La chute des titans, Giulio romano

I. Lois de composition internes et groupes

1 — *La structure de groupe produit*

Soit $(G,\star)$ et $(H,\diamond)$ deux groupes. Pour tous couples (g,h) et (g',h') du produit cartésien $G\times H$, on pose

$$(g,h)\otimes(g',h') := (g\star g', h\diamond h')$$

Montrer que $(G\times H,\otimes)$ est un groupe.

2 — *Une question ouverte* f

Sur $E := [-1,+1]$, on définit $x\star y := x\sqrt{1-y^2}+y\sqrt{1-x^2}$.

1. Vérifier que E est stable par $\star$.

2. Le magma $(E,\star)$ est-il un groupe ?

3 — *Un exemple*

Sur $I=[0,1[$, on considère sur la loi de composition $\star$ définie par $x\star y = x+y-\lfloor x+y\rfloor$. Montrer finalement que $(I,\star)$ est un groupe.

4 — *Théorème de Lagrange* ff

Soit G un groupe de cardinal fini et H un sous-groupe de G. Pour tout y dans G, on pose

$$yH := \{yh;\ h\in H\}$$

1. Pour $(x,y)\in G^2$, on dit que $x\mathscr{R}y$ si $x\in yH$. Vérifier que $\mathscr{R}$ est une relation d'équivalence sur G.

2. Pour $x\in G$, déterminer la classe d'équivalence de x et vérifier qu'elle a le même cardinal que H.

3. En déduire que $|H|$ divise $|G|$.

5 — *Groupes d'exposant deux* f

Soit G un groupe tel que $\forall g\in G,\ g^2=e$.

1. Montrer que G est commutatif.

2. Trouver des exemples de groupes G finis et infinis vérifiant $\forall g\in G,\ g^2=e$.

6 — *Parties finies de* $\mathbb{C}^*$ *stables par le produit*

Soit A une partie non vide de $\mathbb{C}^*$ stable par le produit et de cardinal fini n.

1. Soit $a\in A$. Établir que $x\mapsto ax$ est une bijection de A sur lui-même.

2. En déduire que $\forall a\in A,\ a^n=1$.

3. En déduire que $A=\mathbb{U}_n$, où $\mathbb{U}_n$ désigne le sous-groupe multiplicatif des racines n-ièmes de l'unité.

II. Anneaux et corps

7 — *Anneaux de Boole* ƒ

Soit E un ensemble et $\mathbb{A}$ l'anneau $\left(\mathscr{P}(E), \Delta, \cap\right)$ où $A\Delta B = (A \cup B) \setminus (A \cap B)$ pour toutes parties A et B de E.

1. Montrer que $\mathbb{A}$ est un anneau commutatif.
2. À quelle condition sur E cet anneau est-il un corps ? Est-il intègre ?
3. Soit A et B appartenant à $\mathbb{A}$. Résoudre l'équation $A\Delta X = B$ dans $\mathbb{A}$.

8 — *Produit de deux corps*

Soit $(\mathbb{k}, +, \times)$ un corps. Pour tous couples (a, b) et (c, d) d'éléments de $\mathbb{k}$ on pose

$$(a, b) \oplus (c, d) := (a + c, b + d) \quad \text{et} \quad (a, b) \star (c, d) := (a \times c, b \times d)$$

1. Vérifier que $\left(\mathbb{k}^2, \oplus, \star\right)$ est un anneau commutatif.
2. L'anneau $\left(\mathbb{k}^2, \oplus, \star\right)$ est-il un corps ?

9 — *Anneau des décimaux*

Soit $\mathbb{D} := \left\{x \in \mathbb{Q} ; \exists n \in \mathbb{N}, 10^n x \in \mathbb{Z}\right\}$.

1. Montrer que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.
2. Déterminer le groupe $\mathbb{D}^\times$ des inversibles de l'anneau $\mathbb{D}$.

10 — *Unités de l'anneau* $\mathbb{Z}[j]$ ƒƒ

On rappelle la notation usuelle $j = e^{2i\pi/3}$ et on pose $\mathbb{Z}[j] = \left\{x + jy ; (x, y) \in \mathbb{Z}^2\right\}$.

1. Montrer que $\mathbb{Z}[j]$ est un sous-anneau de $(\mathbb{C}, +, \times)$. Est-ce un sous-corps de $(\mathbb{C}, +, \times)$?
2. Vérifier que $\forall z \in \mathbb{Z}[j], |z|^2 \in \mathbb{N}$.
3. On note $U\left(\mathbb{Z}[j]\right)$ l'ensemble des éléments de l'anneau $\left(\mathbb{Z}[j], +, \times\right)$ inversibles pour la loi $\times$.
   a. Montrer que $U\left(\mathbb{Z}[j]\right) = \mathbb{Z}[j] \cap \mathbb{U}$.
   b. Déterminer l'ensemble $\mathbb{U}_6$ des racines sixièmes de l'unité.
   c. Montrer que $U\left(\mathbb{Z}[j]\right) = \mathbb{U}_6$.

III. Problème

11 — *Anneaux $\mathbb{Z}/n\mathbb{Z}$ et corps $\mathbb{F}_p$* ff

Soit $n \in \mathbb{N}^*$. On sait que la relation $\mathscr{R}$ définie sur $\mathbb{Z}$ par $x \equiv y\,[n]$ est une relation d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de cette relation, i.e. l'ensemble des classes d'équivalences $\overline{x}$ de cette relation.

Partie I – Préliminaires sur les anneaux $\mathbb{Z}/n\mathbb{Z}$

1. Établir que $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \dots, \overline{n-1}\right\}$. Quel est le cardinal de $\mathbb{Z}/n\mathbb{Z}$?

2. Démontrer que les relations suivantes définissent bien des opérations internes sur $\mathbb{Z}/n\mathbb{Z}$:

$$\forall (k,\ell) \in \mathbb{Z}^2,\ \overline{k} + \overline{\ell} := \overline{k+\ell} \quad \text{et} \quad \overline{k} \times \overline{\ell} := \overline{k\ell} \quad (\text{aussi noté } \overline{k}\,\overline{\ell}\,)$$

3. Déterminer les tables de Cayley des opérations + et × de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

4. Montrer que $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ a une structure d'anneau commutatif.

5. Établir que $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un corps *si et seulement si* n est premier.

6. Donner une condition nécessaire et suffisante d'intégrité de l'anneau $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$.

Partie II – Carrés du corps $\mathbb{F}_p$ et équations du second degré

Dans cette question, on fixe un nombre premier p et on note $\mathbb{F}_p$ le corps $\left(\mathbb{Z}/p\mathbb{Z}, +, \times\right)$.

1. On appelle carré de $\mathbb{F}_p$ tout élément de la forme a^2 où $a \in \mathbb{F}_p$.

On dit que $\ell \in \mathbb{Z}$ est un carré modulo p si $\overline{\ell}$ est un carré de $\mathbb{F}_p$, i.e. si $\exists\, k \in [\![0, p-1]\!]$ vérifiant $k^2 \equiv \ell\,[p]$.

a. Déterminer les carrés de $\mathbb{F}_3$ et $\mathbb{F}_5$.

b. Pour tout $(a,b) \in \mathbb{F}_p^2$, on note $a\mathscr{R}b$ la propriété $a^2 = b^2$.

Vérifier que $\mathscr{R}$ est une relation d'équivalence sur l'ensemble $\mathbb{F}_p$.

c. Déterminer la classe d'équivalence $c\ell(a)$ d'un élément a de $\mathbb{F}_p$.

d. En déduire le nombre de carrés de $\mathbb{F}_p$.

2. Dans cette question, on s'intéresse au cas où $p = 5$.

a. Déterminer les carrés de $\mathbb{F}_5$.

b. Résoudre l'équation $x^2 + 2x + \overline{4} = 0$ dans $\mathbb{F}_5$.

c. Plus généralement, résoudre $x^2 + px + \overline{q} = 0$ dans $\mathbb{F}_5$ où $(p,q) \in \mathbb{Z}^2$.

INDICATION : Mettre sous forme canonique le trinôme $x^2 + px + \overline{q}$ nécessite le calcul de l'inverse de $\overline{2}$ dans $\mathbb{F}_5$.

3. Résoudre l'équation $x^2 + 2x + \overline{4} = 0$ dans $\mathbb{Z}/6\mathbb{Z}$.

Partie III – Théorèmes de Fermat et de Wilson

On fixe p premier.

1. On pose $\pi := \overline{(p-1)!}$ (classe modulo p).

a. Soit $x \in \mathbb{Z}$ tel que $x \wedge p = 1$. Justifier que l'application suivante est bien définie et bijective :

$$\tau_x : \mathbb{F}_p^* \to \mathbb{F}_p^* \quad \text{et} \quad u \mapsto \overline{x}\, u$$

b. En déduire que $\overline{x}^{p-1}\pi = \pi$ puis que $\forall a \in \mathbb{F}_p,\ a^p = a$ (petit théorème de Fermat).

2. L'objectif de cette question est d'établir le théorème de Wilson :

$$\text{Pour tout } n \in \mathbb{N} \text{ tel que } n \geqslant 2\ ,\quad n \text{ est premier} \iff (n-1)! \equiv -1\,[n]$$

a. Démontrer le sens indirect par contraposition.

b. On suppose dans cette question que $p \geqslant 2$ est premier. Démontrer que, dans $\mathbb{F}_p$,

$$\overline{(p-1)!} = \overline{-1}$$

puis conclure.

INDICATION : Dans le cas où $p \geqslant 3$, regrouper les éléments de $\mathbb{F}_p^*$ par paires d'inverses.

3. Soit $p \in \mathbb{P} \setminus \{2\}$. Nous allons démontrer que -1 est un carré modulo p *si et seulement si* $p \equiv 1\,[4]$.

a. On suppose l'existence de $x \in \mathbb{F}_p$ tel que $x^2 = \overline{-1}$. Déduire du petit théorème de Fermat que $p \equiv 1\,[4]$.

b. On suppose que $p \equiv 1\,[4]$. Déduire du théorème de Wilson que $\overline{-1}$ est un carré de $\mathbb{F}_p$.

IV. Indications

1

Aucune difficulté particulière : vérifier les axiomes de la structure de groupe. Il est clair que (e_G, e_H) est un neutre pour $\otimes$, où e_G et e_H sont les neutres respectifs de G et H.

2

On peut par exemple appliquer l'inégalité de Cauchy-Schwarz au 1.

3

L'inverse de x vaut $1-x$ si $x \neq 0$...

4

On se souviendra que G est la réunion disjointe des classes d'équivalence de $\mathscr{R}$.

5

On pourra songer à la différence symétrique pour la deuxième question.

6

Utiliser les cardinaux pour la dernière question.

7

Rappel : $A\Delta B = \left(\overline{A} \cap B\right) \cup \left(A \cap \overline{B}\right)$.

8

La réponse à la dernière question est non.

9

Revenir à la caractérisation des sous-anneaux du cours.

10

Procéder par double inclusion à la dernière question.

11

Pour établir que $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un corps dans le cas où n est premier, on pourra utiliser une relation de Bezout.