Groupes

Exercice 1. ($\heartsuit$) Pour un groupe d'ordre 2, c'est-à-dire à deux éléments, $G = \{e, a\}$ (e est le neutre) il n'existe qu'une seule table possible :

$*$	e	a
e	e	a
a	a	e

1) Montrer qu'il n'existe qu'une seule table possible pour un groupe d'ordre 3.

2) En est-il de même pour un groupe d'ordre 4?

Exercice 2. ($\heartsuit$) On définit sur $G = \mathbb{R} \setminus \{1\}$ la loi $*$ définie par $x * y = x + y - xy$.

1) Montrer que $(G, *)$ est un groupe commutatif.

2) Soit $n \in \mathbb{N}$ et $x \in G$. Calculer $x^{*n} = \underbrace{x * \cdots * x}_{n \text{ facteurs}}$.

3) **Avec un morphisme.** On définit l'application φ par $\varphi(x) = 1 - x$.

   -a- Démontrer que φ est un isomorphisme de groupes de $(G, *)$ vers $(\mathbb{R}^*, \cdot)$.

   -b- Utiliser la question précédente pour calculer $x^{*n} =$, pour $x \in G$ et $n \in \mathbb{N}$.

Exercice 3. ($\heartsuit$) Soient $(G, *)$ et $(G', \otimes)$ deux groupes. On définit sur $G \times G'$ la loi de composition interne $\top$ par

$$(x, x')\top(y, y') = (x * y, x' \otimes y').$$

Montrer que $(G \times G', \top)$ est un groupe (appelé groupe produit).

Exercice 4. ($*$)mais classique ! Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{Z}$.

Exercice 5. ($\heartsuit$) Montrer que $H = \{p\sqrt{2} + q\sqrt{3} \,/\, (p, q) \in \mathbb{Z}^2\}$ est un sous-groupe de $(\mathbb{R}, +)$.

Exercice 6. ($**$) Soit H un sous-groupe de $(\mathbb{R}, +)$ non réduit au singleton $\{0\}$.

1) Montrer que $H \cap \mathbb{R}_+^*$ admet une borne inférieure, que l'on note α.

2) Si a est le minimum de $H \cap \mathbb{R}_+^*$ montrer que H est le sous-groupe $a\mathbb{Z}$.

3) Si $H \cap \mathbb{R}_+^*$ n'admet pas de minimum, montrer par l'absurde que a est nul puis que H est dense dans $\mathbb{R}$.

Exercice 7. ($\heartsuit$) Soit $(G, *)$ un groupe. On définit le centre de G par

$$Z(G) = \{x \in G \,/\, \forall y \in G, x * y = y * x\}.$$

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

Exercice 8. ($*$) Soit $(G, *)$ un groupe tel que pour tout $x \in G$, $x * x = e$ où e est l'élément neutre de G. Montrer que ce groupe est commutatif.

Exercice 9. ($*$) Soit $(G, *)$ un groupe et $H \subset G$ un ensemble fini stable par $*$. Montrer que $(H, *)$ est un sous-groupe de G.

Exercice 10 Soit $(G, *)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

1) Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.

2) Pour $a \in G$, on note $f_a : G \to G$ l'application définie par $f_a(x) = a * x * a^{-1}$.
   Montrer que pour tout $a \in G$, $f_a \in \mathrm{Aut}(G)$.

3) Montrer que l'application $\psi : G \to \mathrm{Aut}(G)$, définie par $\psi(a) = f_a$ est un morphisme de groupe. Déterminer son noyau.

Groupes et arithmétique

Exercice 11. ($*$) Soient deux entiers non nuls a et b.

1) Montrer que : $\delta = a \wedge b \Leftrightarrow \delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.
2) Montrer que : $\mu = a \vee b \Leftrightarrow \mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Exercice 12. ($**$)Théorème de Wilson Soit un entier naturel $p \geqslant 3$.

1) On suppose que $(p-1)! \equiv -1\ [p]$. Montrer que p est premier.
2) On suppose p premier. On pose $G = [\![1, p-1]\!]$ et pour tout $(x, y) \in G^2$, $x*y$ est le reste de la division euclidienne de xy par p.
   -a- Montrer que $(G, *)$ est un groupe.
   -b- Résoudre l'équation $x * x = e$ dans G.
   -c- Démontrer que $(p-1)! \equiv -1\ [p]$.
3) Énoncer le théorème démontré (théorème de Wilson).

Anneaux et corps

Exercice 13. ($*$) Soit $(A, +, \cdot)$ un anneau. Un élément $x \in A$ est dit nilpotent lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0_A$.

1) On suppose A commutatif. Soient a et b deux éléments nilpotents de A. Montrer que $a + b$ est nilpotent.
2) On suppose A commutatif. Soient a et b deux éléments de A avec a nilpotent. Montrer que ab est nilpotent.
3) Soient a et b deux éléments de A. Montrer que si ab est nilpotent alors ba est nilpotent.
4) Montrer que si a est nilpotent alors $1 - a$ est inversible (pour le produit de A) et calculer $(1-a)^{-1}$.

Exercice 14 Soit $(A, +, \times)$ un anneau non nul, on note 1 le neutre de $\times$. On pose l'application $\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & A \\ & n & \mapsto & n \times 1 = 1 + \cdots + 1 \end{array}$.

1) Montrer que φ est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A.
2) Dans le cas où φ n'est pas injectif, montrer qu'il existe un unique $c \in \mathbb{N}^*$, tel que $\operatorname{Ker}\varphi = c\mathbb{Z}$.
   On se place désormais dans ce cas de figure, c est appelé la caractéristique de l'anneau A.
3) Montrer que si A est intègre alors c est un nombre premier.
4) Montrer que si A est commutatif alors $x \mapsto x^c$ est un endomorphisme de l'anneau A.

Exercice 15. ($\heartsuit$) Montrer que l'ensemble $\{a + b\sqrt{3} \;/\; (a, b) \in \mathbb{Q}^2\}$ est un corps.

Exercice 16. ($*$) On note $Z[i] = \{a + \mathrm{i}\, b \;/\; (a, b) \in \mathbb{Z}^2\}$ et $Z(i) = \{a + \mathrm{i}\, b \;/\; (a, b) \in \mathbb{Q}^2\}$.

1) Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau intègre qui n'est pas un corps.
2) Montrer que $(\mathbb{Z}(i), +, \times)$ est un corps.
3) Montrer que toute fraction $\dfrac{A}{B}$ avec $(A, B) \in (\mathbb{Z}[i])^2$ appartient à $\mathbb{Z}(i)$. Et réciproquement que tout élément de $\mathbb{Z}(i)$ s'écrit $\dfrac{A}{B}$ avec $(A, B) \in (\mathbb{Z}[i])^2$.