TD 12 Structures algébriques

Exercice 1: ★

Soient les quatre fonctions de $\mathbb{R}^*$ dans $\mathbb{R}^*$ définies par

$$f_1(x) = x, \quad \frac{1}{x}, \quad f_3(x) = -x, \quad f_4(x) = -\frac{1}{x}.$$

Montrer que $(\{f_1, f_2, f_3, f_4\}, \circ)$ est un groupe.

Exercice 2: ★★★

Soit $(G, .)$ un groupe.

(1) Montrer que les propositions suivantes sont équivalentes.

i. G est abélien ;

ii. Pour tout $a, b \in G$, $(ab)^2 = a^2b^2$;

iii. Pour tout $a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$

(2) En déduire que si pour tout $x \in G$, $x^2 = e$, alors G est abélien.

Exercice 3: ★★★

Montrer que les groupes multiplicatifs $\mathbb{R}^*$ et $\mathbb{C}^*$ ne sont pas isomorphes.

Exercice 4: ★

Les couples $(E, \times)$ suivants sont-ils des groupes ?

(1) $E = \{z \in \mathbb{C} \mid |z| = 2\}$, $\times$ la multiplication usuelle ;

(2) $E = \mathbb{R}^+$, $\times$ la multiplication usuelle ;

(3) $E = \{x \in \mathbb{R} \mapsto ax + b \mid a, b \in \mathbb{R}\}$, $\times$ la composition des applications.

Exercice 5: ★★★

Soit H un sous-groupe de $(\mathbb{Z}, +)$. Montrer qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Exercice 6: ★★

Quel est le plus petit sous-groupe de $(\mathbb{R}, +)$ contenant 1 ? contenant 2 ?

Exercice 7: ★★★

Les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*, \times)$ sont-ils isomorphes ?

Exercice 8: ★★

Soit $(G, +)$ un groupe commutatif. On note $End(G)$ l'ensemble des endomorphismes de G sur lequel on définit la loi $+$ par $f + g : x \in G \mapsto f(x) + g(x)$.

Montrer que $(End(G), +, \circ)$ est un anneau.

Exercice 9: ★★★

Soit $(A, +, \times)$ un anneau. On dit que $x \in A$ est *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

(1) Soit $x \in A$ nilpotent. Montrer que $1 - x$ est inversible.

(2) Soient x et y deux éléments nilpotents de A tels que $x \times y = y \times x$. Montrer que $x + y$ et $x \times y$ sont nilpotents.

(3) Un corps admet-il des éléments nilpotents ?

Exercice 10: ★★

On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ tet déterminer ses éléments inversibles.

Exercice 11: ★★★

Soit A un sous-anneau de $\mathbb{R}$. Montrer que A est dense dans $\mathbb{R}$ si et seulement si $A \cap]0, 1[\neq \emptyset$.

Exercice 12: ★★★

Soit G un sous-groupe additif non nul de $\mathbb{R}$ et $a = \inf(G \cap \mathbb{R}_*^+)$.

(1) Montrer que si $a \in G \in \mathbb{R}_+^*$, alors $G = a\mathbb{Z}$.

(2) Montrer que si $a \notin (G \cap \mathbb{R}_+^*)$ alors $a = 0$ et G est dense dans $\mathbb{R}$.

Exercice 13: ★★

Soit $(A, +, \times)$ un anneau. On appelle *centre* de A l'ensemble $C = \{x \in A \mid \forall y \in A,\ x \times y = y \times x\}$. Montrer que C est un sous-anneau de A.

Exercice 14: ★

Soit $A = \left\{ \frac{p}{2^q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$.

(1) Montrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.

(2) Déterminer les éléments inversibles de A.

Exercice 15: ★★★

Soit $f : \mathbb{C} \to \mathbb{C}$ un morphisme d'anneaux tel que pour tout $x \in \mathbb{R}$, $f(x) = x$. Montrer que f est l'identité ou la conjugaison complexe.

Exercice 16: ★★★ théorème de Wilson

Soit p un nombre premier. On considère l'ensemble $\mathcal{F}_p = [\![0, p-1]\!]$ muni des deux lois $\oplus$ et $\otimes$ définies de la façon suivante. Pour $a, b \in \mathcal{F}_p$, on note $a \oplus b$ le reste de la division de $a + b$ par p, et $a \otimes b$ le reste de la division de ab par p.

(1) Montrer que $(\mathcal{F}_p, \oplus, \otimes)$ est un corps.

(2) Montrer que 1 et $p - 1$ sont les seuls éléments de $\mathcal{F}_p$ égaux à leur propre inverse.

(3) En déduire le théorème de Wilson : p divise $(p-1)! + 1$.

Exercice 17: ★★★★

Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps.

(1) Montrer que pour tout $x \in \mathbb{Q}$, $f(x) = x$.

(2) Montrer que f est croissante.

(3) En déduire que pour tout $x \in \mathbb{R}$, $f(x) = x$.

Exercice 18: ★★

On définit sur $\mathbb{R}$ les deux lois $\oplus$ et $\otimes$ par $x \oplus y = x + y - 1$ et $x \otimes y = x + y - xy$. Montrer que $(\mathbb{R}, \oplus, \otimes)$ est un corps.

Exercice 19: ★★★

Soit A un anneau fini commutatif non nul intègre. Montrer que A est un corps.

Exercice 20: ★★★★

Déterminer à isomorhisme près tous les corps à 4 éléments.

Exercice 21: ★★★

Ce problème présente quelques propriétés des corps finis.

1. Préliminaires

Soient $(G, \times)$ et $(H, \times)$ deux groupes finis et $f : G \to H$ un morphisme de groupes.

(1) On définit une relation R sur G de la façon suivante :

$$xRy \iff f(x) = f(y)$$

Montrer que R est une relation d'équivalence.

(2) Montrer que toutes les classes d'équivalence sont de cardinal $\mathrm{Card}(\mathrm{Ker}\, f)$.

(3) En déduire que $\mathrm{Card}\, G = \mathrm{Card}(\mathrm{Ker}\, f) \times \mathrm{Card}(\mathrm{Im}\, f)$.

2. Un exemple de corps fini.

Dans cette partie, $(K, +, \times)$ désigne un corps de cardinal 4 : $K = \{0_K, 1_K, a, b\}$ où 0_K désigne le neutre pour $+$ et 1_K le neutre pour $\times$.

(4) Montrer que l'équation $x^2 = 1_K$ a au plus deux racines.

(5) En déduire que $a \times b = 1_K$ et donner la table de Pythagore de $\times$.

(6) Donner la table de Pythagore de $+$. Que vaut $1_K + 1_K$?

3. Caractéristique d'un corps fini.

Soit $(K, +, \times)$ un corps fini de cardinal n. On considère l'application

$$\begin{array}{rccc} f : & \mathbb{N} & \to & K \\ & n & \mapsto & n1_K = \sum_{k=1}^{n} 1_K \end{array}$$

(7) Montrer que f n'est pas injective.

(8) En déduire l'existence de $p = \min\{k \in \mathbb{N}^* \mid k1_K = 0_K\}$. Cet entier p est appelé **caractéristique** de K.

(9) On suppose que $p = ab$ avec $(a, b) \in \mathbb{N}^2$. Montrer que $a1_K = 0_K$ ou $b1_K = 0_K$. En déduire que p est premier.

(10) Montrer que $F = \{n1_K \mid n \in \mathbb{N}\}$ est un sous-corps de K de cardinal p. On dit que F est le sous-corps premier de K.

4. Cardinal d'un corps fini.

Soit $(K, +, \times)$ un corps fini de cardinal n et de caractéristique p. Soit F le sous-corps premier de K. On note $\{x_1, \dots / x_n\}$ les éléments distincts de K. On considère l'application

$$\begin{array}{rccc} f : & F^n & \to & K \\ & (\lambda_1, ..., \lambda_n) & \mapsto & \sum_{k=1}^{n} \lambda_k x_k \end{array}$$

(11) On munit F^n d'une loi de composition $\oplus$ de la façon suivante :

$$(\lambda_1, \dots, \lambda_n) \oplus (\mu_1, \dots, \mu_n) = (\lambda_1 + \mu 1, \dots, \lambda_n + \mu_n).$$

Montrer que $(F^n, \oplus)$ est un groupe.

(12) Montrer que f est un morphisme de groupes.

(13) Montrer que f est surjective.

(14) En utilisant le résultat 3, montrer que $n = p^k$ avec $k \in \mathbb{N}^*$.

5. Automorphisme de Frobenius

Soit $(K, +, \times)$ un corps fini de caractéristique p et

$$\begin{array}{rccc} f : & K & \to & K \\ & x & \mapsto & x^p \end{array}$$

(1) En utilisant la formule du binôme, montrer que pour tout $(x, y) \in K^2$, $(x + y)^p = x^p + y^p$.

(2) En déduire que f est un automorphisme de corps.