EXERCICES : STRUCTURES ALGÈBRIQUES

1 Groupes

1.1 Transport de structure

1. Soit $(G, \star)$ un groupe et H un ensemble tel qu'il existe une fonction $f : H \mapsto G$ bijective. On définit la loi $\star$ sur H par

$$\forall x, y \in H \quad x \star y = f^{-1}\left(f(x) \star f(y)\right)$$

Montrer que $(H, \star)$ est un groupe isomorphe à $(G, \star)$.

2. On définit la loi $\oplus$ sur $\mathbb{R}$ par

$$\forall x, y \in \mathbb{R} \quad x \oplus y = \sqrt[3]{x^3 + y^3}$$

Montrer que $(\mathbb{R}, \oplus)$ est un groupe commutatif.

1.2 Sous-groupe de $\mathbb{U}$

Montrer que $\cup_{n\in\mathbb{N}^*}\mathbb{U}_n$ est un sous-groupe strict de $(\mathbb{U}, \cdot)$.

1.3 Union de deux sous-groupes

Soient $(G, *)$ un groupe, et H et K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

1.4 Groupes tels que $x^2 = e$

Soit $(G, \star)$ un groupe tel que :

$$\forall x \in G \quad x^2 = e$$

Montrer que G est commutatif.

2 Ordre d'un élément, $\mathbb{Z}/n\mathbb{Z}$

2.1 Ordre d'un produit

Soit $(G, \star)$ un groupe fini et x, y deux éléments de G d'ordre respectifs ω_x et $\omega_y \in \mathbb{N}^*$. On suppose que $x \star y = y \star x$ et que $\omega_x \wedge \omega_y = 1$. Montrer que $\mathrm{Gr}(x) \cap \mathrm{Gr}(y) = \{e\}$ puis que xy est d'ordre $\omega_x\omega_y$.

2.2 Élément d'ordre 2

Soit $(G, \star)$ un groupe fini de cardinal pair. Le but de cet exercice est de montrer qu'il existe un élément x de G, différent de e, tel que $x^2 = e$. Pour cela, on considère l'ensemble :

$$E = \left\{x \in G : x^2 \neq e\right\}$$

1. Montrer que si $x \in E$, $x^{-1} \in E$.
2. En déduire que E est de cardinal pair et conclure.

2.3 Les groupes d'ordre inférieurs à 5 sont commutatifs

1. Soit $(G, \star)$ un groupe fini dont le cardinal p est un nombre premier et x un élément de G différent de e. Montrer que

$$G = \left\{x^k : k \in [\![0, p-1]\!]\right\}$$

puis en déduire que G est commutatif.

2. Montrer que les groupes finis de cardinal inférieur ou égal à 5 sont commutatifs. *On montrera qu'il n'y a que deux tables possibles pour les groupes de cardinal 4.*
3. Montrer que le groupe $(\sigma([\![1, 3]\!]), \circ)$ est de cardinal 6 et est non commutatif.

2.4 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. Déterminer et dénombrer les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$.

2.5 Théorème chinois

Soit $p, q \in \mathbb{N}^*$ deux entiers premiers entre eux. Montrer que l'application φ de $(\mathbb{Z}/pq\mathbb{Z}, +)$ dans $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, +)$ qui à $\overline{k}$ associe $(\overline{k}, \overline{k})$ est bien définie et est un isomorphisme de groupe.

3 Anneaux

3.1 Anneau de Boole

Soit E un ensemble. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif. Montrer qu'il est intègre si et seulement si E est vide ou réduit à un singleton.

3.2 Fonction définie sur un anneau

Soit $(A, +, \times)$ un anneau et f une application de A dans $\mathbb{R}_+$ telle que
— $\forall x \in A \quad f(x) = 0 \Longleftrightarrow x = 0$.
— $\forall x, y \in A \quad f(xy) = f(x)f(y)$.
— $\forall x, y \in A \quad f(x + y) \leqslant \max\left(f(x), f(y)\right)$.
Montrer que $\{x \in A : f(x) \leqslant 1\}$ est un sous-anneau de A.

4 Corps

4.1 Exemple de corps

On définit sur $\mathbb{R}$ deux lois $\oplus$ et $\otimes$ par :

$$\begin{aligned} \forall (x,y) \in \mathbb{R}^2 \quad x \oplus y &= x + y - 1\,, \\ \forall (x,y) \in \mathbb{R}^2 \quad x \otimes y &= x + y - xy\,. \end{aligned}$$

Montrer que $(\mathbb{R}, \oplus, \otimes)$ est un corps commutatif.

4.2 Extension quadratique

Soit $\alpha \in \mathbb{N}$ tel que $\sqrt{\alpha} \notin \mathbb{Q}$. On pose

$$\mathbb{Q}(\sqrt{\alpha}) = \left\{ a + b\sqrt{\alpha} : (a,b) \in \mathbb{Q}^2 \right\}$$

1. Soit $x \in \mathbb{Q}(\sqrt{\alpha})$. Montrer qu'il existe un unique couple $(a,b) \in \mathbb{Q}^2$ tel que $x = a + b\sqrt{\alpha}$.
2. Montrer que $\mathbb{Q}(\sqrt{\alpha})$ est un sous-corps de $(\mathbb{R}, +, \times)$.
3. Pour $x = a + b\sqrt{\alpha} \in \mathbb{Q}(\sqrt{\alpha})$, on pose $\overline{x} = a - b\sqrt{\alpha}$; on l'appelle le conjugué de x. Montrer que l'application $x \mapsto \overline{x}$ est bien définie et est un automorphisme du corps $\mathbb{Q}(\sqrt{\alpha})$.
4. Montrer que l'automorphisme construit à la question précedente est le seul automorphisme non trivial de $\mathbb{Q}(\sqrt{\alpha})$.

4.3 Théorème de Wilson

Soit p un nombre premier.

1. Montrer que l'application φ de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ qui à x associe $1/x$ est une bijection. Quels sont les points fixes de cette bijection ?
2. En déduire que $(p-1)! \equiv -1\ [p]$.