EPFL Automne 2024
Algebre Lineaire Avancee, MATH-110

Série 3

Vous etes fortement encourages a essayer de resoudre (eventuellement a plusieurs) l'exercice ($\star$) et a rendre votre solution (eventuellement a plusieurs) avant le vendredi de la semaine suivante celle ou la serie a ete postee. Il faudra transmettre votre solution sur moodle, sous forme de fichier pdf (eventuellement tape en LaTeX) en suivant le lien a cet effet dans la semaine de la serie.

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 commutatif.

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

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

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 $e_{\mathcal{P}(X)} \in \mathcal{P}(X)$ et une inversion $\bullet^{-1} : \mathcal{P}(X) \to \mathcal{P}(X)$ de sorte que

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

   forme un groupe commutatif.

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

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

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 $f_1, f_2 \in \mathcal{F}(X, G)$ 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.
2. Soit $U \subset G$ un sous-ensemble de G. Donner une condition necessaire et suffisante pour que le sous-ensemble des fonctions a valeurs dans U

   $$\mathcal{F}(X, U) \subset \mathcal{F}(X, G)$$

   forme un sous-groupe de $\mathcal{F}(X, G)$.

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

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

(c'est donc un sous-ensemble de $\mathcal{P}(\mathbb{Z})$).

1. Montrer que la relation de congruence modulo q est une relation d'equivalence (reflexive, symetrique, transitive).
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
$$a \,(\mathrm{mod}\, q) = r \,(\mathrm{mod}\, q).$$
Quel est le cardinal de $\mathbb{Z}/q\mathbb{Z}$?

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 $a \,(\mathrm{mod}\, q),\ b \,(\mathrm{mod}\, q) \in \mathbb{Z}/q\mathbb{Z}$, montrer que
$$a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) = a + b \,(\mathrm{mod}\, q) = a + b + q\mathbb{Z}.$$
et que
$$\boxminus a \,(\mathrm{mod}\, q) = (-a) \,(\mathrm{mod}\, q) = -a + q\mathbb{Z}.$$

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

6. On rappelle la notation "multiple" (dans la notation additive) pour $n \geqslant 1$
$$n.a \,(\mathrm{mod}\, q) := a \,(\mathrm{mod}\, q) + \cdots + a \,(\mathrm{mod}\, q)\ (n \text{ fois})$$
(et on rappelle qu'on a une notation simnilaire pour $n \leqslant 0$). Montrer que pour $n \in \mathbb{Z}$
$$n.a \,(\mathrm{mod}\, q) = na \,(\mathrm{mod}\, q)$$
(la classe de congruence de l'entier na).

7. Montrer que le sous-groupe $\mathbb{Z}.1 \,(\mathrm{mod}\, q)$ verifie
$$\mathbb{Z}.1 \,(\mathrm{mod}\, q) = \{n.1 \,(\mathrm{mod}\, q),\ n \in \mathbb{Z}\} = \mathbb{Z}/q\mathbb{Z}.$$

8. Montrer que si a est premier avec q (ie. $\mathrm{pgcd}(a, q) = 1$) alors
$$\mathbb{Z}.a \,(\mathrm{mod}\, q) = \{n.a \,(\mathrm{mod}\, q),\ n \in \mathbb{Z}\} = \mathbb{Z}/q\mathbb{Z}$$
(on utilisera Bezout pour montrer qu'il existe $n \in \mathbb{Z}$ tel que $n.a \,(\mathrm{mod}\, q) = 1 \,(\mathrm{mod}\, q)$.

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

Exercice 5. Soit $(G, \star, e, \bullet^{-1})$ un groupe fini de cardinal $n \geqslant 1$. On enumere ses elements de la maniere suivante

$$G = \{g_0 = e, g_1, \cdots, g_{n-1}\}.$$

On peut representer la loi de groupe sous forme d'un tableau

$\star$	e	g_1	$\cdots$	g_{n-1}
e	e	g_1	$\cdots$	g_{n-1}
g_1	g_1	$g_1 \star g_1$	$\cdots$	$g_1 \star g_{n-1}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g_{n-1}	g_{n-1}	$g_{n-1} \star g_1$	$\cdots$	$g_{n-1} \star g_{n-1}$

.

1. Donner ces tableaux pour $n = 1, 2, 3$ (si on veut, on pourra utiliser un corollaire convenable du Thm de Lagrange).