Université Aix-Marseille 2019–2020

Licence – Mathématiques
Algèbre 2

TD2 : Groupes
corrigé partiel

Exercice 1.
Dans chaque cas, il s'agira de vérifier que l'opération :

i. est bien défnie, c'est-à-dire qu'à toute paire d'éléments de l'ensemble considéré, elle associe bien un élément de ce même ensemble ;
ii. est associative ;
iii. possède un élément neutre ;
iv. possède un inverse pour tout élément de l'ensemble ;
v. est ou n'est pas commutative.

Pour chaque question, nous reprendrons donc chacun de ces points.

1. i. Pour tous $x, y \in]-1,1[$, on a $1-x, 1-y > 0$ et donc $0 < (1-x)(1-y) = 1-x-y+xy$, dont on déduit que $x+y < 1+xy$. Or $xy > -1$, on a donc $1+xy > 0$ et, par division, $\frac{x+y}{1+xy} < 1$. En appliquant cette inégalité à $-x, -y$, lesuels sont également dans $]-1,1[$, on obtient $-\frac{x+y}{1+xy} < 1$ et donc $\frac{x+y}{1+xy} > -1$. Au final, on a bien $x * y \in]-1,1[$.
   ii. Pour tous $x, y, z \in]-1,1[$, on a
   $$(x*y)*z = \frac{x*y+z}{1+(x*y)z} = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z} = \frac{\frac{x+y+z(1+xy)}{1+xy}}{\frac{1+xy+(x+y)z}{1+xy}} = \frac{1+x+y+z}{1+xy+yz+xz}$$
   et
   $$x*(y*z) = \frac{x+y*z}{1+x(y*z)} = \frac{x+\frac{y+z}{1+yz}}{1+x\frac{y+z}{1+yz}} = \frac{\frac{x(1+yz)+y+z}{1+yz}}{\frac{1+yz+x(y+z)}{1+yz}} = \frac{1+xyz}{1+xy+yz+xz}.$$
   Au final, on a bien $(x*y)*z = x*(y*z)$.
   v. Pour tous $x, y \in]-1,1[$, on a $x*y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y*x$. L'opération est donc commutative.
   iii. Pour tout $x \in]-1,1[$, on a $x*0 = 0*x = \frac{0+x}{1+0x} = x$, la première égalité provenant de la commutativité de $*$. L'élément 0 est donc un élément neutre pour $*$.
   iv. Pour tout $x \in]-1,1[$, on a $(-x)*x = x*(-x) = \frac{x-x}{1-x^2} = 0$ qui est un élément neutre, la première égalité provenant de la commutativité de $*$. L'élément $-x \in]-1,1[$ est donc un inverse pour x.
2. i.,v. Pour tout $(x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$, il est clair que $(x_1+y_1, x_2e^{y_1}+y_2e^{x_1}) \in \mathbb{R}^2$, ainsi que $(x_1,x_2)*(y_1,y_2) = (y_1,y_2)*(x_1,x_2)$.
   ii. Pour tous $(x_1,x_2), (y_1,y_2), (z_1,z_2) \in \mathbb{R}^2$, on a
   $$\begin{aligned}(x_1,x_2)*\big((y_1,y_2)*(z_1,z_2)\big) &= (x_1,x_2)*\big(y_1+z_1, y_2e^{z_1}+z_2e^{y_1}\big)\\ &= \big(x_1+y_1+z_1, x_2e^{y_1+z_1}+(y_2e^{z_1}+z_2e^{y_1})e^{x_1}\big)\\ &= \big(x_1+y_1+z_1, x_2e^{y_1+z_1}+y_2e^{x_1+z_1}+z_2e^{x_1+y_1}\big)\\ &= \big(z_1+x_1+y_1, z_2e^{x_1+y_1}+x_2e^{z_1+y_1}+y_2e^{z_1+x_1}\big)\\ &= (z_1,z_2)*\big((x_1,x_2)*(y_1,y_2)\big) = \big((x_1,x_2)*(y_1,y_2)\big)*(z_1,z_2),\end{aligned}$$
   l'avant-dernière égalité étant obtenue en permutant cycliquement les notations x, y et z dans les calculs précédents, et la dernière égalité par commutativité de $*$.

iii. Pour tout $(x_1, x_2) \in \mathbb{R}^2$, on a

$$(0,0) * (x_1, x_2) = (x_1, x_2) * (0,0) = \big(x_1 + 0, x_2 e^0 + 0 e^{x_1}\big) = (x_1, x_2),$$

la première égalité provenant de la commutativité de $*$. L'élément $(0,0)$ est donc un élément neutre.

iv. Pour tout $(x_1, x_2) \in \mathbb{R}^2$, on a

$$\begin{aligned}(-x_1, -x_2 e^{-2x_1}) * (x_1, x_2) &= (x_1, x_2) * (-x_1, -x_2 e^{-2x_1}) = \big(x_1 - x_1, x_2 e^{-x_1} - x_2 e^{-2x_1} e^{x_1}\big) \\ &= \big(x_1 - x_1, x_2 e^{-x_1} - x_2 e^{-x_1}\big) = (0,0),\end{aligned}$$

qui est un élément neutre, la première égalité provenant de la commutativité de $*$. L'élément $(-x_1, -x_2 e^{-2x_1})$ est donc un inverse pour (x_1, x_2).

3. i. Soit $f_1 : (x \mapsto a_1 x + b_1)$ et $f_2 : (x \mapsto a_2 x + b_2)$ deux éléments de L. Alors on a $f_1 \circ f_2 : (x \mapsto f_1(a_2 x + b_2) = a_1 a_2 x + a_1 b_2 + b_1)$ qui est bien dans L puisque $a_1 a_2 \in \mathbb{R}^*$ et $a_1 b_2 + b_1 \in \mathbb{R}$.

ii. Pour toutes applications de $\mathbb{R}$ dans $\mathbb{R}$, la composition est une opération associative. C'est donc notamment vrai pour les éléments de L.

iii. La fonction identité Id : $(x \mapsto x = 1.x + 0)$ est bien dans L, et c'est clairement un élément neutre pour la composition.

iv. Soit $f : (x \mapsto ax + b)$ un élément de L. En posant $g : \big(x \mapsto \frac{1}{a}x - \frac{b}{a}\big) \in L$, on a, pour tout $x \in \mathbb{R}$,

$$\big(f \circ g\big)(x) = f\left(\frac{1}{a}x - \frac{b}{a}\right) = a\frac{1}{a}x - a\frac{b}{a} + b = x$$

et

$$\big(g \circ f\big)(x) = g(ax + b) = \frac{1}{a}ax + \frac{1}{a}b - \frac{b}{a} = x.$$

L'élément g est donc un inverse pour f.

v. Ce groupe n'est pas abélien car, en prenant par exemple $f : (x \mapsto x + 1)$ et $g = (x \mapsto 2x)$, $f \circ g : (x \mapsto 2x + 1)$ et $g \circ f : (x \mapsto 2x + 2)$ sont deux applications distinctes.

4. Pour commencer, on remarque, pour tout $A, B \subset E$, que $x \in A\Delta B$ ssi x est exclusivement dans l'un des deux ensembles, c'est-à-dire que soit x est dans A mais pas dans B, soit il est dans B mais pas dans A. A l'inverse, $x \notin A\Delta B$ ssi x est soit dans les deux ensembles, soit dans aucun.

i.,v. Pour tout $A, B \subset E$, il est clair que $A\Delta B$ est bien un sous-ensemble de E, et que $A\Delta B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B\Delta A$.

ii. Soit $A, B, C \subset E$. Montrons par double inclusion que

$$A\Delta(B\Delta C) = \Big((A \cup B \cup C) \setminus \big((A \cap B) \cup (B \cap C) \cup (C \cap A)\big)\Big) \cup (A \cap B \cap C).$$

Notons F ce dernier ensemble. Soit $x \in A\Delta(B\Delta C)$. Il y a alors plusieurs possibilités :

cas 1 : x est dans A mais pas dans $B\Delta C$; il y a alors encore deux cas :

cas 1.1 : x est dans A, B et C ; alors il est dans $A \cap B \cap C$, donc dans F ;

cas 1.2 : x est dans A mais ni dans B ni dans C ; alors $x \in A \subset A \cup B \cup C$ mais il n'est dans aucun des ensembles $A \cap B$, $A \cap C$ et $B \cap C$. Il est donc dans

$$\Big((A \cup B \cup C) \setminus \big((A \cap B) \cup (B \cap C) \cup (C \cap A)\big)\Big) \subset F \ ;$$

cas 2 : x est dans $B\Delta C$ mais pas dans A ; il y a alors encore deux cas :

cas 2.1 : x est dans B mais ni dans C, ni dans A ; alors en raisonnant comme dans le cas 1.2, on obtient $x \in F$;

cas 2.1 : x est dans C mais ni dans B, ni dans A ; alors en raisonnant comme dans le cas 1.2, on obtient $x \in F$.

Dans tous les cas, $x \in F$. On en déduit donc que $A\Delta(B\Delta C) \subset F$.

Réciproquement, soit $x \in F$. Il y a alors deux cas :

cas 1 : $x \in \Big((A\cup B\cup C)\setminus\big((A\cap B)\cup(B\cap C)\cup(C\cap A)\big)\Big)$; alors x est exclusivement dans l'un des trois ensembles. S'il est dans A, il n'est alors pas dans $B\cup C$, donc pas dans $B\Delta C$, et donc dans $A\Delta(B\Delta C)$. S'il est dans B (resp. C), alors il n'est pas dans C (resp. B) et il est donc dans $B\Delta C$; mais comme il n'est pas dans A, il est donc dans $A\Delta(B\Delta C)$;

cas 2 : $x \in A\cap B\cap C$; alors il n'est pas dans $B\Delta C$, mais comme il est dans A, il est donc dans $A\Delta(B\Delta C)$.

Dans tous les cas, $x \in A\Delta(B\Delta C)$. On en déduit donc que $A\Delta(B\Delta C) = F$.

Maintenant, on peut remarquer que par définition, F est invariant par permutation cyclique de A, B et C. On en déduit que que $A\Delta(B\Delta C) = C\Delta(A\Delta B)$ et donc, par commutativité de Δ, que $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

iii. Pour tout $A\subset E$, on a $\Delta A = A\Delta\emptyset = (A\cup\emptyset)\setminus(A\cap\emptyset) = A\setminus\emptyset = A$. L'ensemble vide est donc un élément neutre pour Δ.

iv. Pour tout $A\subset E$, on a $A\Delta A = (A\cup A)\setminus(A\cap A) = A\setminus A = \emptyset$, qui est un élément neutre. Tout sous-ensemble de E est donc un inverse pour soi-même.

Exercice 5.

1. Si $H = n\mathbb{Z}$ avec $n > 0$, alors n est le plus petit élément strictement positif de H, c'est-à-dire $n = \min H\cap\mathbb{N}^*$. Cela permet de caractériser n à partir de H, ce qui sera clairement d'une grande aide pour montrer le résultat.

   On commence donc par considérer $H\cap\mathbb{N}^*$. Si cet ensemble est vide, alors $H = \{0\}$ car s'il contient un élément non nul, il contient également son opposé et, parmi les deux, l'un est nécessairement dans $\mathbb{N}^*$; on a alors $H = 0\mathbb{Z}$. S'il est non vide, alors il contient un plus petit élément que l'on note n. Puisque H est stable par addition et par opposé, il contient alors également tous les multiples de n et on a $n\mathbb{Z}\subset H$.

   Réciproquement, soit $k\in H$. On note $k = qn + r$ la division euclidienne de k par n. Alors $r = k - qn \in H$ puisque $k, qn \in H$. Or $r \in [\![0, n-1]\!]$, donc par minimalité de n, on a $r = 0$ et donc $k = qn \in n\mathbb{Z}$. On en déduit que $H\subset n\mathbb{Z}$ et donc que $H = n\mathbb{Z}$.
2. Les éléments de $\langle a, b\rangle$ sont les combinaisons linéaires (à coefficients entiers) de a et b, ils sont donc tous divisibles par $\mathrm{pgcd}(a,b)$, c'est-à-dire tous dans $\mathrm{pgcd}(a,b)\mathbb{Z}$. Mais réciproquement, d'après le théorème de Bachet–Bézout, $\mathrm{pgcd}(a,b)$ est une combinaison linéaire de a et b, c'est donc un élément de $\langle a,b\rangle$, de même que tous ses multiples. On en déduit par double inclusion que $\langle a,b\rangle = \mathrm{pgcd}(a,b)\mathbb{Z}$.

   Un élément de $a\mathbb{Z}\cap b\mathbb{Z}$ est simultanément un multiple de a et de b, c'est donc un multiple de $\mathrm{ppcm}(a,b)$, donc un élément de $\mathrm{ppcm}(a,b)\mathbb{Z}$. Mais réciproquement, tout multiple de $\mathrm{ppcm}(a,b)$ est simultanémént un multiple de a et de b, donc un élément de $a\mathbb{Z}\cap b\mathbb{Z}$. On en déduit par double inclusion que $a\mathbb{Z}\cap b\mathbb{Z} = \mathrm{ppcm}(a,b)\mathbb{Z}$.
3. Par récurrence immédiate sur $n\in N^*$, on obtient de la question précédente que $\langle a_1,\dots,a_n\rangle = \mathrm{pgcd}(a_1,\dots,a_n)\mathbb{Z}$ et que $\cap_{1\le i\le n} a_i\mathbb{Z} = \mathrm{ppcm}(a_1,\dots,a_n)\mathbb{Z}$.

Exercice 12.

1. Pour tout $n\in\mathbb{N}^*$, on a $g_1^n = e \Leftrightarrow \left(g_1^{-1}\right)^n = g_1^{-n} = e$. Les ensembles $\{n\in\mathbb{N}^* \mid g_1^n = e\}$ et $\{n\in\mathbb{N}^* \mid \left(g_1^{-1}\right)^n = e\}$ sont donc identiques, de même que leurs plus petits éléments. On a donc bien $|g_1| = |g_1^{-1}|$.
2. Pour tout $n\in\mathbb{N}^*$, on a $\left(g_2.g_1.g_2^{-1}\right)^n = g_2.g_1^n.g_2^{-1}$. Donc si $g_1^n = e$, alors $\left(g_2.g_1.g_2^{-1}\right)^n = g_2.e.g_2^{-1} = e$, et si $\left(g_2.g_1.g_2^{-1}\right)^n = e$, alors $g_2.g_1^n.g_2^{-1} = e$ et donc $g_1^n = g_2^{-1}.g_2 = e$. Les ensembles $\{n\in\mathbb{N}^* \mid g_1^n = e\}$ et $\{n\in\mathbb{N}^* \mid \left(g_2.g_1.g_2^{-1}\right)^n = e\}$ sont donc identiques, de même que leurs plus petits éléments. On a donc bien $|g_1| = |g_1.g_1.g_2^{-1}|$.
3. Il suffit d'utiliser la question précédente avec "$g_1 = g_1.g_2$", ou bien d'utiliser la question 2. de l'exercice 4.
4. (a) Rappelons que, pour tout $k\in\mathbb{N}$ et $g\in G$, $k.g$ est la somme itérée k fois de g avec lui-même. Par définition de l'ordre, on a donc $|g_1|.g_1 = |g_2|.g_2 = 0$, et donc $(|g_1|.|g_2|).(g_1+g_2) = (|g_1|.|g_2|).g_1 + (|g_1|.|g_2|).g_2 = |g_2|.\big(|g_1|.g_1\big) + |g_1|.\big(|g_2|.g_2\big) = |g_2|.0 + |g_1|.0 = 0$. L'élément g_1+g_2 est donc d'ordre fini, avec $|g_1+g_2| \le |g_1|.|g_2|$.

Réciproquement, soit $k \in \mathbb{N}^*$ tel que $k.(g_1 + g_2) = 0$, alors $k.g_1 = -k.g_2 = k.(-g_2)$, et donc $\big(k.|g_1|\big).(-g_2) = |g_1|.\big(k.(-g_2)\big) = |g_1|.(k.g_1) = k.\big(|g_1|.g_1\big) = k.0 = 0$. L'entier $k.|g_1|$ est donc un multiple de $|-g_2| = |g_2|$, mais $|g_1|$ et $|g_2|$ étant premiers entre eux, on en déduit du lemme de Gauss que $|g_2|$ divise k. De même, on montre que $|g_1|$ divise k. L'entier k est donc un multiple commun de $|g_1|$ et $|g_2|$, donc un multiple de $\mathrm{ppcm}\big(|g_1|, |g_2|\big) = \frac{|g_1|.|g_2|}{\mathrm{pgcd}\big(|g_1|,|g_2|\big)} = |g_1|.|g_2|$. On a donc $|g_1 + g_2| \geq |g_1|.|g_2|$, et donc $|g_1 + g_2| = |g_1|.|g_2|$.

(b) Dans $\mathbb{Z}/2\mathbb{Z}$, en prenant $g_1 = g_2 = 1$, on a $g_1 + g_2 = 0$ et donc $|g_1| = |g_2| = 2$, mais $|g_1 + g_2| = 1 \neq \mathrm{ppcm}(2, 2)$. Dans $\mathbb{Z}/8\mathbb{Z}$, en prenant par exemple $g_1 = g_2 = 2$, on a $|g_1| = |g_2| = 4$ mais $|g_1 + g_2| = 2 \neq \mathrm{ppcm}(4, 4)$.

Dans tous les cas, on observe que la condition $\mathrm{pgcd}(|g_1|, |g_2|) = 1$ est bien nécessaire pour conclure dans la question précédente.

(c) Dans $\mathfrak{S}_3$, on peut considérer $\sigma_1 := (12)$ et $\sigma_2 := (123)$. On a alors $|\sigma_1| = 2$ et $|\sigma_2| = 3$, donc $\mathrm{pgcd}(|\sigma_1|, |\sigma_2|) = 1$. Or $\sigma_1 \circ \sigma_2 = (23)$, et donc $|\sigma_1 \circ \sigma_2| = 2 \neq 6 = \mathrm{ppcm}(2, 3)$.

On observe donc que la caractère abélien de G est bien nécessaire pour conclure dans la question (a).

Exercice 13.

- D'après les formules de conjugaison dans $\mathbb{C}$, pour tout $z_1, z_2 \in \mathbb{C}$, on a $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$ et $\overline{z_1.z_2} = \overline{z}_1.\overline{z}_2$. Les deux applications sont donc bien des morphismes de groupes.
- Pour tout $z_1, z_2 \in \mathbb{C}$, on a $|z_1.z_2| = |z_1|.|z_2|$ mais, en général, $|z_1 + z_2| \neq |z_1| + |z_2|$ (par exemple, pour $z_1 = 1$ et $z_2 = -1$). On en déduit que la seconde application est un morphisme de groupe mais pas la première.
- Notons

$$f_0\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & (\{\pm 1\}, .) \\ n & \longmapsto & \begin{cases} 1 & \text{si } n \text{ pair} \\ -1 & \text{si } n \text{ impair} \end{cases} \end{array} \quad \text{et} \quad f_1\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & (\{\pm 1\}, .) \\ n & \longmapsto & \begin{cases} 1 & \text{si } n \text{ impair} \\ -1 & \text{si } n \text{ pair} \end{cases} \end{array},$$

et considérons $n_1, n_2 \in \mathbb{Z}$. Si n_1 et n_2 sont tous les deux pairs ou tous les deux impaires, alors $n_1 + n_2$ est pair et on a $f_0(n_1 + n_2) = 1 = (\pm 1)^2 = f_0(n_1).f_0(n_2)$. Si n_1 et n_2 sont de parité différentes, alors $n_1 + n_2$ est impair et on a $f_0(n_1 + n_2) = -1 = (\pm 1).(\mp 1) = f_0(n_1).f_0(n_2)$. Dans tous les cas, on a bien $f_0(n_1 + n_2) = f_0(n_1).f_0(n_2)$ et f_0 est un morphisme de groupes. Par contre, on a $f_1(0.0) = f_1(0) = -1 \neq 1 = (-1).(-1) = f_1(0).f_1(0)$, l'application f_1 n'en est donc pas un.
- Notons

$$g_\infty\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & n^2 \end{array}, \quad g_2\colon \begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ \overline{n} & \longmapsto & \overline{n}^2 \end{array} \quad \text{et} \quad g_3\colon \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \\ \overline{n} & \longmapsto & \overline{n}^2 \end{array}.$$

Alors $g_\infty(1 + 1) = g_\infty(2) = 4 \neq 2 = g_\infty(1) + g_\infty(1)$; donc g_∞ n'est pas un morphisme de groupes. De même, $g_3(\overline{1} + \overline{1}) = g_3(\overline{2}) = \overline{4} = \overline{1} \neq \overline{2} = g_3(\overline{1}) + g_3(\overline{1})$ et g_3 n'est pas un morphisme de groupes. Par contre, $g_2(\overline{0}) = \overline{0}$ et $g_2(\overline{1}) = \overline{1}$. On a donc $g_2 = \mathrm{Id}_{\mathbb{Z}/2\mathbb{Z}}$, qui est bien un morphisme de groupes, et même un automorphisme de groupe.
- Pour toutes matrices M_1 et M_2, on a $\det(M_1.M_2) = \det(M_1).\det(M_2)$ mais, en général, $\det(M_1 + M_2) \neq \det(M_1) + \det(M_2)$ (en prenant, par exemple, M_1 la matrice identité et M_2 son opposé). On en déduit que la seconde application est un morphisme de groupe, mais pas la première.
- Pour toutes matrices M_1 et M_2, on a $\mathrm{Tr}(M_1 + M_2) = \mathrm{Tr}(M_1) + \mathrm{Tr}(M_2)$ mais, en général, $\mathrm{Tr}(M_1.M_2) \neq \mathrm{Tr}(M_1).\mathrm{Tr}(M_2)$ (en prenant, par exemple, $n \geq 2$ et la matrice identité pour M_1 et M_2). On en déduit que la première application est un morphisme de groupe, mais pas la seconde.
- Pour toutes applications f_1 et f_2 dérivables sur $\mathbb{R}$, on a $(f_1 + f_2)' = f_1' + f_2'$ mais, en général, $(f_1.f_2)' = f_1.f_2' + f_1'.f_2 \neq f_1'.f_2'$ (en prenant, par exemple, l'identité pour f_1 et f_2). On en déduit que la première application est un morphisme de groupe, mais pas la seconde.

Exercice 14.

1. Pour que f soit bien définie, il faut que son image $\overline{3k}$ ne dépende pas du choix k du représentant de $\overline{k}$. Considérons donc un autre représentant k'. Alors $k-k'$ est un multiple de 8, et $3k-3k' = 3(k-k')$ un multiple de $3.8 = 24$, donc un multiple de 12. On a alors bien $\overline{3k'} = \overline{3k}$ dans $\mathbb{Z}/_{12\mathbb{Z}}$.
2. Pour tous $\overline{k}_1, \overline{k}_2 \in \mathbb{Z}/_{8\mathbb{Z}}$, on a $f(\overline{k}_1 + \overline{k}_2) = f(\overline{k_1 + k_2}) = \overline{3(k_1 + k_2)} = \overline{3k_1} + \overline{3k_2} = f(\overline{k}_1) + f(\overline{k}_2)$. L'application f est donc bien un morphisme de groupes.
3. On a
$$f(\overline{0}) = \overline{0} \qquad f(\overline{1}) = \overline{3} \qquad f(\overline{2}) = \overline{6} \qquad f(\overline{3}) = \overline{9}$$
$$f(\overline{4}) = \overline{12} = \overline{0} \qquad f(\overline{5}) = \overline{15} = \overline{3} \qquad f(\overline{6}) = \overline{18} = \overline{6} \qquad f(\overline{7}) = \overline{21} = \overline{9}.$$
On en déduit que $\mathrm{Im}(f) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}\left(\subset \mathbb{Z}/_{12\mathbb{Z}}\right)$ et $\mathrm{Ker}(f) = \{\overline{0}, \overline{4}\}\left(\subset \mathbb{Z}/_{8\mathbb{Z}}\right)$.

Exercice 15.
On rappelle que, pour $f_1, f_2 \in \mathcal{F}(\mathbb{R}, \mathbb{R})$,
$$f_1 + f_2 : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f_1(x) + f_2(x) \end{array}.$$
Dans la suite, on notera $0_{\mathbb{R}} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 0 \end{array}$ et, pour tout $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$, $-f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & -f(x) \end{array}$.

1. Pour tous $f_1, f_2, f_3 \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ et tout $x \in \mathbb{R}$, on a
$$\big((f_1 + f_2) + f_3\big)(x) = \big(f_1(x) + f_2(x)\big) + f_3(x) = f_1(x) + \big(f_2(x) + f_3(x)\big) = \big(f_1 + (f_2 + f_3)\big)(x).$$
L'addition est donc associative sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$. De plus, $0_{\mathbb{R}}$ est un élément neutre, et $-f$ est un inverse pour tout $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$. L'addition munit donc bien $\mathcal{F}(\mathbb{R}, \mathbb{R})$ d'une structure de groupe.
2. Pour tous $f_1, f_2 \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ et tout $x \in \mathbb{R}$, on a
$$\begin{aligned} \sigma(f_1 + f_2)(x) &= \frac{1}{2}\big(f_1(x) + f_2(x) + f_1(-x) + f_2(-x)\big) \\ &= \frac{1}{2}\big(f_1(x) + f_1(-x)\big) + \frac{1}{2}\big(f_2(x) + f_2(-x)\big) \\ &= \sigma(f_1)(x) + \sigma(f_2)(x). \end{aligned}$$
L'application σ est donc bien un endomorphisme de groupe.
3. Soit $f \in \mathrm{Im}(\sigma)$. Alors il existe $g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ tel que, pour tout $x \in \mathbb{R}$, $f(x) = \frac{1}{2}\big(g(x) + g(-x)\big)$ et on a alors
$$f(-x) = \frac{1}{2}\big(g(-x) + g(x)\big) = \frac{1}{2}\big(g(x) + g(-x)\big) = f(x).$$
L'application f est donc paire. Réciproquement, si f est paire, alors pour tout $x \in \mathbb{R}$, $\sigma(f)(x) = \frac{1}{2}\big(f(x) + f(-x)\big) = \frac{1}{2}\big(f(x) + f(x)\big) = f(x)$ et donc $f = \sigma(f) \in \mathrm{Im}(\sigma)$. On en déduit que $\mathrm{Im}(\sigma)$ est l'ensemble des applications paires de $\mathbb{R}$ dans $\mathbb{R}$.

   Pour tout $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$, on a
$$\begin{aligned} f \in \mathrm{Ker}(\sigma) &\Leftrightarrow \forall x \in \mathbb{R}, \frac{1}{2}\big(f(x) + f(-x)\big) = 0 \\ &\Leftrightarrow \forall x \in \mathbb{R}, f(-x) = -f(x) \\ &\Leftrightarrow f \text{ est impaire.} \end{aligned}$$
On en déduit que $\mathrm{Ker}(f)$ est l'ensemble des applications impaires de $\mathbb{R}$ dans $\mathbb{R}$.