

# 1 Arithmétique

**Exercice 1.** On considère  $\mathbb{Z}$  muni de sa structure de groupe.

- Montrer que les sous groupes de  $\mathbb{Z}$  sont de la forme  $n\mathbb{Z}$  avec  $n$  entier naturel.
- Montrer que les sous-groupes  $n\mathbb{Z}$  sont tous distingués.

**Exercice 2.** Dresser la table des groupes suivants

$$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}.$$

En omettant 0 ces ensembles ont ils une structure de groupe pour la multiplication ?

**Exercice 3.** 1. Montrer que l'intersection de deux sous-groupes de  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ . Caractériser le sous-groupe  $a\mathbb{Z} \cap b\mathbb{Z}$ . Caractériser les sous-groupes suivants :

$$2\mathbb{Z} \cap 3\mathbb{Z}; \quad 5\mathbb{Z} \cap 13\mathbb{Z}; \quad 5\mathbb{Z} \cap 25\mathbb{Z}.$$

2. Montrer que toute intersection de sous-groupes de  $\mathbb{Z}$  est un sous-groupe de  $\mathbb{Z}$ . Caractériser les sous-groupes suivants :

$$\bigcap_{n=1}^{17} 2^n \mathbb{Z}; \quad 4\mathbb{Z} \cap 6\mathbb{Z} \cap 8\mathbb{Z} \cap 19\mathbb{Z} \cap 35\mathbb{Z}.$$

**Exercice 4.** 1. Déterminer  $2\mathbb{Z} \cup 3\mathbb{Z}$ . Est-ce un sous-groupe de  $\mathbb{Z}$  ?

2. Déterminer :  $7\mathbb{Z} \cup 49\mathbb{Z}$ ;  $5\mathbb{Z} \cup 45\mathbb{Z}$ ;  $\bigcup_{n=1}^{28} 2^n \mathbb{Z}$ . Ces ensembles sont-ils des sous-groupes de  $\mathbb{Z}$  ?
3. Trouver une condition nécessaire et suffisante pour qu'une réunion de deux sous-groupes de  $\mathbb{Z}$  soit un sous-groupe de  $\mathbb{Z}$ .

# 2 Groupes, théorie générale

**Exercice 5.** Construire, à isomorphisme près, les groupes à  $n$  éléments pour  $1 \leq n \leq 4$ .

**Exercice 6.** Soient les quatre fonctions de  $\mathbb{R}^*$  dans  $\mathbb{R}^*$

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

Montre que  $G = \{f_1, f_2, f_3, f_4\}$  est un groupe pour la loi  $\circ$ .

**Exercice 7.** Les ensembles suivants, pour les lois considérées, sont-ils des groupes ?

1.  $] - 1, 1[$  muni de la loi définie par  $x \star y = \frac{x+y}{1+xy}$  ;
2.  $\{z \in \mathbb{C} : |z| = 2\}$  pour la multiplication usuelle ;
3.  $\mathbb{R}_+$  pour la multiplication usuelle ;
4. L'ensemble des fonctions

$$f : \begin{array}{l} \mathbb{R} \mapsto \mathbb{R} \\ x \mapsto ax + b \end{array}$$

$a \in \mathbb{R} \setminus \{0\}, b \in \mathbb{R}$ , pour la loi de composition des applications.

**Exercice 8.** Soit le groupe  $G = \mathbb{Z}/12\mathbb{Z}$ .

1. Déterminer le sous-groupe  $H$  de  $G$  engendré par  $\bar{6}$  et  $\bar{8}$  et déterminer son ordre.
2. Caractériser les générateurs de  $G$ .
3. Quel est l'ordre de l'élément  $\bar{9}$  ?

**Exercice 9.** Soit  $G$  un groupe et  $H$  une partie finie, non vide, de  $G$  stable pour la loi  $\cdot$ , montrer que  $H$  est un sous-groupe de  $G$ .

**Exercice 10.** Soit  $G$  un groupe fini de cardinal  $n$  et  $m$  un entier premier avec  $n$ . Montrer que, pour tout  $y$  élément de  $G$ , il existe un unique  $x$  élément de  $G$  tel que  $x^m = y$ .

[[Utiliser le théorème de Bezout.]]

**Exercice 11.** Soit  $(G, \cdot)$  un groupe fini de cardinal  $n$ . On suppose que, tout  $x$  élément de  $G$ , satisfait l'égalité  $x^2 = e$ .

1. Montrer que  $G$  est un groupe commutatif.
2. Soit  $A = \{a_1, \dots, a_p\}$  une partie génératrice de  $G$ , montrer que :

$$\forall x \in G, \quad \exists (\epsilon_1, \dots, \epsilon_p) \in (\mathbb{Z}/2\mathbb{Z})^p \text{ tels que, } x = a_1^{\epsilon_1} \dots a_p^{\epsilon_1}.$$

3. On suppose, dans les questions suivantes, que  $A$  est une partie génératrice de cardinal minimum  $p$ . Montrer que l'écriture :

$$x = a_1^{\epsilon_1} \dots a_p^{\epsilon_p}$$

est unique.

4. Soit  $\Phi$  l'application définie par :

$$\begin{aligned} \Phi : G &\rightarrow (\mathbb{Z}/2\mathbb{Z})^p \\ x &\mapsto (\epsilon_1, \dots, \epsilon_p). \end{aligned}$$

Montrer que  $\Phi$  est bien définie et que c'est un isomorphisme de groupes. En déduire que le cardinal de  $G$  est  $2^p$ .

**Exercice 12.** Soit  $p$  un nombre premier fixé, soit

$$U_p = \left\{ \exp\left(\frac{2i\pi a}{p^\alpha}\right), a \in \mathbb{Z}, \text{PGCD}(a, p) = 1, \alpha \in \mathbb{N} \right\}$$

1. Montrer que  $U_p$  est un groupe infini dont tous les éléments sont d'ordre fini. Trouver l'ordre de  $\exp\left(\frac{2i\pi a}{p^\alpha}\right)$ , pour  $a$  entier premier avec  $p$  et pour  $\alpha \in \mathbb{N}$ .
2. Montrer que tout sous-groupe strict de  $U_p$  est cyclique.  
[[Soit  $H$  un sous-groupe de  $U_p$ . Montrer tout d'abord que, si  $x = \exp\left(\frac{2i\pi a}{p^\alpha}\right)$  appartient à  $H$  alors, tout  $z = \exp\left(\frac{2i\pi b}{p^\beta}\right)$  avec  $\beta \leq \alpha$  appartient à  $H$ .]]

**Exercice 13.** Soit  $G$  un groupe et  $\Sigma_1, \dots, \Sigma_n$  des morphismes distincts de  $G$  dans  $(\mathbb{C}^*, \times)$ . Montrer que  $\Sigma_1, \dots, \Sigma_n$  sont linéairement indépendants sur  $\mathbb{C}$  dans l'espace vectoriel des fonctions de  $G$  à valeurs dans  $\mathbb{C}$ .  
[[On pourra faire intervenir une combinaison linéaire des  $(\Sigma_i)$  de cardinal minimum.]]

### 3 Morphisme de groupes

**Exercice 14.** Décrire tous les homomorphismes de groupes de  $\mathbb{Z}$  dans  $\mathbb{Z}$ . Déterminer ceux qui sont injectifs et ceux qui sont surjectifs.

**Exercice 15.** Pour tout couple  $(a, b)$  de  $\mathbb{R}^2$ , on pose la matrice  $M_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ . Soit  $\mathcal{S} = \{M_{a,b} : (a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}\}$ . Soit l'application  $f : \mathcal{S} \rightarrow \mathbb{R}, M_{a,b} \mapsto a^2 + b^2$ .

1. Montrer que  $\mathcal{S}$  est un groupe pour la loi usuelle de multiplication des matrices carrées.
2. Montrer que  $f$  est un morphisme du groupe  $(\mathcal{S}, \times)$  dans le groupe multiplicatif  $\mathbb{R} \setminus \{(0, 0)\}$ .

**Exercice 16.** Soit  $f : \mathbb{R} \rightarrow \mathbb{C}^*$  l'application qui à tout  $x \in \mathbb{R}$  associe  $e^{ix} \in \mathbb{C}^*$ . Montrer que  $f$  est un homomorphisme de groupes. Calculer son noyau et son image.  $f$  est-elle injective ?

**Exercice 17.** Traduire en termes d'homomorphisme de groupes les propriétés traditionnelles suivantes :

1.  $\ln(xy) = \ln x + \ln y$  ;
2.  $\det(MM') = \det(M) \det(M')$  ;
3.  $|zz'| = |z||z'|$  ;
4.  $(xy)^{\frac{1}{2}} = x^{\frac{1}{2}}y^{\frac{1}{2}}$  ;
5.  $e^{z+z'} = e^z e^{z'}$  ;
6.  $\overline{z + z'} = \bar{z} + \bar{z}'$ .

**Exercice 18.** Pour tout couple  $(a, b)$  de  $\mathbb{R}^2$ , on pose  $M_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ ,  $\mathcal{S} = \{M_{a,b} : (a, b) \in \mathbb{R}^2\}$  et  $\mathcal{S}^* = \mathcal{S} \setminus \{M_{0,0}\}$ . Soit l'application  $f : \mathcal{S} \rightarrow \mathbb{C}$ ,  $M_{a,b} \mapsto a + ib$ .

1. (a) Montrer que  $\mathcal{S}$  est un sous-groupe du groupe additif usuel  $\mathcal{M}_2(\mathbb{R})$ .  
(b) Montrer que  $\mathcal{S}^*$  est un sous-groupe multiplicatif de  $GL_2(\mathbb{R})$ .
2. Montrer que  $f$  est un isomorphisme du groupe  $(\mathcal{S}, +)$  sur le groupe additif  $\mathbb{C}$ .
3. (a) Montrer que  $f$  définit un homomorphisme du groupe  $(\mathcal{S}^*, \times)$  sur le groupe multiplicatif  $\mathbb{C}^*$ .  
(b) Déterminer le noyau et l'image de cet homomorphisme.
4. Montrer que  $\Omega = \{M_{a,b} : (a, b) \in \mathbb{R}^2, a^2 + b^2 = 1\}$  est un sous-groupe distingué du groupe multiplicatif  $\mathcal{S}^*$ .

**Exercice 19.** Soit  $G$  un groupe. Montrer que l'application  $x \rightarrow x^{-1}$  est un morphisme si et seulement si  $G$  est commutatif. On suppose  $G$  fini ; soit  $\phi$  un morphisme involutif de  $G$  dont le seul point fixe est  $e$ , montrer que :

$$\forall z \in G, \exists t \in G, z = t(\phi(t))^{-1}.$$

En déduire  $\phi$  puis que  $G$  est commutatif.

**Exercice 20.** Montrer que les groupes  $(\mathbb{R}, +)$  et  $(\mathbb{R}_+^*, \times)$  sont isomorphes.

**Exercice 21.** Soit  $G$  un groupe.

1. Montrer que l'ensemble des automorphismes de  $G$  muni de la loi de composition des applications est un groupe. Ce groupe est noté  $\text{Aut}(G)$ .
2. Vérifier que l'application  $\phi : G \rightarrow \text{Aut}(G)$  qui associe à  $g \in G$  l'application  $\phi_g : G \rightarrow G, x \mapsto gxg^{-1}$  est un morphisme de groupes. Déterminer son noyau  $Z(G)$ , dit centre de  $G$ .
3. Déterminer  $\text{Aut}(\mathbb{Q})$  et  $\text{Aut}(\mathbb{Z})$ .

## 4 Sous-groupes distingués, groupes quotients

**Exercice 22** (Normalisateur). Soit  $H$  un sous-groupe de  $G$ , on appelle normalisateur de  $H$  l'ensemble des  $x$  éléments de  $G$ , tels que  $xHx^{-1} = H$  ; le normalisateur de  $H$  est noté  $N_H$ .

1. Montrer que  $N_H$  est un sous-groupe de  $G$  et que  $H$  est distingué dans  $N_H$ .
2. Soit  $K$  un sous groupe de  $G$  contenant  $H$  et tel que  $H$  soit distingué dans  $K$ . Montrer que  $K$  est un sous-groupe de  $N_H$  ; en déduire que  $N_H$  est le plus grand sous-groupe de  $G$  dans lequel  $H$  est distingué.
3. Soit  $K$  un sous-groupe de  $N_H$  montrer que  $HK$  est un groupe et que  $H$  est distingué dans  $HK$ .
4. Soient  $H$  et  $K$  deux sous-groupes de  $G$ . Montrer que  $HK$  est un groupe si et seulement si  $HK = KH$ .

**Exercice 23.** 1. Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes de  $G$ , on suppose que  $H$  est contenu dans le normalisateur de  $K$ .

Montrer que  $H \cap K$  est un sous-groupe distingué de  $H$ .

Montrer que  $H/(H \cap K)$  est isomorphe à  $HK/K$ .

[[Utiliser le théorème de factorisation des morphismes.]]

2. Soit  $G$  un groupe,  $H$  et  $K$  deux sous-groupes distingués de  $G$  tel que  $K$  est contenu dans  $H$ .

Montrer que  $K$  est distingué dans  $H$ .

Montrer que  $(G/K)/(H/K)$  est isomorphe à  $G/H$ .

[[Utiliser le théorème de factorisation des morphismes.]]

**Exercice 24.** Soit  $G$  un groupe tel que  $G/Z(G)$  est cyclique, ( $Z(G)$  est le centre de  $G$ ), montrer que  $G$  est abélien.

**Exercice 25** (Sous-groupe dérivé). Soit  $G$  un groupe, on note  $D(G)$  (sous-groupe dérivé de  $G$ ) le sous groupe engendré par :

$$\{xyx^{-1}y^{-1}, \text{ où } x, y \in G\}.$$

1. Montrer que  $G$  est abélien si et seulement si  $D(G)$  est réduit à l'élément neutre.
2. Montrer que  $D(G)$  est invariant par tout automorphisme de  $G$ . En déduire que  $D(G)$  est un sous-groupe distingué de  $G$ .
3. Montrer que  $G/D(G)$  est un groupe commutatif.
4. Soit  $H$  un sous-groupe de  $G$  tel que  $G/H$  est commutatif, montrer que  $D(G)$  est inclus dans  $H$ .

## 5 Groupes abéliens

**Exercice 26.** Le groupe  $(\mathbb{Q}, +)$  est-il monogène ?

**Exercice 27.** Soit  $G$  un groupe abélien fini,  $a$  et  $b$  deux éléments de  $G$ . On note  $O(a)$  l'ordre de  $a$  et  $O(b)$  l'ordre de  $b$ . Le but de l'exercice est de voir quelles sont les valeurs que peut prendre l'ordre de l'élément  $ab$ .

1. Soit  $p$  entier non nul tel que  $(ab)^p = e$ , soit  $m$  le PPCM de  $p$  et  $O(a)$ ,  $n$  le PPCM de  $p$  et  $O(b)$ . Montrer que  $O(a)$  divise  $n$  et que  $O(b)$  divise  $m$ .
2. En déduire que  $O(ab)$  est le PPCM de  $O(a)$  et  $O(b)$  si aucun facteur premier ne figure à un même exposant non nul dans les décompositions en facteurs premiers de  $O(a)$  et  $O(b)$ .  
En déduire que lorsque  $O(a)$  et  $O(b)$  sont premiers entre eux, alors  $O(ab) = O(a)O(b)$ .
3. Montrer que le résultat précédent est faux en général.
4. Notons  $d$  le PGCD de  $O(a)$  et  $O(b)$  et  $M$  le PPCM de  $O(a)$  et  $O(b)$ , en utilisant la première question, montrer que :  
 $\frac{M}{d}$  divise  $O(ab)$  et que  $O(ab)$  divise  $M$ .

5. En choisissant des éléments convenables dans le groupe  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ , vérifier que l'on peut avoir :

$$\frac{M}{d} < O(ab) < M.$$

6. Montrer qu'il existe toujours dans  $G$  un élément d'ordre  $M$ .
7. Si  $G$  est non abélien, donner un exemple où  $a$  et  $b$  sont d'ordre 2 et où  $ab$  est d'ordre infini.

**Exercice 28** (Indicateur d'Euler). Soit  $n$  un nombre entier naturel non nul, on pose :

$$\phi(n) = \text{card} \{k, 1 \leq k \leq n, \text{ tels que } k \text{ et } n \text{ sont premiers entre eux}\}.$$

Le but de l'exercice est de montrer la formule  $(\star)$  :

$$\sum_{d/n} \phi(d) = n.$$

1. Soit  $m$  un élément d'ordre  $d$  dans  $\mathbb{Z}/n\mathbb{Z}$ , montrer que  $m$  appartient au sous-groupe  $H$  de  $\mathbb{Z}/n\mathbb{Z}$  engendré par  $\frac{n}{d}$ .
2. Montrer que les éléments d'ordre  $d$  dans  $H$  sont ceux de la forme :  $\frac{kn}{d}$  où  $k$  et  $d$  sont premiers entre eux.
3. Conclure qu'il y a exactement  $\phi(d)$  éléments d'ordre  $d$  dans  $\mathbb{Z}/n\mathbb{Z}$ .
4. Prouver la formule  $(\star)$ .

**Exercice 29** (Automorphismes de  $\mathbb{Z}/n\mathbb{Z}$ ). Soit  $n$  un entier naturel supérieur ou égal à 2, montrer que le groupe des automorphismes de  $\mathbb{Z}/n\mathbb{Z}$  (noté  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ ) est isomorphe à  $(\mathbb{Z}/n\mathbb{Z})^*$ .

[[Considérer l'application qui, à un automorphisme  $\phi$ , associe  $\phi(1)$  et utiliser le fait que les générateurs de  $\mathbb{Z}/n\mathbb{Z}$  sont les inversibles de  $\mathbb{Z}/n\mathbb{Z}$ .]]

**Exercice 30.** Montrer que, pour tout entier naturel non nul  $n$ , le groupe additif  $\mathbb{Q}/\mathbb{Z}$  possède un seul sous-groupe d'ordre  $n$ .

[[Considérer  $H$  un sous-groupe de  $\mathbb{Q}/\mathbb{Z}$  d'ordre  $n$  et  $\Pi$  la projection canonique de  $\mathbb{Q}$  dans  $\mathbb{Q}/\mathbb{Z}$ . En utilisant le fait que les sous-groupes de  $\mathbb{R}$  sont soit denses, soit de la forme  $a\mathbb{Z}$ , montrer que  $\Pi^{-1}(H)$  est de la forme  $\frac{p}{q}\mathbb{Z}$ , avec  $p$  et  $q$  entiers. ]]