Exercices sur les structures algébriques

1 Groupe ou pas groupe ?

Exercice 1 (Des lois non associatives)

1. Soit a, b, c dans $\mathbb{N}$. A-t-on $a^{(b^c)} = (a^b)^c$?
2. En géométrie : on note $(\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ la base orthonormée de l'espace. Calculer $\overrightarrow{j} \wedge (\overrightarrow{i} \wedge \overrightarrow{j})$ et $(\overrightarrow{j} \wedge \overrightarrow{i}) \wedge \overrightarrow{j}$. Commenter.

Exercice 2 Dire dans chaque cas si les ensembles suivants sont des groupes.

1. $G = (\mathbb{N}, +)$; $\quad G = (\mathbb{Z}, +)$, $\quad G = (\mathbb{Z}^*, \times)$, $\quad G = (2\mathbb{Z}, +)$
2. $G = (\{-1, 1\}, \times)$, $\quad G = (\{-1, 1\}, +)$
3. $G = (\{z \in \mathbb{C} \mid \ |z| \leqslant 1\}, +)$, $\quad G = (\{z \in \mathbb{C} \mid \ |z| \geqslant 1\}, \times)$
4. $G = (\mathcal{P}(E), \cap)$, $\quad G = (\mathcal{P}(E), \cup)$ où E est un ensemble.
5. $G = (\mathbb{R}_n[X], +)$, $\quad G = (\mathbb{R}_n[X], \times)$ où $\mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \mid \ \deg P \leqslant n\}$.

Exercice 3 Pour x et y dans $G =]-1, 1[$, on pose $x \star y = \dfrac{x+y}{1+xy}$.

1. Soit $y \in]-, 1, 1[$. Démontrer que pour tout $x \in]-1, 1[$ on a $\frac{x+y}{1+xy} \in]-1, 1[$, en étudiant la fonction $f : x \mapsto \frac{x+y}{1+xy}$.
2. Montrer que $(G, \star)$ est un groupe commutatif.

Exercice 4 Pour (x, y) et (x', y') dans $G = \mathbb{R}^* \times \mathbb{R}$, on pose

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

Démontrer que $(G, \star)$ est un groupe non commutatif.

2 Résultats généraux

Exercice 5 Soit $(G, \times)$ un groupe. Démontrer que G est commutatif, si et seulement si, pour tout $a, b \in G$, on a $(ab)^2 = a^2 b^2$.

Exercice 6 (Intersection et réunion de groupes) Soit G un groupe. Démontrer que l'intersection de deux sous-groupes de G est un sous-groupe de G. Et la réunion ?

Exercice 7 (Difficile, mais classique) Soit H et K deux sous-groupes de $(G, +)$. On suppose que $H \cup K$ est un groupe. On veut démontrer alors que $H \subset K$ ou que $K \subset H$.

1. Écrire avec des quantificateurs la négation de l'assertion «$H \subset K$ ou $K \subset H$».
2. Soit $h \in H \setminus K$ et $k \in K \setminus H$. Considérer $h+k$, puis aboutir à une contradiction.

Exercice 8 Soit $(G, \times)$ un groupe. On appelle centre du groupe G l'ensemble

$$Z(G) = \{g \in G \quad | \quad \forall a \in G,\ a \times g = g \times a\}.$$

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

Exercice 9 (Groupes d'exposant 2) Soit $(G, \times)$ un groupe tel que $\forall x \in G$, $x^2 = e$ où e est l'élément neutre de G. On dit que G est d'exposant 2.

1. Soit $x \in G$. Quel est son inverse ?
2. Montrer que G est commutatif.
3. Donner l'exemple d'un groupe D, d'exposant 2, à 4 éléments, inclus dans $\mathcal{M}_2(\mathbb{R})$.

Exercice 10 (Deux morphismes) Soit $(G, \bullet)$ un groupe. Les deux questions sont indépendantes.

1. On suppose en plus que G est commutatif. On considère l'application $\phi : G \to G$ définie par $\phi(x) = x^{-1}$. Démontrer que ϕ est un isomorphisme.
2. Soit $a \in G$. On considère l'application $\phi : G \to G$ définie par $\phi(x) = a \bullet x \bullet a^{-1}$. Démontrer que ϕ est un isomorphisme. Déterminer son inverse.

Exercice 11 Démontrer qu'il n'existe pas d'isomorphisme entre les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$. On pourra raisonner par l'absurde et calculer $\phi(j^3)$ avec $\phi : \mathbb{C}^* \to \mathbb{R}^*$ un isomorphisme

Exercice 12 Pour x et y dans $G =]-1, 1[$, on pose $x \star y = \dfrac{x+y}{1+xy}$. On a vu que $(G, \star)$ est un groupe.

1. Démontrer que pour tout $a, b \in \mathbb{R}$, on a $\operatorname{th}(a+b) = \frac{\operatorname{th} a + \operatorname{th} b}{1 + \operatorname{th} a \operatorname{th} b}$.
2. En déduire que G est isomorphe au groupe $(\mathbb{R}, +)$.

Exercice 13 On pose $G = \{\operatorname{diag}(1,1), \operatorname{diag}(-1,1), \operatorname{diag}(-1,1), \operatorname{diag}(-1,-1)\}$.

1. Justifier que G est un sous-groupe de $GL_2(\mathbb{K})$.
2. Démontrer que G n'est pas isomorphe au groupe $\mathbb{U}_4$.

3 Avec des matrices

Exercice 14 Les ensembles suivants sont-ils des sous-groupes de $\mathcal{M}_n(\mathbb{K})$ pour la loi $+$:

1. l'ensemble $D_n(\mathbb{K})$ des matrices diagonales de $\mathcal{M}_n(\mathbb{K})$
2. l'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbb{K})$
3. l'ensemble des matrices symétriques de $\mathcal{M}_n(\mathbb{K})$

Exercice 15
1. Démontrer que l'application «trace» Tr : $(\mathcal{M}_n(\mathbb{K}), +) \to (\mathbb{K}, +)$ est un morphisme de groupe.
2. L'ensemble des matrices de trace nulle de $\mathcal{M}_n(\mathbb{K})$ est-il un sous-groupe de $\mathcal{M}_n(\mathbb{K})$?

4 Sous-groupes de $\mathbb{Z}$

Exercice 16 (Description des sous-groupes de $\mathbb{Z}$) Si a est un entier, on pose $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$.

1. Quelques exemples
   (a) Démontrer que $G = 4\mathbb{Z} + 6\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Déterminer un entier d tel que $G = d\mathbb{Z}$ (on dit que d est un générateur de G).
   (b) L'ensemble $4\mathbb{Z} \cup 6\mathbb{Z}$ est-il un sous-groupe de $\mathbb{Z}$?
   (c) Généralisation :soit si a et b sont des entiers et $d = \operatorname{pgcd}(a, b)$, démontrer que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
2. Nous allons prouver que tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$. Soit H un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$.
   (a) Justifier l'existence de a le plus petit élément de $H \cap \mathbb{N}^*$.
   (b) Soit $x \in H$. Démontrer que $x \in a\mathbb{Z}$ (on pourra effectuer la division euclidienne de x par a), en déduire que $H = a\mathbb{Z}$.

5 Sous-groupes de $(\mathbb{C}^*, \times)$

Exercice 17 (Sous-groupe borné de $\mathbb{C}^*$) Soit G un sous-groupe borné de $(\mathbb{C}^*, \times)$, c'est à dire qu'il existe $M > 0$ tel que pour tout $z \in G$, $|z| \leqslant M$.

1. Donner deux exemples de sous-groupes bornés de $\mathbb{C}^*$ et un exemple de sous-groupe non borné distinct de $\mathbb{C}^*$.

Le but de la suite de l'exercice est de démontrer que $G \subset \mathbb{U}$, le groupe des nombres complexes de module 1. Soit $z \in G$.

2. On suppose que $|z| > 1$. Que dire de la limite de la suite $(|z^n|)_{n\in\mathbb{N}}$? Conclure à une contradiction.

3. Traiter le cas où $|z| < 1$ et conclure.

Exercice 18 (Description des sous-groupes de $\mathbb{U}_n$, difficile) Soit $n \in \mathbb{N}^*$.

1. Démontrer que $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

2. Soit $d \in \mathbb{N}^*$.

   (a) Démontrer que si d divise n, alors $\mathbb{U}_d \subset \mathbb{U}_n$.

   (b) Démontrer ensuite que la réciproque est vraie en considérant $z = \mathrm{e}^{i\frac{2\pi}{d}}$.

3. En déduire à l'aide du théorème de Lagrange démontré à l'exercice 19 que les sous-groupes de $\mathbb{U}_n$ sont les groupes de la forme $\mathbb{U}_d$ avec $d \mid n$.

4. Déterminer le nombre de sous-groupes de $\mathbb{U}_{720}$.

Exercice 19 (Un théorème de Lagrange, difficile) Soit $(G, \bullet)$ un groupe commutatif de cardinal n.

1. Soit $g \in G$. Démontrer que l'application $\phi : G \to G$ définie par $\phi(x) = g \bullet x$ est une bijection. Comparer ainsi les ensembles G et $\{gx \mid x \in G\}$.

2. En déduire que $g^n = 1$ en calculant de deux façons différentes le produit $\prod_{x\in G} gx$.

3. En déduire les sous-groupes finis de $\mathbb{C}^*$.

Remarque : vous montrerez l'année prochaine que ce résultat reste vrai même si G n'est pas commutatif.

6 Anneaux

Exercice 20 Parmi les ensembles suivants lesquels sont des anneaux ou des corps :

1. $\mathbb{Z}, \mathbb{Q}$, l'ensemble des irrationnels.

2. l'ensemble des nombres décimaux.

Exercice 21 On note $\mathbb{D}_2 = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$ l'ensemble des nombres dyadiques. C'est un sous-anneau de $\mathbb{R}$. Déterminer ses éléments inversibles.

Exercice 22 (Exemples matriciels) Indiquer si les ensembles suivants sont des anneaux ou des corps.

1. l'ensemble $\mathcal{D}_n(\mathbb{K})$ des matrices diagonales de $\mathcal{M}_n(\mathbb{K})$ et $\mathcal{D}^*{}_n(\mathbb{K})$ l'ensemble des matrices diagonales de $\mathcal{M}_n(\mathbb{K})$ dont les coefficients diagonaux sont non nuls.

2. l'ensemble des matrices triangulaires supérieures de $\mathcal{M}_n(\mathbb{K})$.

Exercice 23 (Une équation de Pell-Fermat) On note $A = \{a + b\sqrt{5} \mid (a,b) \in \mathbb{Z}^2\}$.

1. Montrer que $(A, +, \times)$ est un sous-anneau de $\mathbb{R}$.
2. Soit $N : A \to \mathbb{Z}$ définie par $N(a + b\sqrt{5}) = a^2 - 5b^2$. Montrer que N est multiplicative, c'est-à-dire pour tous x, y de K, $N(xy) = N(x)N(y)$.
3. Démontrer que $x \in A$ est inversible dans K si et seulement si $N(x)$ vaut ± 1.
4. On pose $x = 9 + 4\sqrt{5}$. Calculer pour tout $n \in \mathbb{N}^*$, $N(x^n)$.
5. Application : donner trois couples d'entiers naturels (a, b) solutions de l'équation de Pell-Fermat $a^2 - 5b^2 = 1$.

Exercice 24 Démontrer que $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ est un corps.

Exercice 25 (Eléments nilpotents) Soit $(A, +, \times)$ un anneau. On dit que $a \in A$ est nilpotent s'il existe un entier naturel n tel que $a^n = 0$.

1. Quels sont les nilpotents de l'anneau $\mathbb{R}$? de l'anneau $\mathbb{Z}/4\mathbb{Z}$? Exhiber une infinité d'éléments nilpotents de $\mathcal{M}_n(\mathbb{K})$.
2. Un élément nilpotent peut-il être inversible ?
3. Soit a et b deux éléments de A qui commutent.
   (a) Démontrer que $\forall n \in \mathbb{N},\ (ab)^n = a^n b^n$.
   (b) On suppose de plus que a et b sont nilpotents. Démontrer que ab et $a+b$ sont encore nilpotents.

7 Un peu de géométrie

Exercice 26 On se place dans $(G, \circ)$ le groupe des bijections de $\mathbb{R}^2$ et on considère les symétries orthogonales $s : (x, y) \mapsto (y, x)$ et $s' : (x, y) \mapsto (x, -y)$.

1. Calculer $s^2 \circ s'^2$ et $(s \circ s')^2$. Commenter.
2. On pose $r = s \circ s'$. Reconnaître la transformation géométrique r (si le point M a pour affixe z, on pourra exprimer l'affixe de $r(M)$ en fonction de z), en déduire r^2, r^4 puis r^3.

Exercice 27 (un modèle géométrique du groupe de Klein) On munit le plan d'un repère orthonormé, d et d' sont l'axe des abscisses et l'axe des ordonnées. On note s_d et $s_{d'}$ les symétries orthogonales par rapport à d et d'. On note $G = \{\mathrm{id}, s_d, s_{d'}, -\mathrm{id}\}$.

1. Soit M un point du plan de coordonnées (x, y). Donner les coordonnées du point $s_d \circ s'_d(M)$. Que vaut $s_d \circ s'_d$?
2. Démontrer que $(G, \circ)$ est un groupe commutatif.
3. Est-il isomorphe au groupe des racines quatrièmes de l'unité qui lui aussi possède 4 éléments ? On pourra calculer les carrés de chaque élément.