EPFL Automne 2025
Algebre Lineaire Avancee, MATH-110

Série 3

Tous les exercices seront corriges. La correction sera postee sur le moodle apres environ 2 semaines.

Exercice 1. Soit $G = [0, 1[$ et $\oplus : G \times G \mapsto \mathbb{R}$ la loi de composition definie par

$$x \oplus x' := \begin{cases} x + x' & \text{si } x + x' < 1 \\ x + x' - 1 & \text{si } x + x' \geqslant 1 \end{cases}.$$

1. Montrer que $\oplus$ est a valeurs dans G et trouver un element neutre $0_G \in G$ et une application inversion $\ominus : G \mapsto G$ telles que

   $$(G, \oplus, 0_G, \ominus)$$

   forme un groupe.
2. Montrer que pour tout $x, x' \in G$ on a

   $$x \oplus x' = x' \oplus x;$$

   on dit que $(G, \oplus)$ est un groupe commutatif.

Exercice 2 $(\star)$**.** Soit X un ensemble. Dans la premiere serie, on a defini sur l'ensemble de ses parties $\mathscr{P}(X)$ une loi de composition

$$\Delta : (A, B) \in \mathscr{P}(X) \times \mathscr{P}(X) \to A\Delta B \in \mathscr{P}(X),$$

ou $A\Delta B$ est la difference *symetrique* de A et B :

$$A\Delta B := A \cup B - A \cap B = \{x \in A \cup B,\ x \notin A \cap B\} \subset X$$

(les elements de X qui sont dans la reunion de A et B et qui ne sont pas dans leur intersection).

1. Definir un element neutre $e_{\mathscr{P}(X)} \in \mathscr{P}(X)$ et une inversion $\bullet^{-1} : \mathscr{P}(X) \to \mathscr{P}(X)$ de sorte que

   $$(\mathscr{P}(X), \Delta, e_{\mathscr{P}(X)}, \bullet^{-1})$$

   forme un groupe.
2. Est ce que $(\mathscr{P}(X), \Delta)$ est un groupe commutatif ?

Exercice 3 (Groupes de fonctions)**.** Soit X un ensemble et $(G, \star)$ un groupe. Soit

$$\mathcal{F}(X, G) = G^X = \{f : X \mapsto G\}$$

l'ensemble des fonctions de X a valeurs dans G (les applications de X vers G).

On muni $\mathcal{F}(X, G)$ de la loi de composition interne suivante : etant donne des fonctions $f_1, f_2 \in \mathcal{F}(X, G)$ on defini la fonction $f_1 \star f_2$ par

$$\forall x \in X,\ f_1 \star f_2(x) := f_1(x) \star f_2(x).$$

(ici on abuse les notations en notant la loi de composition sur $\mathcal{F}(X, G)$ de la meme maniere que celle sur G).

1. Trouver un element neutre $e_{\mathcal{F}(X,G)}$ et une inversion $\bullet^{-1}$ de sorte que $(\mathcal{F}(X, G), \star, e_{\mathcal{F}(X,G)}, \bullet^{-1})$ forme un groupe.

Exercice 4 (Groupes modulaires)**.** Soit $q \geqslant 1$ un entier non nul ; on definit sur $\mathbb{Z}$ la relation suivante (de congruence modulo q)

$$m \equiv n \,(\mathrm{mod}\, q) \iff m - n = qk,\ k \in \mathbb{Z}$$

et on dit que m et n sont congrus modulo q (ie. la difference $m - n$ est divisible par q).

Pour $a \in \mathbb{Z}$ la classe de congruence $a \,(\mathrm{mod}\, q)$ est l'ensemble des entiers m congrus a a modulo q :

$$a \,(\mathrm{mod}\, q) = \{m \in \mathbb{Z},\ m \equiv a \,(\mathrm{mod}\, q)\} \subset \mathbb{Z}.$$

L'ensemble de ces classes de congruences modulo q est note

$$\mathbb{Z}/q\mathbb{Z} := \{a \,(\mathrm{mod}\, q),\ a \in \mathbb{Z}\}$$

(comme $a \,(\mathrm{mod}\, q)$ est un sous-ensemble de $\mathbb{Z}$, l'ensemble des classes de congruences $\mathbb{Z}/q\mathbb{Z}$ un sous-ensemble de $\mathscr{P}(\mathbb{Z})$).

1. Montrer que la relation de *congruence modulo* q est une relation d'equivalence (reflexive, symetrique, transitive) sur $\mathbb{Z}$.
2. Montrer que

$$a \,(\mathrm{mod}\, q) := a + q\mathbb{Z} = \{a + q.k,\ k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

3. Montrer que pour toute classe $a \,(\mathrm{mod}\, q) \in \mathbb{Z}/q\mathbb{Z}$ il existe $r \in \{0, \cdots, q-1\}$ tel que

$$a \,(\mathrm{mod}\, q) = r \,(\mathrm{mod}\, q).$$

Montrer que

$$|\mathbb{Z}/q\mathbb{Z}| = q.$$

4. Pour $A, B \in \mathscr{P}(\mathbb{Z})$ des sous-ensembles de $\mathbb{Z}$, on a pose

$$A \boxplus B := \{a + b,\ a \in A,\ b \in B\} \in \mathscr{P}(\mathbb{Z}).$$

On definit egalement

$$\boxminus A := \{-a,\ a \in A\} \in \mathscr{P}(\mathbb{Z}),$$

l'ensemble des opposes des elements de A.
Soient $a \pmod q,\ b \pmod q \in \mathbb{Z}/q\mathbb{Z}$, montrer que

$$a \pmod q \boxplus b \pmod q = a + b \pmod q = a + b + q\mathbb{Z}.$$

et que

$$\boxminus a \pmod q = -a \pmod q = -a + q\mathbb{Z}.$$

5. Montrer que $(\mathbb{Z}/q\mathbb{Z}, \boxplus, 0 \pmod q, \boxminus)$ forme un groupe : c'est le groupe des classes de congruence modulo q.
6. Montrer que $(\mathbb{Z}/q\mathbb{Z}, \boxplus)$ est commutatif.

Remarque. On a donc montre que pour tout entier $q \geqslant 1$ il existe un groupe commutatif fini d'ordre q.