EPFL Automne 2025
Algèbre Lineaire Avancée, MATH-110

Solution Série 3

Tous les exercices seront corrigées. La correction sera postée sur le moodle après 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' est un groupe commutatif.

Solution : . 1. Il n'est pas difficile de voir que 0 est neutre pour l'addition, puisque $x \oplus 0 = x + 0 = x$ pour tout $x \in G$. Similairement on voit que $0 \oplus x = x$. Dans ce qui suis, on suppose $\oplus$ commutatif (à démontrer dans la question 2). Pour chaque $x \in G$ on a que $1 - x \in G$ et que $1 - x$ est l'inverse de x, en fait $x + (1 - x) = 1$ et donc $x \oplus (1 - x) = 0.$, $1 - x$ est aussi l'inverse à droite. Il ne reste plus qu'à montrer que l'opération est associative. Soient $x_1, x_2, x_3 \in G$, il y a trois possibilités :

— Si $x_1 + x_2,\ x_2 + x_3 < 1$, on a

$$x_1 \oplus x_2 = x_1 + x_2,\ x_2 \oplus x_3 = x_2 + x_2$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2) \oplus x_3 = x_1 + x_2 + x_3 - \varepsilon$$

avec $\varepsilon = 0$ ou 1 suivant que $x_1 + x_2 + x_3$ est < 1 ou $\geqslant 1$ (on observe que comme $+$ est associative sur $\mathbb{R}$ on n'a pas besoin de mettre de paranthèses dans cette inégalité et que

$$\varepsilon = \varepsilon(x_1 + x_2 + x_3)$$

ne depend que de la somme des trois termes et pas de leurs valeurs individuelles). D'autre part

$$x_1 \oplus (x_2 + x_3) = x_1 + x_2 + x_3 - \varepsilon$$

avec le même $\varepsilon = \varepsilon(x_1 + x_2 + x_3)$. Ainsi on a

$$(x_1 \oplus x_2) \oplus x_3 = x_1 \oplus (x_2 \oplus x_3). \tag{0.1}$$

— Si $x_1 + x_2 < 1 \leqslant x_2 + x_3$, on a

$$x_1 \oplus x_2 = x_1 + x_2, \ x_2 \oplus x_3 = x_2 + x_3 - 1$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2) \oplus x_3 = x_1 + x_2 + x_3 - 1 - \varepsilon$$

avec $\varepsilon = 0$ ou 1 suivant que $x_1 + x_2 + x_3$ est < 2 ou $\geqslant 2$. On a également

$$x_1 \oplus (x_2 \oplus x_3) = x_1 \oplus (x_2 + x_3 - 1) = x_1 + x_2 + x_3 - 1 - \varepsilon.$$

On a donc (0.1). Par commutativité supposée de $\oplus$ (et de $+$) cela traite aussi le cas $x_2 + x_3 < 1 \leqslant x_1 + x_2$

— Si $1 \leqslant x_1 + x_2, x_2 + x_3$ alors

$$x_1 \oplus x_2 = x_1 + x_2 - 1 < 1, \ x_2 \oplus x_3 = x_2 + x_3 - 1 < 1$$

et

$$(x_1 \oplus x_2) \oplus x_3 = (x_1 + x_2 - 1) \oplus x_3 = x_1 + x_2 + x_3 - 1 - \varepsilon$$

avec $\varepsilon = 0$ ou 1 suivant que $x_1 + x_2 + x_3$ est < 2 ou $\geqslant 2$. Également

$$x_1 \oplus (x_2 \oplus x_3) = x_1 \oplus (x_2 + x_3 - 1) = x_1 + x_2 + x_3 - 1 - \varepsilon.$$

On a donc bien (0.1).

2. Observons qu'il est équivalent de vérifier que $x + x' < 1$ que de vérifier $x' + x < 1$ par commutativité de $+$. Ainsi la commutativité de $\oplus$ suit automatiquement de celle de $+$.

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 :

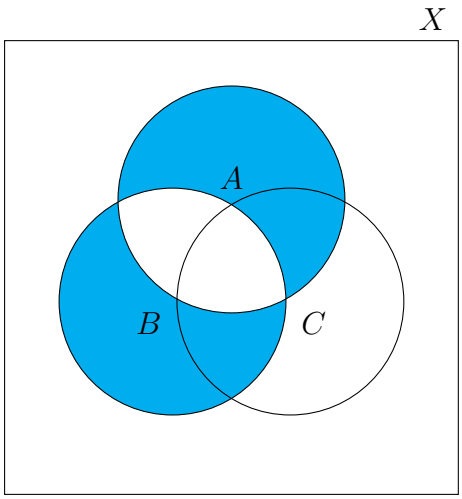
$$A\Delta B := A \cup B - A \cap B = \{x \in A \cup B, \ x \notin A \cap B\} \subset X$$

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

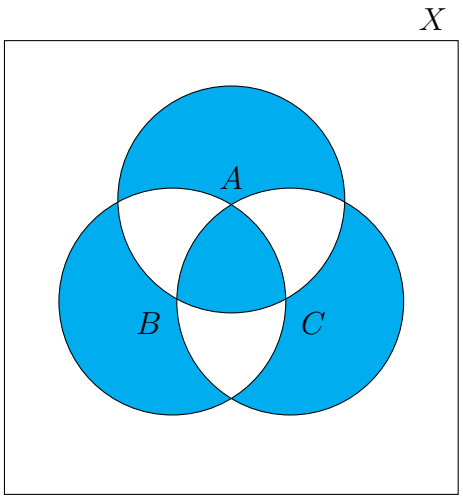
1. Definir un element neutre $e_{\mathcal{P}(X)} \in \mathcal{P}(X)$ et une inversion $\bullet^{-1} : \mathcal{P}(X) \to \mathcal{P}(X)$ de sorte que
$$(\mathcal{P}(X), \Delta, e_{\mathcal{P}(X)}, \bullet^{-1})$$
forme un groupe.
2. Est ce que $(\mathcal{P}(X), \Delta)$ est un groupe commutatif ?

Solution : .

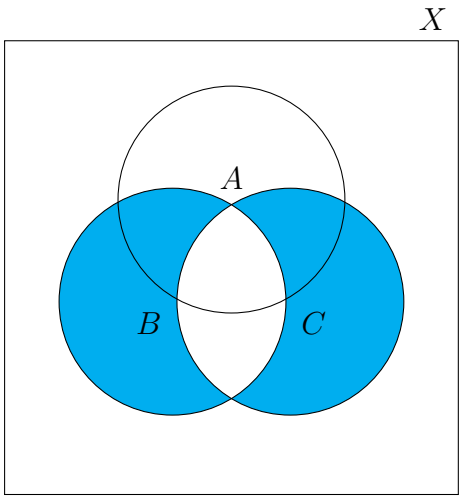
1. On montre d'abord que l'opération Δ est associative. L'associativité peut être démontrée à l'aide de simples diagrammes de Venn : Ici, on voit les deux types de calcul avec chacun une étape intermédiaire, pour que l'on puisse mieux voir ce qui se passe.



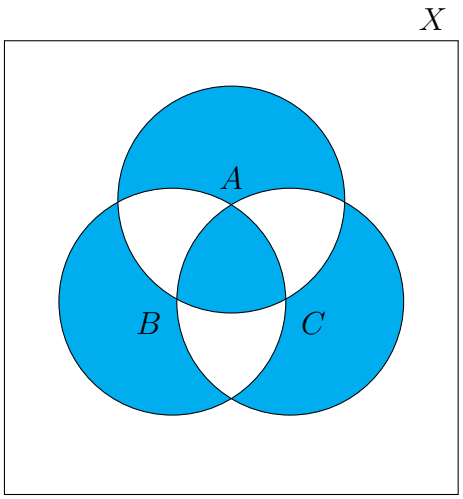
$A\Delta B$



$(A\Delta B)\Delta C$



$B\Delta C$



$A\Delta(B\Delta C)$

On peut également effectuer les calculs suivants. On note que :

$$A\Delta B = A \cup B - A \cap B = A \cup B \cap (A \cap B)^c.$$

De plus :

$$(A \cap B)^c = A^c \cup B^c \text{ et } (A \cup B)^c = (A^c \cap B^c).$$

Donc on calcule :

$$\begin{aligned}
&(A\Delta B)\Delta C \\
&= \big((A\Delta B) \cup C\big) \cap \big((A\Delta B) \cap C\big)^c \\
&= \big(((A \cup B) \cap (A \cap B)^c) \cup C\big) \cap \big(((A \cup B) \cap (A \cap B)^c) \cap C\big)^c \\
&= \big(((A \cup B) \cap (A^c \cup B^c)) \cup C\big) \cap \big(((A \cup B) \cap (A^c \cup B^c))^c \cup C^c\big) \\
&= \big((A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) \cup C\big) \cap \big((A \cup B)^c \cup (A^c \cup B^c)^c \cup C^c\big) \\
&= \big((A \cap B^c) \cup (B \cap A^c) \cup C\big) \cap \big((A^c \cap B^c) \cup (A \cap B) \cup C^c\big) \\
&= (A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c) \cup (C \cap A \cap B).
\end{aligned}$$

Pareil on obtient :

$$\begin{aligned}
&A\Delta(B\Delta C) \\
&= \big((A \cup (B\Delta C\big) \cap \big(A \cap (B\Delta C)\big)^c \\
&= \big(A \cup ((B \cup C) \cap (B \cap C)^c)\big) \cap \big(A \cap ((B \cup C) \cap (B \cap C)^c)\big)^c \\
&= \big(A \cup ((B \cup C) \cap (B^c \cup C^c))\big) \cap \big(A^c \cup ((B \cup C) \cap (B^c \cup C^c))^c\big) \\
&= \big(A \cup (B \cap B^c) \cup (B \cap C^c) \cup (C \cap B^c) \cup (C \cap C^c)\big) \cap \big(A^c \cup (B \cup C)^c \cup (B^c \cup C^c)^c\big) \\
&= \big(A \cup (B \cap C^c) \cup (C \cap B^c)\big) \cap \big(A^c \cup (B^c \cap C^c) \cup (B \cap C)\big) \\
&= (A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c) \cup (C \cap A \cap B).
\end{aligned}$$

Alors Δ est bien associatif. On cherche l'elément neutre. De la série 1 exercice 5.2 on sait que :

$$\emptyset\Delta A = A\Delta\emptyset = A,$$

alors $\emptyset = e_\Delta$ est l'élément neutre. De plus on a vue que

$$A\Delta A = \emptyset = e_\Delta,$$

donc $\bullet^{-1} : \mathscr{P}(X) \mapsto \mathscr{P}(X), A \mapsto A$ est l'application d'inversion. Avec l'associativité et la commutativité de la première parti on obtient un groupe commutatif.

2. On utilise la définition

$$A\Delta B = A \cup B - A \cap B = B \cup A - B \cap A = B\Delta A,$$

Puisque $\cup$ et $\cap$ sont les deux des opérations commutatives, on voit que Δ l'est aussi.

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 : étant 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 même manière 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.

Solution : . L'idée sera vraiment tout au long de l'exercice de puiser autant de choses que possibles dans la structure de groupe de G pour en déduire des choses sur celle de $\mathcal{F}(X, G)$.

1. On pose

$$e_{\mathcal{F}(X,G)} \colon X \to G,\ x \mapsto e_G$$

et pour $f \in \mathcal{F}(X, G)$,

$$f^{-1} \colon X \to G,\ x \mapsto (f(x))^{-1}.$$

En effet, pour tout $f \in \mathcal{F}(X, G)$ et pour tout $x \in X$ on a :

- $f \star e_{\mathcal{F}(X,G)}(x) = f(x) \star e_{\mathcal{F}(X,G)}(x) = f(x) \star e_G = f(x)$. Puisque $f \star e_{\mathcal{F}(x,G)}$ et f correspondent sur tout $x \in X$, ils sont égaux, et donc $e_{\mathcal{F}(X,G)}$ est neutre a droite.On montre la neutralité à gauche de la même manière.
- $f \star f^{-1}(x) = f(x) \star (f(x))^{-1} = e_G = e_{\mathcal{F}(X,G)}(x)$. Comme les deux applications correspondent sur tout $x \in X$, elles sont égales, et donc f^{-1} est bien l'inverse à droite de f. On montre de la même manière que f^{-1} est bien l'inverse à gauche.

On peut se convaincre facilement que l'associativité de la loi de $\mathcal{F}(X, G)$ découle de celle de la loi de G par un argument similaire (On montre que $(f \star g) \star h$ et $f \star (g \star h)$ correspondent sur tout $x \in X$.)

Remarque. : On a fait ici un petit abus de notations en écrivant f^{-1} sans avoir encore vérifié que c'etait bien l'inverse de f (mais on s'en remettra). Notez cependant que f^{-1} ne désigne pas la reciproque de f (au sens reciproque d'une bijection).

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

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

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 congruence $\mathbb{Z}/q\mathbb{Z}$ est 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) 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 posé
$$A \boxplus B := \{a + b,\ a \in A,\ b \in B\} \in \mathscr{P}(\mathbb{Z}).$$
On definit egalement
$$\boxminus A := \{-a,\ a \in A\} \in \mathscr{P}(\mathbb{Z}),$$
l'ensemble des opposés 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 : 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 montré que pour tout entier $q \geqslant 1$ il existe un groupe commutatif fini d'ordre q.

Solution : .

1. On montre que cette relation est une relation d'équivalence. Pour cela, il faut verifier trois choses :
   i) Reflexivite : Soit $m \in \mathbb{Z}$. Alors on voit que $m - m = 0 = 0 \cdot q$, donc $m \equiv m \,(\mathrm{mod}\, q)$
   ii) Symetrie : Soient $m, n \in \mathbb{Z}$ tels que $m \equiv n \,(\mathrm{mod}\, q)$, i.e. il existe $k \in \mathbb{Z}$ tel que $m - n = kq$. Mais alors $n - m = -kq = (-k)q$. En posant $p := -k \in \mathbb{Z}$, on alors que $m \equiv n \,(\mathrm{mod}\, q) \implies n \equiv m \,(\mathrm{mod}\, q)$.
   iii) Transitivite : Soient $m \equiv n \,(\mathrm{mod}\, q)$, et $n \equiv l \,(\mathrm{mod}\, q)$, i.e.

$$\exists\, k, k' \in \mathbb{Z} : \quad m - n = kq \;\text{ et }\; n - l = k'q$$

   mais alors, $m - l = q(k + k')$ et on obtient donc que $m \equiv l \,(\mathrm{mod}\, q)$.
2. Il suffit simplement de voir que :

$$\begin{aligned} a \,(\mathrm{mod}\, q) &= \{m \in \mathbb{Z} : \; m - a = kq \;\text{ pour un }\; k \in \mathbb{Z}\} \\ &= \{m \in \mathbb{Z} : \; m = a + kq \;\text{ pour un }\; k \in \mathbb{Z}\} \\ &= \{a + kq \;\text{ pour un }\; k \in \mathbb{Z}\} \subseteq \mathbb{Z} \end{aligned}$$

3. Soit $a \,(\mathrm{mod}\, q) \in \mathbb{Z}/q\mathbb{Z}$. On effectue la division euclidienne de a par q. On a alors que

$$\exists k \in \mathbb{Z}, \;\text{ et }\; r \in \{0, 1, \cdots, q-1\} \;\text{ t.q. }\; a = kq + r$$

   On voit que $a \equiv r \,(\mathrm{mod}\, q)$ car $a - r = a - (a - kq) = kq$. Puisque a et r sont en relation, leurs classes d'équivalence sont égales.
   On veut montrer que $|\mathbb{Z}/q\mathbb{Z}| = q$. Mais on voit que $\mathbb{Z}/q\mathbb{Z}$ correspond a l'ensemble des classes d'équivalence. Or chaque classe a un représentant unique dans $\{0, 1, \cdots, q-1\}$. Cela nous donne alors le nombre de classes, modulo le choix des représentants, est exactement q.
4.

$$\begin{aligned} a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) &= \{a + kq \;\; k \in \mathbb{Z}\} \boxplus \{b + kq \;\; k \in \mathbb{Z}\} \\ &= \{a + kq + b + k'q \;\; k \in \mathbb{Z}\} \\ &= \{(a + b) + q(k + k') \;\; k, k' \in \mathbb{Z}\} \\ &= \{(a + b) + q \cdot p \;\; p \in \mathbb{Z}\}, \;\text{ en posant }\; p = k + k' \\ &= (a + b) \,(\mathrm{mod}\, q) \end{aligned}$$

et

$$\begin{aligned}\boxminus a \,(\mathrm{mod}\, q) &= \{-(a+kq), k \in \mathbb{Z}\} \\ &= \{-a-kq, k \in \mathbb{Z}\} = \{-a+pq, p \in \mathbb{Z}\} \ \text{ en posant } \ p=-k \\ &= (-a) \,(\mathrm{mod}\, q)\end{aligned}$$

5. On vient de vérifier que $\boxplus$ est bien a valeurs dans $\mathbb{Z}/q\mathbb{Z}$.
Il faut maintenant vérifier que cette loi de groupe est associative :

$$\begin{aligned}(a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q)) \boxplus c \,(\mathrm{mod}\, q) &= a+b \,(\mathrm{mod}\, q) \boxplus c \,(\mathrm{mod}\, q) \\ &= (a+b)+c \,(\mathrm{mod}\, q) \\ &= a+(b+c) \,(\mathrm{mod}\, q) = a \,(\mathrm{mod}\, q) \boxplus (b+c) \,(\mathrm{mod}\, q) \\ &= a \,(\mathrm{mod}\, q) \boxplus (b \,(\mathrm{mod}\, q) \boxplus c \,(\mathrm{mod}\, q))\end{aligned}$$

Donc l'operation $\boxplus$ est associative.

On doit montrer à présent que $0 \,(\mathrm{mod}\, q)$ est bien le neutre :

$$\begin{aligned}a \,(\mathrm{mod}\, q) \boxplus 0 \,(\mathrm{mod}\, q) &= a+0 \,(\mathrm{mod}\, q) = a \,(\mathrm{mod}\, q) \\ &= 0+a \,(\mathrm{mod}\, q) = 0 \,(\mathrm{mod}\, q) \boxplus a \,(\mathrm{mod}\, q).\end{aligned}$$

Donc $0 \,(\mathrm{mod}\, q)$ est bien l'élément neutre pour $\boxplus$.

Il reste à voir que $\boxminus$ est effectivement l'inverse pour $\boxplus$.

$$a \,(\mathrm{mod}\, q) \boxplus \boxminus a \,(\mathrm{mod}\, q) = a-a \,(\mathrm{mod}\, q) = 0 \,(\mathrm{mod}\, q)$$

et

$$\boxminus a \,(\mathrm{mod}\, q) \boxplus a \,(\mathrm{mod}\, q) = -a+a \,(\mathrm{mod}\, q) = 0 \,(\mathrm{mod}\, q).$$

Donc $\boxminus a \,(\mathrm{mod}\, q)$ est l'inverse de $a \,(\mathrm{mod}\, q)$.

6. On a que

$$\begin{aligned}a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) &= a+b \,(\mathrm{mod}\, q) \\ &= b+a \,(\mathrm{mod}\, q) = b \,(\mathrm{mod}\, q) \boxplus a \,(\mathrm{mod}\, q).\end{aligned}$$

Et on obtient ainsi un groupe commutatif, comme voulu.