrence.
- 

**Indication pour l'exercice 2 ▲**

Appliquer le théorème de caractérisation des sous-groupes.

---

**Indication pour l'exercice 3 ▲**

1. Utiliser les formules de Cramer.
  2. Utiliser la caractérisation des sous-groupes. On utilisera dans l'exercice  $\det(A^{-1}) = \dots$  et  $\det(AB) = \dots$
- 

**Indication pour l'exercice 4 ▲**

Démontrer que  $H$  est inclus dans ce sous-groupe. On pourra utiliser un élément  $a \in H^c$ .

---

**Indication pour l'exercice 5 ▲**

1. Construire une bijection.
  - 2.
  3. Réaliser une partition de  $G$ .
- 

**Indication pour l'exercice 6 ▲**

Pour montrer que  $AB$  sous-groupe entraîne  $AB = BA$ , on pourra utiliser la stabilité par  $x^{-1}$ .

---

**Indication pour l'exercice 7 ▲**

Revenir à la définition !

---

**Indication pour l'exercice 8 ▲**

1. Vérifier la définition.
  - 2.
  3. Utiliser la question précédente avec  $b = a^{-1}$ .
  4. Démontrer qu'il s'agit d'un sous-groupe de  $(S_G, \circ)$ .
- 

**Indication pour l'exercice 9 ▲**

Partir de  $a \in G$  tel que  $f(a) \neq 1$  et calculer  $\sum_{x \in G} f(ax)$ .

---

**Indication pour l'exercice 10 ▲**

Il suffit de connaître l'image de 1.

---

**Indication pour l'exercice 11 ▲**

Démontrer et utiliser que si  $f$  est un tel morphisme et  $p$  et  $q$  sont des entiers naturels,  $f(p) = pf(1)$  et  $f\left(\frac{1}{q}\right) = \frac{1}{q}f(1)$ .

---

**Indication pour l'exercice 12 ▲**

Seul le morphisme qui à  $x$  associe l'élément neutre de  $G_2$  convient.

---

**Indication pour l'exercice 13 ▲**

---

Dans les deux cas, un morphisme est complètement déterminé par l'image de  $\bar{1}$ . Quelles sont ces images possibles ? (penser à des raisonnements en terme d'ordre...)

---

Indication pour l'exercice 14 ▲

Il suffit de calculer les multiples successifs de  $\bar{9}$ ...

---

Indication pour l'exercice 15 ▲

Distinguer les cas  $n$  est pair et  $n$  est impair.

---

Indication pour l'exercice 16 ▲

Comparer  $x^2y^2$  et  $(xy)^2$ .

---

Indication pour l'exercice 17 ▲

1. Il faut vérifier l'associativité, l'existence d'un élément neutre et
  2. On pourra remarquer que  $x^{*n} = nx - \lfloor nx \rfloor$ .
- 

Indication pour l'exercice 18 ▲

1. Si un élément n'est pas d'ordre fini, le sous-groupe engendré par cet élément est isomorphe à  $(\mathbb{Z}, +)$ .
  2. Remarquer que  $G$  est la réunion des sous-groupes engendrés par ses éléments.
- 

Indication pour l'exercice 19 ▲

Si  $G$  n'est pas isomorphe à  $\mathbb{Z}/4\mathbb{Z}$ , alors tous les éléments de  $G$  différents de l'élément neutre sont d'ordre 2. On pourra alors établir la table de multiplication de  $G$  et observer qu'elle correspond à celle de  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

---

Indication pour l'exercice 20 ▲

1. Il y a un critère...
  2. Prendre un élément et toutes ses puissances, jusqu'à tomber sur 1.
  - 3.
  4. La question 2. donne la réponse !
  5. Quels sont les sous-groupes engendrés par deux éléments d'ordre 2 ?
  - 6.
- 

Indication pour l'exercice 21 ▲

1. Appliquer la définition !
  2. Quel est le cardinal d'une classe d'équivalence ?
- 

Indication pour l'exercice 22 ▲

1. Remarquer que  $(xy)^q = e$ , puis que si  $d$  est l'ordre de  $xy$ , alors  $p|d$ ...
2. Calculer  $A^4, B^3$  et  $(AB)^n$ .
3. Penser à un élément et à son inverse.
4. Une application :  
Considérer une puissance de  $x$  bien choisie. Décomposer  $p$  et  $q$  en facteurs premiers, calculer le ppcm en fonction de cette décomposition, utiliser la question précédente et la première. Par récurrence d'après la question précédente.
5. Considérer une puissance de  $x$  bien choisie.

6. Décomposer  $p$  et  $q$  en facteurs premiers, calculer le ppcm en fonction de cette décomposition, utiliser la question précédente et la première.

7. Par récurrence d'après la question précédente.

---

Indication pour l'exercice 23 ▲

---

1. Calculer  $(g, h)^n \dots$

2. Prendre un générateur de  $G$  et un générateur de  $H$  et les accoupler... Réciproquement, si  $(x, y)$  est un générateur de  $G \times H$ ,  $x$  est générateur de  $G$  donc d'ordre...

---

Indication pour l'exercice 24 ▲

---

Soit  $a$  un générateur de  $G$  et  $n$  le plus petit entier supérieur ou égal à 1 tel que  $a^n \in H$ . Démontrer que  $H$  est engendré par  $a^n$ . On pourra utiliser la division euclidienne.

---

## Correction de l'exercice 1 ▲

**1. On n'a pas affaire à une loi "classique" et donc on ne peut pas démontrer qu'on a un sous-groupe d'un groupe connu. Il faut donc vérifier à la main les trois propriétés d'un groupe ainsi que le fait qu'il s'agit bien d'une loi interne.**

**Si  $(x, y)$  et  $(x', y')$  sont dans  $\mathbb{R}^* \times \mathbb{R}$ , alors  $xx' \in \mathbb{R}^*$  et  $xy' + y \in \mathbb{R}$  et donc il s'agit bien d'une loi interne. La loi  $\star$  est associative : en effet, si  $(x, y)$ ,  $(x', y')$  et  $(x'', y'')$  sont dans  $\mathbb{R}^* \times \mathbb{R}$ , alors d'une part**

$$\begin{aligned}((x, y) \star (x', y')) \star (x'', y'') &= (xx', xy' + y) \star (x'', y'') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

**et d'autre part**

$$\begin{aligned}(x, y) \star ((x', y') \star (x'', y'')) &= (x, y) \star (x'x'', x'y'' + y') \\ &= (xx'x'', x(x'y'' + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y).\end{aligned}$$

**La loi possède un élément neutre, qui est  $(1, 0)$ . Il est en effet facile de vérifier que**

$$(x, y) \star (1, 0) = (1, 0) \star (x, y) = (x, y).$$

**Tout élément  $(x, y)$  possède un inverse. Expliquons comment le trouver. Il n'est pas très difficile de remarquer qu'il doit s'écrire sous la forme  $(1/x, a)$ . De**

$$(x, y) \star (1/x, a) = (1, xa + y)$$

**on voit qu'on doit avoir  $xa + y = 0$  et donc  $a = -y/x$ . On vérifie alors que  $(1/x, -y/x)$  est un inverse de  $(x, y)$  :**

$$(x, y) \star (1/x, -y/x) = (1/x, -y/x) \star (x, y) = (1, 0).$$

**Le groupe n'est pas commutatif. En effet on a**

$$(1, 1) \star (2, 1) = (2, 2)$$

**alors que**

$$(2, 1) \star (1, 1) = (2, 3).$$

**2. Si  $(x, y)$  et  $(x', y')$  sont dans  $\mathbb{R}^* \times \mathbb{R}$ , alors  $xx' \in \mathbb{R}^*$  et  $xy' + y \in \mathbb{R}$  et donc il s'agit bien d'une loi interne.**

**3. La loi  $\star$  est associative : en effet, si  $(x, y)$ ,  $(x', y')$  et  $(x'', y'')$  sont dans  $\mathbb{R}^* \times \mathbb{R}$ , alors d'une part**

$$\begin{aligned}((x, y) \star (x', y')) \star (x'', y'') &= (xx', xy' + y) \star (x'', y'') \\ &= (xx'x'', xx'y'' + xy' + y)\end{aligned}$$

**et d'autre part**

$$\begin{aligned}(x, y) \star ((x', y') \star (x'', y'')) &= (x, y) \star (x'x'', x'y'' + y') \\ &= (xx'x'', x(x'y'' + y') + y) \\ &= (xx'x'', xx'y'' + xy' + y).\end{aligned}$$

**4. La loi possède un élément neutre, qui est  $(1, 0)$ . Il est en effet facile de vérifier que**

$$(x, y) \star (1, 0) = (1, 0) \star (x, y) = (x, y).$$

**5. Tout élément  $(x, y)$  possède un inverse. Expliquons comment le trouver. Il n'est pas très difficile de remarquer qu'il doit s'écrire sous la forme  $(1/x, a)$ . De**

$$(x, y) \star (1/x, a) = (1, xa + y)$$



on voit qu'on doit avoir  $xa + y = 0$  et donc  $a = -y/x$ . On vérifie alors que  $(1/x, -y/x)$  est un inverse de  $(x, y)$  :

$$(x, y) \star (1/x, -y/x) = (1/x, -y/x) \star (x, y) = (1, 0).$$

6. On remarque que

$$(x, y)^2 = (x^2, xy + y) \text{ et } (x, y)^3 = (x^3, x^2y + xy + y).$$

On prouve alors par récurrence sur  $n \in \mathbb{N}^*$  que

$$(x, y)^n = (x^n, x^{n-1}y + x^{n-2}y + \cdots + xy + y).$$

### Correction de l'exercice 2 ▲

Il suffit, pour chaque cas, d'appliquer le théorème de caractérisation des sous-groupes.

1.  $e$  est élément de  $C(G)$  car  $ey = ye = y$  pour tout  $y \in G$ . Soient  $x_1, x_2 \in C(G)$ . Alors, pour tout  $y \in G$ , on a

$$x_1x_2y = x_1(x_2y) = (x_1y)x_2 = yx_1x_2$$

et donc  $x_1x_2 \in C(G)$ . Enfin, si  $x \in C(G)$ , alors pour tout  $y \in G$ ,

$$xy = yx \implies xyx^{-1} = yxx^{-1} = y \implies x^{-1}xyx^{-1} = x^{-1}y \implies yx^{-1} = x^{-1}y$$

où on a multiplié à droite puis à gauche par  $x^{-1}$ . On en déduit que  $x^{-1} \in C(G)$  qui est donc un sous-groupe de  $G$ .

2. Puisque  $H$  est un sous-groupe de  $G$ ,  $e \in H$  et donc  $aea^{-1} \in aHa^{-1}$ . Mais  $aea^{-1} = e$  et donc  $e \in aHa^{-1}$ . Soient  $x = aha^{-1}$  et  $y = ah'a^{-1}$  deux éléments de  $aHa^{-1}$  avec donc  $h, h' \in H$ . On a

$$xy = aha^{-1}ah'a^{-1} = ah'h'a^{-1} \in aHa^{-1}$$

puisque  $hh' \in H$  ( $H$  est un sous-groupe de  $G$ ). Enfin, si on choisit  $h' = h^{-1}$ , le calcul précédent montre que

$$xy = yx = e$$

et donc  $x^{-1} = y \in aHa^{-1}$  puisque  $h^{-1} \in H$ .  $aHa^{-1}$  est donc bien un sous-groupe de  $G$ .

3. Notons  $T$  l'ensemble des éléments de torsion de  $G$ . On a  $e^1 = e$ , donc  $e \in T$ . De plus, si  $x, y \in T$ , avec respectivement  $x^n = e$  et  $y^m = e$ , il suffit de remarquer que

$$(y^{-1})^m = (y^m)^{-1} = e^{-1} = e$$

puis d'utiliser le fait que  $x$  et  $y^{-1}$  commutent pour prouver que

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

Ainsi,  $xy^{-1}$  est élément de  $T$ , et  $T$  est bien un sous-groupe de  $G$ .

### Correction de l'exercice 3 ▲

1. Prenons d'abord  $M \in GL_n(\mathbb{Z})$ . Alors on a

$$\det(M) \times \det(M^{-1}) = \det(MM^{-1}) = \det(I_n) = 1$$

et de plus  $\det(M)$  et  $\det(M^{-1})$  sont des éléments de  $\mathbb{Z}$ . Ceci n'est possible que si  $\det(M)$  et  $\det(M^{-1})$  sont égaux à 1 ou  $-1$ . Réciproquement, si  $\det(M) = \pm 1$ , alors les formules de Cramer nous disent que

$$M^{-1} = \frac{1}{\det M} (\text{comat } M)^T.$$

La comatrice d'une matrice à coefficients dans  $\mathbb{Z}$  étant à coefficients dans  $\mathbb{Z}$  et  $\det(M)$  valant  $\pm 1$ , on a bien que  $M^{-1}$  est une matrice à coefficients entiers.

**2. On remarque d'abord que  $I_n \in GL_n(\mathbb{Z})$ . Ensuite, si  $A, B \in GL_n(\mathbb{Z})$ , des formules**

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

et

$$\det(AB) = \det(A) \det(B)$$

on déduit facilement que  $\det(A^{-1})$  et  $\det(AB)$  sont éléments de  $\{-1, 1\}$  et donc  $A^{-1}, AB$  sont éléments de  $GL_n(\mathbb{Z})$ .

---

#### Correction de l'exercice 4 ▲

Notons  $K$  le complémentaire de  $H$  et fixons  $a$  un élément de  $K$  (rappelons que  $H$  est strictement inclus dans  $G$ ). Nous allons prouver que le sous-groupe engendré par  $K$ , que nous allons noter  $L$ , est égal à  $G$  tout entier. Puisque ce sous-groupe contient déjà  $K$ , il suffit de prouver qu'il contient également son complémentaire, à savoir  $H$ . Soit donc  $x \in H$ . Alors  $ax$  ne peut pas être un élément de  $H$ , sinon  $a = axx^{-1}$  serait élément de  $H$  lui aussi. Donc  $ax$  est élément de  $K$ . Mais alors,  $x = a^{-1}ax$  est un élément de  $L$  puisque  $a$  et  $ax$  sont tous deux éléments de  $K$ , donc de  $L$ , et que  $L$  est un sous-groupe (ce qui entraîne que  $a^{-1} \in L$  et que le produit  $a^{-1}ax$  est aussi dans  $L$ ).

---

#### Correction de l'exercice 5 ▲

1. Soit  $f : H \rightarrow aH$  définie par  $f(h) = ah$ . Il s'agit clairement d'une surjection de  $H$  sur  $aH$ . De plus, si  $ah_1 = ah_2$ , alors  $h_1 = h_2$  car  $a$  est inversible, et donc  $f$  est aussi injective.  $f$  est donc une bijection de  $H$  sur  $aH$ ; ces deux ensembles ont le même nombre d'éléments.

2. Supposons que  $aH \cap bH \neq \emptyset$  et prouvons que  $aH = bH$ . Par symétrie, il suffit de prouver que  $aH \subset bH$ . Soit  $x \in aH \cap bH, x = ah_1 = bh_2$ . Prenons  $y = ah \in aH$ . Alors  $a = bh_2h_1^{-1}$  et donc  $y = bh_2h_1^{-1}h \in bH$ .

3. La réunion des ensembles  $aH$  est clairement égale à  $G$  (si  $x \in G$ , il est dans  $xH$ ). On ne garde que les  $aH$  deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de  $G$  avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de  $H$ . Si  $k$  est le nombre d'ensembles nécessaires pour réaliser cette partition, on a

$$k \text{ card}(H) = \text{card}(G)$$

et donc le cardinal de  $H$  divise celui de  $G$ .

---

#### Correction de l'exercice 6 ▲

Supposons d'abord que  $AB = BA$ . Alors  $AB$  est un sous-groupe de  $G$  car :

1.  $e \in AB$ , car  $e = ee$  avec  $e \in A$  et  $e \in B$  (ce sont des sous-groupes);

2.  $AB$  est stable par passage au produit. En effet, si  $x = ab \in AB$  et  $y = a'b' \in AB$ , alors  $xy = aba'b'$ . Or,  $ba'$  est un élément de  $BA$ , c'est donc aussi un élément de  $AB$  et donc  $ba' = a''b''$  avec  $a'' \in A$  et  $b'' \in B$ . On en déduit que

$$xy = aa''b''b' \in AB$$

puisque  $aa'' \in A$  et  $b''b' \in B$ .

3.  $AB$  est stable par passage à l'inverse. En effet, si  $x = ab \in AB$ , alors  $x^{-1} = b^{-1}a^{-1}$  est élément de  $BA$  et  $BA = AB$ . Réciproquement, supposons que  $AB$  est un sous-groupe de  $G$  et prouvons que  $AB = BA$ . Soit d'abord  $x = ab \in AB$ . Alors  $x^{-1} = b^{-1}a^{-1} \in AB$  puisque  $AB$  est un groupe et donc  $b^{-1}a^{-1} = a'b'$  avec  $a' \in A$  et  $b' \in B$ . On passe à l'inverse :

$$ab = b'^{-1}a'^{-1} \in BA.$$

Pour l'autre inclusion, considérons  $y = ba \in BA$ . Alors  $y^{-1} = a^{-1}b^{-1} \in AB$ , et donc  $y = (y^{-1})^{-1} \in AB$  puisque  $AB$  est un groupe. .

---

#### Correction de l'exercice 7 ▲

1. Si  $\phi$  était un morphisme de groupe, on aurait, puisque  $I_n$  est l'élément neutre du groupe  $(GL_n(\mathbb{R}), \times)$  et 0 celui de  $\mathbb{R}_+$ ,  $\phi(I_n) = 0$ . Ce n'est pas le cas, car  $\phi(I_n) = n$ . On peut aussi trouver deux exemple de matrices  $A$  et  $B$  pour lesquelles on n'a pas  $\phi(AB) = \phi(A) + \phi(B)$  (ici aussi,  $A = B = I_n$  conviennent).

2. Dans ce cas,  $\phi$  est bien un morphisme de groupe car on a bien  $\text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B)$ . La morale des deux premières questions est qu'il faut vraiment faire très attention aux groupes en jeu, pas seulement à l'application.

3. Ici aussi,  $\phi$  est un morphisme de groupes car pour tous  $x, y \neq 0$ , on a

$$\phi(xy) = |xy| = |x| \times |y| = \phi(x) \times \phi(y).$$

4. Si  $\phi$  était un morphisme de groupes, on aurait  $\phi(1) = 1$  puisque 1 est l'élément neutre de  $(\mathbb{R}^*, \times)$ . Ce n'est pas le cas puisque  $\phi(1) = 2$ .

5. On va revenir à la définition. Soit  $x, y \in \mathbb{R}$ . On a

$$\phi(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

tandis que par les règles du produit matriciel

$$\phi(x) \times \phi(y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

Les deux résultats coïncident :  $\phi$  est bien un morphisme de groupes.

---

### Correction de l'exercice 8 ▲

---

1. Il suffit d'appliquer la définition : pour tous  $x, y \in G$ , on a

$$\tau_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \tau_a(x)\tau_a(y).$$

2. Soit  $x \in G$ . On a

$$\tau_a \circ \tau_b(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1}$$

tandis que

$$\tau_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1}.$$

On a donc  $\tau_a \circ \tau_b = \tau_{ab}$ .

3. Soit  $a \in G$ . On pourrait prouver que  $\tau_a$  est injectif en calculant son noyau, puisqu'il est surjectif, mais c'est plus facile d'appliquer la question précédente. Avec  $b = a^{-1}$ , elle donne

$$\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_e = Id_G$$

et en inversant le rôle joué par  $a$  et  $b$ , on a aussi

$$\tau_{a^{-1}} \circ \tau_a = Id_G.$$

Ainsi,  $\tau_a$  est inversible d'inverse  $\tau_{a^{-1}}$ .

4. On va prouver que  $\Theta = \{\tau_a; a \in G\}$  est un sous-groupe de  $(S_G, \circ)$ . Il est non-vide parce qu'il contient  $\tau_e$ . Si  $\tau_a, \tau_b \in \Theta$ , alors

$$(\tau_a)^{-1} = \tau_{a^{-1}} \in \Theta$$

et

$$\tau_a \circ \tau_b = \tau_{ab} \in \Theta.$$

Ainsi,  $(\Theta, \circ)$  est bien un sous-groupe de  $(S_G, \circ)$ .

---

### Correction de l'exercice 9 ▲

---

Puisque  $f$  n'est pas constante, il existe  $a \in G$  tel que  $f(a) \neq 1$ . Maintenant, l'application  $x \mapsto ax$  est une permutation de  $G$  : en effet, pour tout  $y \in G$ , il existe un unique  $x \in G$  tel que  $y = ax$  ( $x$  est égal à  $a^{-1}y$ ). On en déduit que

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(x).$$

Mais d'autre part, puisque  $f$  est un morphisme de groupes, on a aussi

$$\sum_{x \in G} f(ax) = \sum_{x \in G} f(a)f(x) = f(a) \sum_{x \in G} f(x).$$

Ainsi, il vient

$$(f(a) - 1) \times \sum_{x \in G} f(x) = 0.$$

Puisque  $f(a) \neq 1$ , on en déduit que  $\sum_{x \in G} f(x) = 0$ .

---

#### Correction de l'exercice 10 ▲

Soit  $f$  un morphisme de  $(\mathbb{Z}, +)$ . Prouvons par récurrence que pour tout  $n \geq 1$ , on a  $f(n) = nf(1)$ . C'est vrai pour  $n = 1$ , et si c'est vrai pour  $n$ , alors

$$f(n+1) = f(n) + f(1) = nf(1) + f(1) = (n+1)f(1).$$

De plus, pour  $n \leq 0$ , on a  $-n \geq 0$  et donc  $f(-n) = -nf(1)$ . On en déduit :

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = f(n) - nf(1).$$

Ainsi, on a toujours  $f(n) = nf(1)$ , quel que soit  $n \in \mathbb{Z}$ . Caractérisons maintenant les morphismes surjectifs. Supposons donc que  $f$  est surjectif. Tout élément de  $\mathbb{Z} = f(\mathbb{Z})$  est un multiple de  $f(1)$ . Or, les seuls éléments de  $\mathbb{Z}$  qui divisent tous les autres entiers sont 1 et  $-1$ . On en déduit que  $f(1) = 1$  ou  $f(1) = -1$ , et donc que  $f(n) = n$  ou  $f(n) = -n$ . Réciproquement, ces deux applications sont clairement des morphismes surjectifs de  $(\mathbb{Z}, +)$ . Déterminons enfin les morphismes injectifs. Soit  $f$  un morphisme et  $n \in \ker(f)$ . Alors  $f(n) = nf(1) = 0$ . Si  $f(1) \neq 0$ , alors  $f(n) = 0 \iff n = 0$  et  $f$  est injectif, et si  $f(1) = 0$ , alors  $f$  n'est pas injectif. Donc tous les morphismes de  $(\mathbb{Z}, +)$  dans  $(\mathbb{Z}, +)$  sont injectifs sauf l'application identiquement nulle.

---

#### Correction de l'exercice 11 ▲

Soit  $f$  un tel morphisme de groupe. On va commencer par démontrer que pour  $p$  et  $q$  des entiers naturels, on a  $f(p) = pf(1)$  et  $f\left(\frac{1}{q}\right) = \frac{1}{q}f(1)$ . La première des deux propriétés se démontre aisément par récurrence. Pour la deuxième, on écrit que

$$f(1) = f\left(\frac{1}{q} + \dots + \frac{1}{q}\right) = qf\left(\frac{1}{q}\right).$$

Notons ensuite  $a = f(1)$ . Alors  $a/q$  est un entier pour tout entier  $q$ , et donc  $a = 0$ . On en déduit que  $f(p) = f(1/q) = 0$  pour tous les entiers  $p$  et  $q$ , puis que  $f(p/q) = pf(1/q) = 0$ . Finalement, on trouve que  $f$  est le morphisme nul.

---

#### Correction de l'exercice 12 ▲

Remarquons d'abord que le morphisme qui à tout  $x$  de  $G_1$  associe l'élément neutre  $e$  de  $G_2$  convient. Réciproquement, soit  $x$  un élément de  $G_1$  et notons  $y = f(x)$ . Puisque  $x$  est un élément de torsion, il existe  $n \geq 1$  tel que  $x^n = e$ . Mais alors,

$$y^n = (f(x))^n = f(x^n) = f(e) = e.$$

Comme  $G_2$  est sans torsion, on a  $y = e$  et donc  $f(x) = e$  pour tout  $x \in G_1$ .

---

#### Correction de l'exercice 13 ▲

Nous noterons dans les deux cas  $\bar{a}$  les éléments de l'ensemble de départ, et  $\tilde{a}$  les éléments de l'ensemble d'arrivée. Dans les deux cas, on peut remarquer qu'il suffit de déterminer l'image de  $\bar{1}$ , qui engendre le groupe...

1. Soit  $\phi$  un tel morphisme. Alors  $\phi(\bar{1})$  a un ordre qui divise 3, puisque  $\phi(\bar{1}) + \phi(\bar{1}) + \phi(\bar{1}) = \phi(\bar{0}) = \tilde{0}$ . Mais  $\phi(\bar{1})$  a aussi un ordre qui divise 4, puisque c'est un élément de  $\mathbb{Z}/4\mathbb{Z}$ . Son ordre divise donc le pgcd de 3 et 4, c'est-à-dire que son ordre est 1. Donc  $\phi(\bar{1}) = \tilde{0}$ , le seul morphisme est le morphisme trivial.

2. Reprenons les mêmes notations. Cette fois on a que  $\phi(\bar{1})$  a pour ordre un diviseur du pgcd de 6 et 8. Son ordre peut donc être égal à 1 ou 2. Si son ordre est égal à 1, il s'agit du morphisme trivial. Si son ordre est égal à 2, on a nécessairement  $\phi(\bar{1}) = \tilde{4}$  qui est le seul élément d'ordre 2 de  $\mathbb{Z}/8\mathbb{Z}$ . Maintenant, il s'agit de voir que cette formule définit bien un morphisme de groupes. Par exemple, on peut remarquer qu'elle donne  $\phi(\bar{k}) = \tilde{0}$  si  $k$  est pair, et  $\phi(\bar{k}) = \tilde{4}$  si  $k$  est impair. A partir de là, il est facile de voir que  $\phi$  définit bien un morphisme de  $\mathbb{Z}/6\mathbb{Z}$  dans  $\mathbb{Z}/8\mathbb{Z}$ .

#### Correction de l'exercice 14 ▲

On a (tenant compte du fait que la loi est notée additivement) :

$$2 \times \bar{9} = \bar{6}, 3 \times \bar{9} = \bar{3}, 4 \times \bar{9} = \bar{0}.$$

$\bar{9}$  est donc d'ordre 4.

#### Correction de l'exercice 15 ▲

D'abord, on remarque que  $x^2$  est d'ordre fini, car  $(x^2)^n = (x^n)^2 = e^2 = e$ . De plus, son ordre que nous allons noter  $d$  divise  $n$ . Distinguons alors deux cas :

Si  $n$  est pair et s'écrit  $2p$ , alors  $(x^2)^p = x^n = e$ , et donc l'ordre de  $x^2$  divise  $p$ . De plus, si l'ordre de  $x^2$  est inférieur strict à  $p$ , on a  $x^{2d} = e$  avec  $1 \leq 2d < n$ , ce qui contredit la définition de l'ordre de  $x$ . Donc, si  $n$  est pair, l'ordre de  $x^2$  est  $n/2$ . Si  $n$  est impair, alors on a  $x^{2d} = e$  et donc  $n|2d$ . Mais comme  $n$  est premier avec 2, on a  $n|d$ . Puisqu'on avait déjà remarqué que  $d|n$ , on en déduit que  $d = n$ . En résumé, si  $n$  est impair, l'ordre de  $x^2$  est  $n$ .

#### Correction de l'exercice 16 ▲

Pour tous  $x, y \in G$ , on a  $x^2 y^2 = e = xyxy$  soit en simplifiant à gauche par  $x$  et à droite par  $y$ ,  $xy = yx$ .

#### Correction de l'exercice 17 ▲

1. On peut commencer par remarquer que, pour  $x, y \in G$ ,

$$x \star y = (x + y) - \lfloor x + y \rfloor.$$

Ainsi, pour  $x, y, z \in G$ ,

$$\begin{aligned} (x \star y) \star z &= (x + y - \lfloor x + y \rfloor) \star z \\ &= x + y - \lfloor x + y \rfloor + z - \lfloor x + y - \lfloor x + y \rfloor + z \rfloor \\ &= x + y - \lfloor x + y \rfloor + z - \lfloor x + y + z \rfloor + \lfloor x + y \rfloor \\ &= x + y + z - \lfloor x + y + z \rfloor \\ &= x \star (y \star z) \end{aligned}$$

(pour passer de la deuxième à la troisième ligne, on a utilisé que  $\lfloor x + n \rfloor = \lfloor x \rfloor + n$  pour tout réel  $x$  et tout entier  $n$ ). La loi est donc associative, et trivialement commutative. On vérifie ensuite facilement que 0 est élément neutre pour  $\star$ , et tout  $x \in G$  admet un symétrique pour  $\star$ , donné par  $1 - x$ .

2. Soit  $x \in G$ ,  $x = \frac{p}{q}$  avec  $q \in \mathbb{N}^*$ . Alors par récurrence on prouve que

$$x^{*q} = qx - \lfloor qx \rfloor = p - p = 0.$$

Ainsi,  $x$  est d'ordre fini (inférieur ou égal à  $q$ ), et  $G$  est un exemple de groupe commutatif infini dont tous les éléments sont d'ordre fini.

---

#### Correction de l'exercice 18 ▲

1. Supposons que  $G$  admette un élément  $x$  d'ordre infini et notons  $H$  le sous-groupe engendré par  $x$ . Alors  $H$  est isomorphe à  $(\mathbb{Z}, +)$ , qui contient une infinité de sous-groupes. On en déduit que  $H$ , et donc  $G$ , contiennent aussi une infinité de sous-groupes (les sous-groupes engendrés par les  $x^n$ ,  $n \geq 1$ , qui ne sont pas deux à deux égaux).

2. Pour  $x \in G$ , notons  $H_x$  le sous-groupe engendré par  $x$ . Alors on a  $G = \bigcup_{x \in G} H_x$ . Mais puisque  $G$  contient seulement un nombre fini de sous-groupes, il y a un nombre fini de  $H_x$  différents, notons-les  $H_{x_1}, \dots, H_{x_p}$ , d'où  $G = \bigcup_{i=1}^p H_{x_i}$ . Mais chacun des  $H_{x_i}$  est fini d'après la question précédente. Donc  $G$  est fini.

---

#### Correction de l'exercice 19 ▲

Si  $G$  n'est pas isomorphe à  $\mathbb{Z}/4\mathbb{Z}$ , alors tous les éléments de  $G$  différents de l'élément neutre sont d'ordre 2. Notons  $a, b, c$  ces éléments, et  $e$  l'élément neutre. On construit alors la table de multiplication du groupe. On peut commencer à écrire :

	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$		
$b$	$b$		$e$	
$c$	$c$			$e$

On peut compléter la deuxième ligne en remarquant que  $ab$  doit être différent de  $a$  (sinon  $b = e$ ), de  $b$  (puisque sinon on aurait  $ab = b$  et donc  $a = e$ ) et de  $e$  (sinon  $ab = aa$  et donc  $a = b$ ). Ainsi, on doit avoir  $ab = c$ . On peut continuer le même raisonnement pour chacun des coefficients manquants et on trouve finalement la table de multiplication suivante :

	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

Mais on reconnaît la table de multiplication (d'addition ?) dans  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , avec par exemple  $a = (\bar{1}, \bar{0})$ ,  $b = (\bar{0}, \bar{1})$ ,  $c = (\bar{1}, \bar{1})$ . Ainsi,  $G$  est bien isomorphe à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , l'isomorphisme étant donné par  $e \mapsto (\bar{0}, \bar{0})$ ,  $a \mapsto (\bar{1}, \bar{0})$ ,  $b \mapsto (\bar{0}, \bar{1})$ ,  $c \mapsto (\bar{1}, \bar{1})$ .

---

#### Correction de l'exercice 20 ▲

1. Rappelons que par le théorème de Bézout,  $n$  est inversible dans  $(\mathbb{Z}/20\mathbb{Z}, \cdot)$  si et seulement si  $n$  est premier avec 20. On a donc  $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$ .

2. On prend un élément et toutes ses puissances, jusqu'à obtenir l'élément neutre 1. On obtient

$$\begin{aligned}
 \langle 1 \rangle &= \{1\} \\
 \langle 3 \rangle &= \{1, 3, 7, 9\} \\
 \langle 7 \rangle &= \{1, 3, 7, 9\} \\
 \langle 9 \rangle &= \{1, 9\} \\
 \langle 11 \rangle &= \{1, 11\} \\
 \langle 13 \rangle &= \{1, 9, 13, 17\} \\
 \langle 17 \rangle &= \{1, 9, 13, 17\} \\
 \langle 19 \rangle &= \{1, 19\}
 \end{aligned}$$

3. On vient de voir qu'on ne peut pas engendrer le groupe avec un seul élément. Essayons avec deux éléments. C'est facile à voir. Si on prend par exemple 3 et 11, le groupe engendré comprend au moins  $\langle 3 \rangle$  et  $\langle 11 \rangle$ , c'est-à-dire au moins 5 éléments. Comme son ordre doit diviser l'ordre du groupe, il contient au moins 8 éléments, c'est-à-dire que c'est  $G$  tout entier. Autrement dit, on a prouvé que  $\langle 3, 11 \rangle = G$  et donc  $\{3, 11\}$  est un ensemble minimal de générateurs de  $G$ .

4. Aucun élément de  $G$  n'engendre seul le groupe.  $G$  n'est pas cyclique.

5. Les sous-groupes de  $G$  sont d'ordre 1, 2, 4 ou 8. Dans  $G$ , il y a un élément d'ordre 1, 4 éléments d'ordre 4 et 3 éléments d'ordre 2. Si on combine deux éléments d'ordre 4 qui n'engendrent pas le même sous-groupe, ou un élément d'ordre 4 avec un élément d'ordre 2 qui n'est pas dans le sous-groupe engendré (comme à la question 3), on obtiendra  $G$  tout entier. Reste à voir les sous-groupes engendrés par les éléments d'ordre 2 : on a

$$\langle 11, 19 \rangle = \{1, 11, 19, 9\}$$

$$\langle 3, 11 \rangle = \langle 3, 13 \rangle = \langle 3, 19 \rangle = \langle 11, 13 \rangle = \langle 13, 19 \rangle = G.$$

6. Parmi les sous-groupes de  $G$ , ceux de la deuxième question sont cycliques, donc isomorphes à  $\mathbb{Z}/m\mathbb{Z}$  où  $m = 1, 2, 4$  suivant le cas. Le sous-groupe  $\langle 11, 19 \rangle$  n'est pas cyclique, car il n'est pas engendré par un seul élément. De même,  $G$  n'est pas cyclique.

### Correction de l'exercice 21 ▲

1. La relation est clairement réflexive et symétrique. De plus, si  $x\mathcal{R}y$  et  $y\mathcal{R}z$ , alors

si  $x = y$  et  $y = z$ , on a  $x = z$ ; si  $x = y$  et  $y = z^{-1}$ , on a  $x = z^{-1}$ ; si  $x = y^{-1}$  et  $y = z$ , on a  $x = z^{-1}$ ; si  $x = y^{-1}$  et  $y = z^{-1}$ , on a  $x = z$ .

Dans tous les cas, on a  $x\mathcal{R}z$  et la relation est transitive.

2. si  $x = y$  et  $y = z$ , on a  $x = z$ ;

3. si  $x = y$  et  $y = z^{-1}$ , on a  $x = z^{-1}$ ;

4. si  $x = y^{-1}$  et  $y = z$ , on a  $x = z^{-1}$ ;

5. si  $x = y^{-1}$  et  $y = z^{-1}$ , on a  $x = z$ .

6. Puisqu'on n'a pas  $x\mathcal{R}y$  si  $y \notin \{x, x^{-1}\}$ , une classe d'équivalence comporte

ou bien un seul élément, si  $x = x^{-1}$ ; ou bien exactement deux éléments, si  $x \neq x^{-1}$ ; ces éléments sont alors  $x$  et  $x^{-1}$ .

Il y a au moins une classe d'équivalence avec un seul élément : la classe de l'élément neutre. De plus, les classes d'équivalence forment une partition de  $G$ , et  $G$  est de cardinal pair. Il doit donc y avoir au moins une autre classe de cardinal 1 (sinon le cardinal de  $G$  serait impair). Cette autre classe de cardinal 1 donne un élément  $x$  égal à son inverse.

7. ou bien un seul élément, si  $x = x^{-1}$ ;

8. ou bien exactement deux éléments, si  $x \neq x^{-1}$ ; ces éléments sont alors  $x$  et  $x^{-1}$ .

### Correction de l'exercice 22 ▲

1. Notons  $d$  l'ordre de  $xy$ . Remarquons que  $(xy)^{pq} = (x^p)^q(y^q)^p = e$ , et donc  $d|pq$ . De plus, puisque  $(xy)^d = e$ , on en déduit que  $x^d = y^{-d}$ . Il vient alors

$$x^{dq} = (y^{-d})^q = (y^q)^{-d} = e.$$

Ainsi,  $p|dq$  et puisque  $p$  et  $q$  sont premiers entre eux, on en déduit que  $p|d$ . De la même façon, on a  $q|d$  et en utilisant à nouveau que  $p$  et  $q$  sont premiers entre eux, on conclut que  $pq|d$ . Ainsi, on a bien que  $d = pq$ .

2. On vérifie facilement que  $A$  est d'ordre 4, que  $B$  est d'ordre 3 et que

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

On prouve alors par récurrence que, pour tout  $n \geq 1$ ,

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

$AB$  n'est pas d'ordre fini, et donc l'hypothèse que  $G$  est commutatif est importante.

3. Si  $x$  est un élément d'ordre  $n \geq 2$  dans un groupe  $G$ , son inverse  $x^{-1}$  est aussi d'ordre  $n$ , et pourtant le produit  $xx^{-1}$  est d'ordre 1, et non d'ordre  $n$  ou  $n^2$  !

4. Une application :

Considérons  $a = x^{p/d}$ . Alors on a  $a^d = x^p = e$ . D'autre part, si  $a^r = e$ , alors  $x^{rp/d} = e$  et donc  $rp/d$  est un multiple de  $p$ . En particulier  $r/d$  est un entier, ce qui signifie que  $d|r$ .  $a$  est donc bien d'ordre  $d$ . Décomposons  $p$  et  $q$  en facteurs premiers (pour avoir les mêmes facteurs, on s'autorise des exposants nuls) :

$$p = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad q = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

On sait qu'alors

$$\text{ppcm}(p, q) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

Par la question précédente, il est possible, pour chaque  $i = 1, \dots, r$ , de fabriquer un élément  $a_i$  d'ordre  $p_i^{\max(\alpha_i, \beta_i)}$  (on le fabrique à partir de  $x$  si  $\alpha_i \geq \beta_i$ , à partir de  $y$  sinon). En utilisant le résultat de la première question et une simple récurrence, le produit  $a_1 \dots a_r$  est bien d'ordre  $\text{ppcm}(p, q)$ . Notons  $x_1, \dots, x_r$  les éléments de  $G$ , d'ordres respectifs  $q_1, \dots, q_r$ . Alors d'après la question précédente, il existe un élément d'ordre  $\text{ppcm}(q_1, q_2)$ . Puis appliquant une nouvelle fois la question précédente, il existe un élément d'ordre  $\text{ppcm}(\text{ppcm}(q_1, q_2), q_3) = \text{ppcm}(q_1, q_2, q_3)$ . Par une récurrence facile, on construit un élément d'ordre le  $\text{ppcm}$  que  $q_1, \dots, q_r$ .

5. Considérons  $a = x^{p/d}$ . Alors on a  $a^d = x^p = e$ . D'autre part, si  $a^r = e$ , alors  $x^{rp/d} = e$  et donc  $rp/d$  est un multiple de  $p$ . En particulier  $r/d$  est un entier, ce qui signifie que  $d|r$ .  $a$  est donc bien d'ordre  $d$ .

6. Décomposons  $p$  et  $q$  en facteurs premiers (pour avoir les mêmes facteurs, on s'autorise des exposants nuls) :

$$p = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad q = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

On sait qu'alors

$$\text{ppcm}(p, q) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

Par la question précédente, il est possible, pour chaque  $i = 1, \dots, r$ , de fabriquer un élément  $a_i$  d'ordre  $p_i^{\max(\alpha_i, \beta_i)}$  (on le fabrique à partir de  $x$  si  $\alpha_i \geq \beta_i$ , à partir de  $y$  sinon). En utilisant le résultat de la première question et une simple récurrence, le produit  $a_1 \dots a_r$  est bien d'ordre  $\text{ppcm}(p, q)$ .

7. Notons  $x_1, \dots, x_r$  les éléments de  $G$ , d'ordres respectifs  $q_1, \dots, q_r$ . Alors d'après la question précédente, il existe un élément d'ordre  $\text{ppcm}(q_1, q_2)$ . Puis appliquant une nouvelle fois la question précédente, il existe un élément d'ordre  $\text{ppcm}(\text{ppcm}(q_1, q_2), q_3) = \text{ppcm}(q_1, q_2, q_3)$ . Par une récurrence facile, on construit un élément d'ordre le  $\text{ppcm}$  que  $q_1, \dots, q_r$ .

### Correction de l'exercice 23 ▲

1. On a  $(g, h)^n = (g^n, h^n) = (e, e)$  si et seulement si on a à la fois  $p|n$  et  $q|n$ , donc si et seulement si  $\text{ppcm}(p, q)|n$ . Ainsi, l'ordre de  $(g, h)$  est bien le  $\text{ppcm}$  de  $p$  et  $q$ .

2. Soit  $p$  l'ordre de  $G$  et  $q$  l'ordre de  $H$ . Si  $p \wedge q = 1$ , si  $x$  est un générateur de  $G$  (d'ordre  $p$  donc) et si  $y$  est un générateur de  $H$  (d'ordre  $q$  donc), alors  $(x, y)$  est d'ordre  $\text{ppcm}(p, q) = pq$ . Puisque  $G \times H$  est de cardinal  $pq$ , c'est bien un groupe cyclique. Réciproquement si  $G \times H$  est cyclique, soit  $(g, h)$  un générateur de  $G \times H$ . Alors  $g$  est un générateur de  $G$  et  $h$  est un générateur de  $H$ . Leur ordre respectif est donc  $p$  (resp.  $q$ ), et par la première question,  $(g, h)$  est d'ordre  $\text{ppcm}(p, q)$ . Puisqu'on sait qu'il est d'ordre  $pq$ , on a bien  $\text{ppcm}(p, q) = pq$  qui implique que  $p$  et  $q$  sont premiers entre eux.

### Correction de l'exercice 24 ▲

Soit  $a$  un générateur de  $G$ . L'ensemble des entiers  $p \geq 1$  tels que  $a^p \in H$  est non-vide (puisque  $a^{\text{card}(G)} = e \in H$ ). Il contient un plus petit élément que nous noterons  $n$ . On va alors prouver que  $H$  est le groupe engendré par  $a^n$ . Il est d'abord évident que le sous-groupe engendré par  $a^n$  est contenu dans  $H$ . Réciproquement, soit  $x \in H$ .  $x$  s'écrit  $x = a^p$ , et il suffit de prouver que  $p = kn$ . Effectuons la division euclidienne de  $p$  par  $n$  :  $p = qn + r$  avec  $0 \leq r < n$ . Mais alors :

$$a^p = (a^n)^q a^r \implies a^r = a^p (a^n)^{-q} \in H.$$



**Par minimalité de  $n$ , ceci n'est possible que si  $r = 0$ , donc que si  $p$  est un multiple de  $n$ . Remarquons la proximité entre cette démonstration et celle des sous-groupes de  $\mathbb{Z}$ .**

---