

1 LOIS DE COMPOSITION INTERNES

1 Pour tout $(x, y) \in [0, 1] \times [0, 1]$, on pose :

$$x \star y = x + y - xy.$$

- 1) Montrer que $([0, 1], \star)$ est un magma commutatif et associatif.
- 2) Montrer que $([0, 1], \star)$ possède un élément neutre.
- 3) Quels sont les éléments inversibles de $([0, 1], \star)$?

2 Soient E un ensemble et \preccurlyeq une relation d'ordre totale sur E . Cette relation étant totale, $\max\{x, y\}$ est bien défini pour tous $x, y \in E$.

- 1) Montrer que le magma (E, \max) est associatif et commutatif.
- 2) À quelle condition nécessaire et suffisante (E, \max) possède-t-il un élément neutre ?
- 3) Si (E, \max) possède un élément neutre, quels sont ses éléments inversibles ?

3 Soit E un ensemble à au moins trois éléments. Montrer qu'alors S_E est non commutatif.

2 STRUCTURE DE GROUPE

4 Pour tous $x, y \in]-1, 1[$, on pose :

$$x \oplus y = \frac{x + y}{1 + xy}.$$

- 1) Montrer que \oplus est une loi interne sur $]-1, 1[$.
- 2) Montrer que $(]-1, 1[, \oplus)$ est un groupe commutatif.

5 Pour tous $(x, y), (x', y') \in \mathbb{R}^* \times \mathbb{R}$, on pose :

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

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

6 Soit $p \in \mathbb{N}^*$ fixé. Montrer que l'ensemble des $e^{\frac{2ik\pi}{p^n}}$, (k, n) décrivant $\mathbb{Z} \times \mathbb{N}$, est un sous-groupe de \mathbb{C}^* .

7 Montrer que $\{z \in \mathbb{C} / \exists n \in \mathbb{N}^* / z^n = 1\}$ est un sous-groupe de \mathbb{C}^* .

8 Montrer que l'ensemble des fonctions $z \mapsto az + b$, (a, b) décrivant $\mathbb{C}^* \times \mathbb{C}$, est un groupe pour la composition.

9 Soit $n \in \mathbb{N}^*$. On note G l'ensemble des permutations $\sigma \in S_{[1, n]}$ telles que pour tout $k \in [1, n]$:

$$\sigma(n - k + 1) = n - \sigma(k) + 1.$$

Montrer que G est un sous-groupe de $S_{[1, n]}$.

10 On introduit six fonctions de $\mathbb{R} \setminus \{0, 1\}$ dans \mathbb{R} définies pour tout $x \in \mathbb{R} \setminus \{0, 1\}$ par :

$$a(x) = x, \quad b(x) = 1 - x, \quad c(x) = \frac{1}{x},$$

$$d(x) = \frac{x}{x-1}, \quad e(x) = \frac{x-1}{x} \quad \text{et} \quad f(x) = \frac{1}{1-x}.$$

Montrer que $\{a, b, c, d, e, f\}$ est un sous-groupe de $S_{\mathbb{R} \setminus \{0, 1\}}$ dont on déterminera la table.

11 Soit G un groupe.

- 1) Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G indexée par un ensemble I . Montrer que $\bigcap_{i \in I} H_i$ est un sous-groupe de G .
- 2) Soit $x \in G$. On appelle *centralisateur de x dans G* , noté $C_G(x)$, l'ensemble des éléments de G qui commutent à x . Montrer que $C_G(x)$ est un sous-groupe de G .
- 3) On appelle *centre de G* et on note $Z(G)$ l'ensemble des éléments de G qui commutent à TOUT élément de G . Montrer que $Z(G)$ est un sous-groupe de G .

12 1) Trouver deux sous-groupes de \mathbb{R}^* dont la réunion n'est PAS un sous-groupe de \mathbb{R}^* .

- 2) Soient G un groupe et $(H_n)_{n \in \mathbb{N}}$ une suite CROISSANTE de sous-groupes de G . Montrer que $\bigcup_{n \in \mathbb{N}} H_n$ est un sous-groupe de G .

13 Soient G un groupe et H un sous-groupe de G .

- 1) Soit $x \in G$. On pose : $xHx^{-1} = \{xhx^{-1}\}_{h \in H}$. Montrer que xHx^{-1} est un sous-groupe de G .
- 2) On pose : $H_G = \bigcap_{x \in G} xHx^{-1}$.
 - a) Montrer que H_G est un sous-groupe de G .
 - b) Montrer que pour tout $x \in G$: $xH_Gx^{-1} = H_G$.

14 1) Soient G un groupe commutatif fini de cardinal n et $g \in G$.

- a) Montrer que l'application $x \mapsto gx$ est bijective de G sur G .
- b) Montrer, en calculant de deux manières le produit : $\prod_{x \in G} (gx)$, que : $g^n = 1_G$. Ce résultat est un cas particulier d'un théorème essentiel — le *théorème de Lagrange*.

2) Déterminer tous les sous-groupes finis de \mathbb{C}^* .

15 Soit G un groupe.

- 1) \odot On suppose que pour tout $x \in G$: $x^2 = 1_G$. Montrer que G est commutatif.
 - 2) $\odot \odot$ On suppose que : $(xy)^3 = x^3y^3$ pour tous $x, y \in G$ et tout élément de G peut être écrit comme un cube.
 - a) Montrer que pour tous $x, y \in G$:

$$x^3y^2 = y^2x^3.$$
 - b) En déduire que pour tout $x \in G$, x^2 commute à tout élément de G .
 - c) En déduire que G est commutatif.
-

16 \odot Soit G un groupe. On définit une relation binaire \sim sur G pour tous $x, y \in G$ par :

$$x \sim y \iff \exists g \in G / y = g^{-1}xg.$$

Montrer que \sim est une relation d'équivalence sur G .

3 STRUCTURE D'ANNEAU

17 \odot On note A l'ensemble des matrices de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}$, λ décrivant \mathbb{R} . Montrer que A est stable par différence et produit, mais n'est pas un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.

18 \odot Montrer que $\mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3}\}_{a,b \in \mathbb{Q}}$ est un corps.

19 \odot On note A l'ensemble des matrices $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, a et b décrivant \mathbb{Z} .

- 1) Montrer que A est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$.
- 2) Déterminer $U(A)$.

20 1) On note A l'ensemble des rationnels $\frac{p}{2^n}$, (p, n) décrivant $\mathbb{Z} \times \mathbb{N}$.

- a) \odot Montrer que A est un sous-anneau de \mathbb{Q} .
- b) $\odot \odot$ Déterminer $U(A)$.

 2) $\odot \odot$ Mêmes questions avec l'ensemble \mathbb{D} des décimaux.

21 1) $\odot \odot$ On rappelle que $\mathbb{Z}[i] = \{a+ib\}_{a,b \in \mathbb{Z}}$ est un sous-anneau de \mathbb{C} . Montrer que pour tout $z \in \mathbb{Z}[i]$: $|z|^2 \in \mathbb{N}$, puis en déduire $U(\mathbb{Z}[i])$.

2) a) \odot Montrer que $\mathbb{Z}[i\sqrt{2}] = \{a+ib\sqrt{2}\}_{a,b \in \mathbb{Z}}$ est un sous-anneau de \mathbb{C} .
 b) $\odot \odot$ Déterminer $U(\mathbb{Z}[i\sqrt{2}])$.

22 $\odot \odot$ On rappelle que pour tous $f, g \in \mathbb{R}^{\mathbb{R}}$, les fonctions $f+g$ et $f \times g$ sont définies pour tout $x \in \mathbb{R}$ par :

$$(f+g)(x) = f(x) + g(x) \quad \text{et} \quad (f \times g)(x) = f(x)g(x).$$

- 1) Montrer que $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau commutatif. Est-il intègre ?
 - 2) Montrer que $\mathcal{C}(\mathbb{R}, \mathbb{R})$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.
 - 3) Déterminer $U(\mathbb{R}^{\mathbb{R}})$.
-

23 $\odot \odot \odot$

- 1) Montrer que \mathbb{Z} est le seul sous-anneau de \mathbb{Z} .
- 2) On s'intéresse à présent aux sous-groupes de \mathbb{Z} .
 - a) \odot Montrer que $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} pour tout $n \in \mathbb{N}$.
 - b) Montrer que tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$.
- 3) Soient $a, b \in \mathbb{Z}$. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de \mathbb{Z} . En particulier : $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$ d'après 2). Montrer qu'en réalité : $d = a \wedge b$.

24 $\odot \odot$ Soient A et B deux anneaux. On pose pour tous $(a, b), (a', b') \in A \times B$: $(a, b) + (a', b') = (a+a', b+b')$ et $(a, b) \times (a', b') = (aa', bb')$.

- 1) Montrer que $(A \times B, +, \times)$ est un anneau.
 - 2) Montrer que si A et B sont non nuls, alors $A \times B$ n'est pas intègre.
-

25 $\odot \odot \odot$ Soit E un ensemble. Pour tous $A, B \in \mathcal{P}(E)$, on appelle *différence symétrique* de A et B , notée $A \Delta B$, l'ensemble $(A \setminus B) \cup (B \setminus A)$.

1) Montrer que pour tous $A, B \in \mathcal{P}(E)$:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

- 2) Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
 - 3) Déterminer $U(\mathcal{P}(E))$.
 - 4) L'anneau $(\mathcal{P}(E), \Delta, \cap)$ est-il intègre ?
 - 5) Soit F une partie de E . Montrer que $\mathcal{P}(F)$ n'est pas loin d'être un sous-anneau de $\mathcal{P}(E)$. Quelle propriété lui manque-t-il ?
-

26 Soit A un anneau. Un élément $x \in A$ est dit *nilpotent* si : $x^n = 0_A$ pour un certain $n \in \mathbb{N}^*$.

- 1) Si A est intègre, montrer que 0_A est le seul élément nilpotent de A .

- 2) Montrer que la somme et le produit de deux éléments nilpotents de A QUI COMMUTENT sont encore nilpotents.
 - 3) Pour tout $x \in A$ nilpotent, montrer que $1_A - x$ est inversible et déterminer $(1_A - x)^{-1}$.
-

27 ☺☺ Soit A un anneau intègre. Pour tous $a, b \in A$, on dit que a divise b (dans A), ce qu'on note : $a|b$, si : $b = ak$ pour un certain $k \in A$. Montrer que pour tous $a, b \in A$:

$$a|b \text{ et } b|a \iff \exists u \in U(A) / b = au.$$

28 ☺☺ Soit A un anneau de Boole, i.e. un anneau non nul tel que pour tout $x \in A$: $x^2 = x$.

- 1) a) Montrer que pour tous $x, y \in A$: $2x = 0_A$ et $yx = -xy$.
 - b) En déduire que A est commutatif.
 - 2) Déterminer A dans le cas où A est intègre.
 - 3) On définit une relation binaire \preceq sur A en posant pour tous $x, y \in A$: $x \preceq y \iff yx = x$. Montrer que \preceq est une relation d'ordre.
-

29 Soit A un anneau.

- 1) ☺ On appelle *centre de A* et on note $Z(A)$ l'ensemble des éléments de A qui commutent à TOUT élément de A . Montrer que $Z(A)$ est un sous-anneau de A .
- 2) ☺☺☺ On suppose que : $x^3 = x$ pour tout $x \in A$.
 - a) Montrer que pour tous $x, y \in A$:

$$xy = 0_A \implies yx = 0_A.$$
 - b) Soit $x \in A$. On suppose que : $x^2 = x$. Montrer que : $x \in Z(A)$ en étudiant $x(y - xy)$ pour tout $y \in A$.
 - c) Montrer que pour tout $x \in A$: $x^2 \in Z(A)$.
 - d) Montrer enfin que A est commutatif.

On peut montrer plus généralement — mais c'est très difficile — que si : $\forall x \in A, \exists n \geq 2 / x^n = x$, alors A est commutatif (théorème de Jacobson).

4 ARITHMÉTIQUE MODULAIRE

30 ☺ Résoudre les équations suivantes d'inconnue $x \in \mathbb{Z}$:

- 1) $5\bar{x} = \bar{2}$ dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$, puis dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$.
 - 2) $\bar{x}^2 = \bar{3}$ dans $\frac{\mathbb{Z}}{5\mathbb{Z}}$, puis dans $\frac{\mathbb{Z}}{11\mathbb{Z}}$.
 - 3) $\bar{x}^2 + 3\bar{x} + \bar{1} = \bar{0}$ dans $\frac{\mathbb{Z}}{7\mathbb{Z}}$.
 - 4) $\bar{x}^2 + \bar{x} = \bar{2}$ dans $\frac{\mathbb{Z}}{9\mathbb{Z}}$, puis dans $\frac{\mathbb{Z}}{21\mathbb{Z}}$.
-

31 ☺☺ Soit $p \in \mathbb{P}$. Effectuer le produit de tous les éléments de $U\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$ et en déduire le *théorème de Wilson* :

$$(p-1)! \equiv -1 [p].$$
