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

---

2 Soient E un ensemble et $\preccurlyeq$ une relation d'ordre totale sur E.
1) Pour tous $x, y \in E$, justifier l'existence de $\max\{x,y\}$.
2) Montrer que le magma $(E, \max)$ est associatif et commutatif.
3) À quelle condition nécessaire et suffisante $(E, \max)$ possède-t-il un élément neutre ?
4) 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 $x, y \in \left]-1,1\right[$, on pose :

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

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

---

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

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

1) Montrer que $\big(\mathbb{R}^* \times \mathbb{R}, \star\big)$ 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 $\left\{z \in \mathbb{C} / \quad \exists\, n \in \mathbb{N}^* / \quad z^n = 1\right\}$ est un sous-groupe de $\mathbb{C}^*$.

---

8 Montrer que l'ensemble des fonctions $z \longmapsto az+b$, (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 :

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

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

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 $\mathrm{C}_G(x)$, l'ensemble des éléments de G qui commutent à x. Montrer que $\mathrm{C}_G(x)$ est un sous-groupe de G.
3) On appelle *centre de G* et on note $\mathrm{Z}(G)$ l'ensemble des éléments de G qui commutent à TOUT élément de G. Montrer que $\mathrm{Z}(G)$ 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 : $\quad xHx^{-1} = \left\{xhx^{-1}\right\}_{h\in H}$. Montrer que xHx^{-1} est un sous-groupe de G.
2) On pose : $\quad H_G = \bigcap_{x\in G} xHx^{-1}$.
   a) Montrer que H_G est un sous-groupe de G.
   b) Montrer que pour tout $x \in G$: $\quad xH_Gx^{-1} = H_G$.

14
1) Soient G un groupe commutatif fini de cardinal n et $g \in G$.
   a) Montrer que l'application $x \longmapsto gx$ 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) ◷ On suppose que : $x^2 = 1_G$ pour tout $x \in G$. Montrer que G est commutatif.

2) ◷◷ 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 : $x^3y^2 = y^2x^3$ pour tous $x, y \in G$.

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

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

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

---

3 STRUCTURE D'ANNEAU

17 ◷ 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. L'ensemble A est-il un sous-anneau de $\mathscr{M}_2(\mathbb{R})$?

18

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

a) ◷ Montrer que A est un sous-anneau de $\mathbb{Q}$.

b) ◷◷ Déterminer $U(A)$.

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

---

19 ◷◷

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

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

b) Déterminer $U(\mathbb{Z}[\mathrm{i}\sqrt{2}])$.

---

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

---

21 ◷ On note $\mathscr{C}$ l'ensemble des matrices $\begin{pmatrix}a & -b\\ b & a\end{pmatrix}$, a et b décrivant $\mathbb{K}$.

1) Montrer que $\mathscr{C}$ est un sous-anneau de $\mathscr{M}_2(\mathbb{K})$.

2) $\mathscr{C}$ est-il un corps ?

---

22 ◷◷ 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 $\mathscr{C}(\mathbb{R},\mathbb{R})$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$.

3) Déterminer $U(\mathbb{R}^{\mathbb{R}})$.

---

23 ◷◷◷

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

$$\text{et} \quad (a,b)\times(a',b') = (aa', bb').$$

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

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

$$A\,\triangle\,B = (A\cup B)\setminus(A\cap B).$$

2) Montrer que $(\mathscr{P}(E), \triangle, \cap)$ est un anneau commutatif.

3) Déterminer $U(\mathscr{P}(E))$.

4) L'anneau $(\mathscr{P}(E), \triangle, \cap)$ est-il intègre ?

5) Soit F une partie de E. Montrer que $\mathscr{P}(F)$ n'est pas loin d'être un sous-anneau de $\mathscr{P}(E)$. 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 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 $\preccurlyeq$ sur A en posant pour tous $x, y \in A$: $x \preccurlyeq y \iff yx = x$. Montrer que $\preccurlyeq$ est une relation d'ordre.

---

28 Soit A un anneau.
1) ◷ On appelle *centre de A* et on note $\mathrm{Z}(A)$ l'ensemble des éléments de A qui commutent à **tout** élément de A. Montrer que $\mathrm{Z}(A)$ 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 : $x \in \mathrm{Z}(A)$ en étudiant $x(y - xy)$ pour tout $y \in A$.
c) Montrer que pour tout $x \in A$: $x^2 \in \mathrm{Z}(A)$.
d) Montrer enfin que A est commutatif.

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

---

4 Arithmétique modulaire

29 ◷ Résoudre les équations suivantes d'inconnue $x \in \mathbb{Z}$:
1) $\overline{5}\,\overline{x} = \overline{2}$ dans $\dfrac{\mathbb{Z}}{7\mathbb{Z}}$, puis dans $\dfrac{\mathbb{Z}}{10\mathbb{Z}}$.
2) $\overline{x}^2 = \overline{3}$ dans $\dfrac{\mathbb{Z}}{5\mathbb{Z}}$, puis dans $\dfrac{\mathbb{Z}}{11\mathbb{Z}}$.
3) $\overline{x}^2 + \overline{3}\,\overline{x} + \overline{1} = \overline{0}$ dans $\dfrac{\mathbb{Z}}{7\mathbb{Z}}$.
4) $\overline{x}^2 + \overline{x} = \overline{2}$ dans $\dfrac{\mathbb{Z}}{9\mathbb{Z}}$, puis dans $\dfrac{\mathbb{Z}}{21\mathbb{Z}}$.

---

30 ◷◷ Soit $p \in \mathbb{P}$. Effectuer le produit de tous les éléments de $U\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)$ et en déduire le *théorème de Wilson* :
$$(p-1)! \equiv -1 \ [p].$$
