EPFL Automne 2024
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 commutatif.

Solution : . 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 $0 \oplus x = x$. Il est aussi claire que l'operation est commutatif, puisque l'addition sur $\mathbb{R}$ est commutatif. 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 $x \oplus (1 - x) = 0$. Par commutativité, $1 - x$ est aussi l'inverse à droite. Il ne reste plus qu'a montrer que l'opération est associative. Soient $x_1, x_2, x_3 \in G$, il y a trois possibilités :

1. 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

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

2. 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 de $\oplus$ (et de $+$) cela traite aussi le cas $x_2 + x_3 < 1 \leqslant x_1 + x_2$

3. 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).

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

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

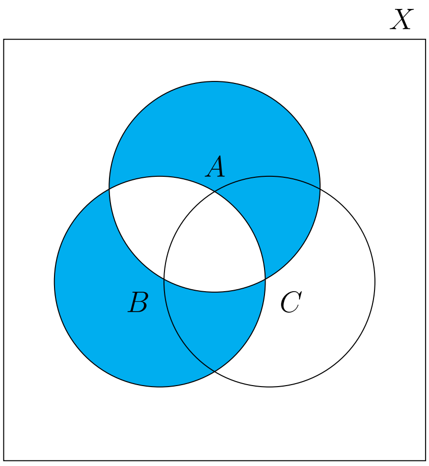
forme un groupe commutatif.

Solution : .

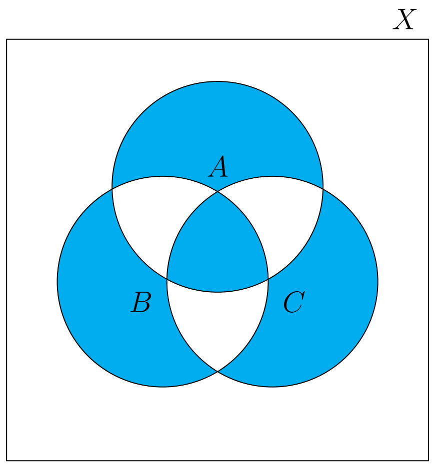
On montre d'abord que l'opération Δ est commutatif et associatif. Pour la commuativité :

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

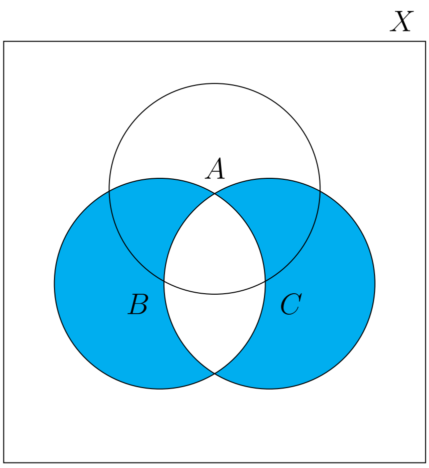
puisque $\cup$ et $\cap$ sont les deux commutatifs. L'associativité peut être démontrée à l'aide de simples diagrammes de Venn : Ici, on voit les deux types de calcul avec chacun une étape intermédiaire, pour que l'on puisse mieux voir ce qui se passe.



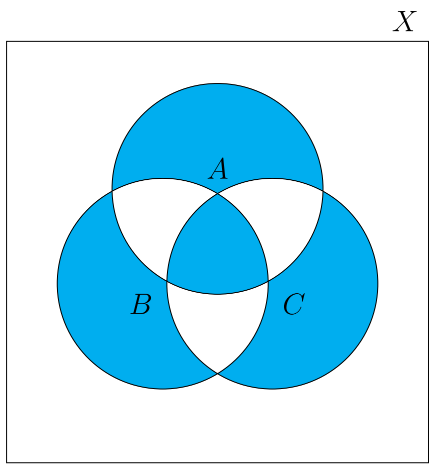
$A \Delta B$



$(A \Delta B) \Delta C$



$B \Delta C$



$A \Delta (B \Delta C)$

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.

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 $\mathcal{F}(X,G)$.

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 correspond 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 application correspond sur tout $x\in X$, ils sont égaux, 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 $f\star(g\star h)$ correspond sur tout $x\in X$.)

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

2. On veut montrer que U est un sous-groupe de G si et seulement si $\mathcal{F}(X, U)$ est un sous-groupe de $\mathcal{F}(X, G)$.

   $\Rightarrow$: Soit U un sous-groupe de G on va montrer que $\mathcal{F}(X, U)$ est un sous-groupe de $\mathcal{F}(X, G)$. On a $e_G \in U$, alors la fonction $e_{\mathcal{F}(X,G)}$ prend valuers dans U, i.e. $e_{\mathcal{F}(X,G)} \in \mathcal{F}(X, U)$. Si $f_1, f_2 \in \mathcal{F}(X, U)$, alors on a que pour tout $x \in X$: $f_1(x), f_2(x) \in U$. Donc $f_1 \star f_2^{-1}(x) = f_1(x) \star (f_2(x))^{-1} \in U$ pour tous les $x \in X$. Alors $f_1 \star f_2^{-1} \in \mathcal{F}(X, U)$. Alors $\mathcal{F}(X, U)$ verifie le critêre de sous-groupe vue en cours.

   $\Leftarrow$: Soit $\mathcal{F}(X, U) \subset \mathcal{F}(X, G)$ un sous-groupe. On va montrer que $U \subset G$ est un sous-groupe. La fonction $e_{\mathcal{F}(X,G)}$ est dans $\mathcal{F}(X, U)$, i.e. son image est inclu dans U, i.e. $e_G \in U$. Soient $g_1, g_2 \in U$. On considere les fonctions constantes $f_i\colon X \to G;\ x \mapsto g_i$, pour $i = 1, 2$. On a $f_1, f_2 \in \mathcal{F}(X, U)$, et alors $f_2^{-1} \in \mathcal{F}(X, U)$. Donc pour n'importe quel $x \in X$:

   $$g_1 \star g_2^{-1} = f_1(x) \star f_2(x)^{-1} = f_1 \star f_2^{-1}(x) \in U.$$

   Alors $U \subset G$ verifie le critère de sous-groupe vue en cours.

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

$$m \equiv n \pmod q \iff m - n = qk,\ \ k \in \mathbb{Z}$$

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 $a \pmod q$ est l'ensemble des entiers m congrus a a modulo q :

$$a \pmod q = \{m \in \mathbb{Z},\ m \equiv a \pmod q\} \subset \mathbb{Z}.$$

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

$$\mathbb{Z}/q\mathbb{Z} := \{a \pmod q,\ a \in \mathbb{Z}\}$$

(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

$$a \pmod q := a + q\mathbb{Z} = \{a + q.k,\ k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

3. Montrer que pour toute classe $a \pmod q \in \mathbb{Z}/q\mathbb{Z}$ il existe $r \in \{0, \cdots, q-1\}$ tel que
$$a \pmod q = r \pmod q.$$
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 $a \pmod q,\ b \pmod q \in \mathbb{Z}/q\mathbb{Z}$, 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 commutatif : le groupe des classes de congruence modulo q.
6. On rappelle la notation "multiple" (dans la notation additive) pour $n \geqslant 1$
$$n.a \pmod q := a \pmod q + \cdots + a \pmod q \ (n \text{ fois})$$
(et on rappelle qu'on a une notation simnilaire pour $n \leqslant 0$). Montrer que pour $n \in \mathbb{Z}$
$$n.a \pmod q = na \pmod q$$
(la classe de congruence de l'entier na).
7. Montrer que le sous-groupe $\mathbb{Z}.1 \pmod q$ verifie
$$\mathbb{Z}.1 \pmod q = \{n.1 \pmod q,\ n \in \mathbb{Z}\} = \mathbb{Z}/q\mathbb{Z}.$$
8. Montrer que si a est premier avec q (ie. $\mathrm{pgcd}(a,q)=1$) alors
$$\mathbb{Z}.a \pmod q = \{n.a \pmod q,\ n \in \mathbb{Z}\} = \mathbb{Z}/q\mathbb{Z}$$
(on utilisera Bezout pour montrer qu'il existe $n \in \mathbb{Z}$ tel que $n.a \pmod q = 1 \pmod q$).

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 $m \equiv m \pmod q$
ii) Symetrie : Soient $m, n \in \mathbb{Z}$ tels que $m \equiv n \pmod q$, 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 $m \equiv n \pmod q \implies n \equiv m \pmod q$.
iii) Transitivite : Soient $m \equiv n \pmod q$, et $n \equiv l \pmod q$, 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 $m \equiv l \pmod q$.

2. Il suffit simplement de voir que :

$$\begin{aligned} a \pmod q &= \{m \in \mathbb{Z} : \ m - a = kq \ \text{ pour un } \ k \in \mathbb{Z}\} \\ &= \{m \in \mathbb{Z} : \ m = a + kq \ \text{ pour un } \ k \in \mathbb{Z}\} \\ &= \{a + kq \ \text{ pour un } \ k \in \mathbb{Z}\} \subseteq \mathbb{Z} \end{aligned}$$

3. Soit $a \pmod q \in \mathbb{Z}/q\mathbb{Z}$. On effectue la division euclidienne de a par q. On a alors que

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

On voit que $a \equiv r \pmod q$ 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.

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

et

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

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 :

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

Donc l'operation $\boxplus$ est associative.

On doit montrer à présent que $0 \pmod q$ est bien le neutre :

$$\begin{aligned}a \pmod q \boxplus 0 \pmod q &= a+0 \pmod q = a \pmod q\\ &= 0+a \pmod q = 0 \pmod q \boxplus a \pmod q.\end{aligned}$$

Donc $0 \pmod q$ est bien l'élément neutre pour $\boxplus$.

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

$$a \pmod q \boxplus \boxminus a \pmod q = a-a \pmod q = 0 \pmod q$$

et

$$\boxminus a \pmod q \boxplus a \pmod q = -a+a \pmod q = 0 \pmod q.$$

Donc $\boxminus a \pmod q$ est l'inverse de $a \pmod q$.

Et enfin, on a que

$$\begin{aligned}a \pmod q \boxplus b \pmod q &= a+b \pmod q\\ &= b+a \pmod q = b \pmod q \boxplus a \pmod q.\end{aligned}$$

Et on obtient ainsi un groupe commutatif, comme voulu.

6. On raisonne par récurrence sur n.
On voit que $a \pmod q = 1 \cdot a \pmod q$.
Supposons à présent que $\sum_{i=1}^{n} a \pmod q = n \cdot a \pmod q$. Montrons que $\sum_{i=1}^{n+1} a \pmod q = (n+1) \cdot a \pmod q$ (avec $\sum_{i=1}^{n} a \pmod q :=$

$$\underbrace{(a \pmod q \boxplus \cdots \boxplus a \pmod q)}_{n \quad \text{fois}}$$

.
$\sum_{i=1}^{n+1} a \pmod q = \sum_{i=1}^{n} a \pmod q \boxplus a \pmod q$
$= n \cdot a \pmod q + a \pmod q = (n \cdot a + a) \pmod q = (n+1) \cdot a \pmod q$.
Ce qui conclut la récurrence.

7. $\mathbb{Z}.1 \pmod q := \{n.1 \pmod q,\ n \in \mathbb{Z}\}$. On se rappelle que

$$\mathbb{Z}/q\mathbb{Z} = \{r + q\mathbb{Z}, r \in \{0, 1, \cdots, q-1\}\}$$

$\boxed{\mathbb{Z}.1 \pmod q \subseteq \mathbb{Z}/q\mathbb{Z}}$: soit $n \in \mathbb{Z}$. Alors il existe un unique $r \in \{0, 1, \cdots, q-1\}$ tel que $n \pmod q = r \pmod q$, ce qui implique que $n \pmod q \in \mathbb{Z}/q\mathbb{Z}$.

$\boxed{\mathbb{Z}.1 \pmod q \supseteq \mathbb{Z}/q\mathbb{Z}}$: Soit $r \in \{0, 1, \cdots, q-1\}$. Alors $r \pmod q = r \cdots 1 \pmod q$, par 6. Donc $r \pmod q \in \mathbb{Z}.1 \pmod q$.

8. Le théorème de Bezout affirme qu'il existe $n, m \in \mathbb{Z}$ tels que $na + mq = 1 \iff 1 - na = mq \iff na \pmod q = 1 \pmod q$.
Considérons alors $A := \{r \cdot na \pmod q, r \in \{0, 1, \cdots, q-1\}\} \subseteq \mathbb{Z} \cdot a \pmod q$.
Mais puisque $na \pmod q = 1 \pmod q$, on obtient que

$$A = \{r \cdot 1 \pmod q, r \in \{0, 1, \cdots, q-1\} = \{r \pmod q, r \in \{0, 1, \cdots, q-1\} = \mathbb{Z}/q\mathbb{Z}$$

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).

Solution : . Pour n = 1 : $G = \{e\}$. Le tableau est le suivant

$\star$	e
e	e

.

En effet, on a que $e \star e = e$, car e est le neutre.

Pour n = 2 : $G = \{e, g_1\}$. Et le tableau donne :

$\star$	e	g_1
e	e	g_1
g_1	g_1	$g_1^2 = e$

.

Il est clair que $g_1 \star e = e \star g_1 = g_1$.
Supposons que $g_1 \star g_1 = g_1$. Mais alors $g_1 = g_1 \star (g_1)^{-1} = e$, et on on aurait $g_1 = e$. Ce qui est une contradiction.

Pour n = 3 : $G = \{e, g_1, g_2\}$. Le tableau est :

$\star$	e	g_1	g_2
e	e	g_1	g_2
g_1	g_1	$g_1 \star g_1 = g_2$	$g_2 \star g_1 = e$
g_2	g_2	$g_1 \star g_2 = e$	$g_2 \star g_2 = g_1$

.

Encore une fois, il est clair que $e \star g_i = g_i \star e = g_i$, pour $i = 1, 2$.
Considérons à présent le sous-groupe engendré par g_1 : $\langle g_1 \rangle \leqslant G$.
Le theoreme de Lagrange affirme que $|\langle g_1 \rangle|$ divise $|G| = 3$, alors son cardinal est soit 1, soit 3. Puisque $g_1 \neq e$, on a que $|\langle g_1 \rangle| = 3$.
Par conséquent, si $g_1^2 = e$, on aurait que $|\langle g_1 \rangle| = 2$, ce qui est absurde. Et si $g_1^2 = g_1$, on obtiendrait $g_1 = e$, ce qu'on a supposé faux. Par conséquent, on obtient que $g_1^2 = g_2$.
Par symétrie, $g_2^2 = g_1$.
Et donc $g_1 \star g_2 = g_1 \star g_1^2 = g_1^3 = e$, car g_1 est d'ordre 3. De la même manière, $g_2 \star g_1 = e$.