EPFL Automne 2022
Algèbre Linéaire Avancée, MATH-110

Correction Série 1

Tous les exercices seront corrigés. La correction sera postée sur le Moodle aprés environ 2 semaines.

Vous êtes fortement encouragés à essayer de résoudre (éventuellement à plusieurs) l'exercice ($\star$) et à rendre votre solution (éventuellement à plusieurs) sur Moodle avant la date indiquée, sous forme de fichier pdf.

Exercice 1. Soit X un ensemble. Pour A, B des sous-ensembles de X on defini la difference de A et B

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

(les elements de A qui ne sont pas des elements de B). En particulier

$$X - A = \{x \in X,\ x \notin A\} \subset X$$

est appelle le *complementaire* de A dans X et est note A^c.

On defini alors la difference symetrique de A et B en posant

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

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

1. Montrer que $A\Delta B = (A - B) \cup (B - A)$.
2. Calculer $\emptyset\Delta A$, $A\Delta A$, $A\Delta X$, $A\Delta A^c$.

Solution 1.

1.

$$\begin{aligned} A\Delta B &= \{x \in A \cup B,\ x \notin A \cap B\} \\ &= \{(x \in A \text{ ou } x \in B) \text{ et } (x \notin A \cap B)\} \\ &= \{(x \in A \text{ et } x \notin A \cap B) \text{ ou } (x \in B \text{ et } x \notin A \cap B)\} \\ &= \{(x \in A \text{ et } x \notin B) \text{ ou } (x \in B \text{ et } x \notin A)\} \\ &= \{(x \in A \text{ et } x \notin B)\} \cup \{(x \in B \text{ et } x \notin A)\} \\ &= (A - B) \cup (B - A) \end{aligned}$$

Peut être egalement démontré par double inclusion.

2. $\emptyset \Delta A = A$, $A \Delta A = \emptyset$, $A \Delta X = A^c$, $A \Delta A^c = X$

Exercice 2. Soit $\mathbb{Z}$ l'ensemble des entiers relatifs. Pour $A, B \in \mathscr{P}(\mathbb{Z})$ des sous-ensembles de $\mathbb{Z}$, on pose

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

l'ensemble de toutes les sommes (resp. de tous les produits) d'elements de A et de B.

Soit $q \geqslant 1$ un entier. On note $\mathbb{Z}/q\mathbb{Z} \subset \mathscr{P}(\mathbb{Z})$ les classes de congruences modulo q : c'est a dire l'ensemble des sous-ensembles de $\mathbb{Z}$ de la forme

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

1. Montrer que
$$a \,(\mathrm{mod}\, q) = a' \,(\mathrm{mod}\, q) \Longleftrightarrow a - a' = qk \text{ pour } k \in \mathbb{Z}$$
2. Soient $a \,(\mathrm{mod}\, q),\ b \,(\mathrm{mod}\, q) \in \mathbb{Z}/q\mathbb{Z}$. Montrer que
$$a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) = a + b \,(\mathrm{mod}\, q),$$
$$a \,(\mathrm{mod}\, q) \boxtimes b \,(\mathrm{mod}\, q) \subset a.b \,(\mathrm{mod}\, q).$$
3. Donner un exemple ou cette derniere inclusion est stricte (n'est pas une egalite). Donner un exemple (avec $q \neq 1$) ou cette derniere inclusion est une egalite.

Solution 2.

1.
$$\begin{aligned}
& a - a' = qk \text{ pour } k \in \mathbb{Z} \\
\Leftrightarrow\quad & a = a' + qk \text{ pour } k \in \mathbb{Z} \\
\Leftrightarrow\quad & \{a + qm,\ m \in \mathbb{Z}\} = \{a' + qk + qm,\ m \in \mathbb{Z}\} \text{ pour } k \in \mathbb{Z} \\
\Leftrightarrow\quad & \{a + qm,\ m \in \mathbb{Z}\} = \{a' + q(k + m),\ m \in \mathbb{Z}\} \text{ pour } k \in \mathbb{Z} \\
\Leftrightarrow\quad & \{a + qm,\ m \in \mathbb{Z}\} = \{a' + qm',\ m' \in \mathbb{Z}\} \\
\Leftrightarrow\quad & a \,(\mathrm{mod}\, q) = a' \,(\mathrm{mod}\, q)
\end{aligned}$$

2. Par définition des classes modulo q :
$$\begin{aligned}
a \,(\mathrm{mod}\, q) \boxplus b \,(\mathrm{mod}\, q) &= \{x + y \mid x \in a \,(\mathrm{mod}\, q), y \in b \,(\mathrm{mod}\, q)\} \\
&= \{(a + qk_1) + (b + qk_2) \mid k_1, k_2 \in \mathbb{Z}\} \\
&= \{a + b + q(\underbrace{k_1 + k_2}_{=k \in \mathbb{Z}}) \mid k_1, k_2 \in \mathbb{Z}\} \\
&= \{a + b + qk \mid k \in \mathbb{Z}\} \\
&= (a + b) \,(\mathrm{mod}\, q)
\end{aligned}$$

et

$$\begin{aligned} a \,(\mathrm{mod}\, q) \boxtimes b \,(\mathrm{mod}\, q) &= \{(a+qk_1)(b+qk_2) \mid k_1, k_2 \in \mathbb{Z}\} \\ &= \{ab + qk_1b + qk_2a + q^2k_1k_2 \mid k_1, k_2 \in \mathbb{Z}\} \\ &= \{ab + q(\underbrace{k_1b + k_2a + q^2k_1k_2}_{\in \mathbb{Z}}) \mid k_1, k_2 \in \mathbb{Z}\} \\ &\subset \{ab + qk \mid k \in \mathbb{Z}\} \end{aligned}$$

La derniere inclusion n'est pas une égalité parce qu'en général les nombres de la forme $k_1b + k_2a + q^2k_1k_2$ n'incluent pas tous les entiers relatifs.

3. Pour l'inclusion stricte : On prend $q = 4,\ a = 2,\ b = 2$ ou d'autres entiers avec $pgcd(a, b, q) > 1$. On a

$$\begin{aligned} 2 \,(\mathrm{mod}\, 4) \boxtimes 2 \,(\mathrm{mod}\, 4) &= \{(2+4k_1)(2+4k_2) \mid k_1, k_2 \in \mathbb{Z}\} \\ &= \{4 + 4(\underbrace{2k_1 + 2k_2 + 16k_1k_2}_{\in 2\mathbb{Z}}) \mid k_1, k_2 \in \mathbb{Z}\} \\ &\neq \{4 + 4k \mid k \in \mathbb{Z}\} \end{aligned}$$

Pour l'égalité : On prend $q = 3,\ a = 1,\ b = 1$ ou d'autres entiers avec $pgcd(a, b, q) = 1$. On a

$$\begin{aligned} 1 \,(\mathrm{mod}\, 3) \boxtimes 1 \,(\mathrm{mod}\, 3) &= \{(1+3k_1)(1+3k_2) \mid k_1, k_2 \in \mathbb{Z}\} \\ &= \{1 + 3(k_1 + k_2 + 9k_1k_2) \mid k_1, k_2 \in \mathbb{Z}\} \\ &= \{1 + 3k_1 \mid k_1 \in \mathbb{Z}\} \end{aligned}$$

Pour la derniere égalité il suffit de considérer le cas $k_2 = 0$. (En général on utilise Bézout.)

Exercice 3. Soit

$$\mathbb{Q} = \{\frac{p}{q},\ (p, q) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})\}$$

l'ensemble des nombres rationels.

1. On considere l'application

$$2^{(\bullet,\bullet)} : (p, q) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mapsto 2^{(p,q)} := (2^p)^{1/q} \in \mathbb{R}_{>0}.$$

Montrer que cette application permet de definir une application de $\mathbb{Q}$ vers $\mathbb{R}_{>0}$ notée

$$2^{\bullet} : x \in \mathbb{Q} \to 2^x \in \mathbb{R}_{>0}$$

qui vérifie pour tout $(p, q) \in\in \mathbb{Z} \times (\mathbb{Z} - \{0\})$

$$2^{p/q} = 2^{(p,q)}.$$

2. On considere l'application

$$(p,q) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mapsto p+q \in \mathbb{Z}.$$

Pourquoi cette application ne permet-elle pas de definir une application de $\mathbb{Q}$ vers $\mathbb{Z}$ en posant $p/q \mapsto (p,q) \mapsto p+q$?

Solution 3.

1. Ce qu'on veut nous faire démontrer ici c'est que le "procédé d'association" $x = \frac{p}{q} \in \mathbb{Q} \longrightarrow (p,q) \in \mathbb{Z} \times \mathbb{Z}^* \longrightarrow 2^{(p,q)} = (2^p)^{1/q}$ est bien défini et forme donc une application, i.e. si on écrit $x \in \mathbb{Q}$ de deux formes différentes $x = \frac{p}{q}$ et $x = \frac{a}{b}$ alors on aura $(2^p)^{1/q} = (2^a)^{1/b}$ et donc on pourra noter $2^x = 2^{p/q}$ cette unique valeur. Par définition de $\mathbb{Q}$, nous savons que $\frac{p}{q} = \frac{a}{b} \iff a = pk$ et $b = qk$ pour un certain $k \in \mathbb{Z}$. Faisons une petite disjonction des cas :
   - Cas $x = 0$, i.e. $p = a = 0$: alors $(2^p)^{1/q} = (2^0)^{1/q} = 1^{1/q} = 1 = 1^{\frac{1}{qk}} = (2^0)^{\frac{1}{qk}} = (2^a)^{1/b}$ ✓
   - Cas $x \neq 0$: alors par propriétés des puissances rélles (ou des racines k-ièmes si certains préferent)

$$(2^p)^{1/q} = (((2^p)^k)^{1/k})^{1/q} = (2^{pk})^{\frac{1}{k}\cdot\frac{1}{q}} = (2^a)^{1/b}$$

   ✓
2. Cette appliaction n'est pas bien définie car pour $x = \frac{1}{2} = \frac{10329}{20658} \in \mathbb{Q}$ l'image n'est pas unique : $1 + 2 = 3 \neq 30987 = 10329 + 20658$.

Les éléments équivalents ont la même image, ainsi la fonction est bien définie sur le quotient $\mathbb{Q}$.

Exercice 4. On reprend les definitions/notations de l'exercice 2 dans le cas $q = 4$.

1. On considere l'application

$$\iota^\bullet : a \in \mathbb{Z} \mapsto \iota^a \in \mathbb{C}$$

(ou ι est le nombre complexe tel que $\iota^2 = -1$). Montrer que cette application permet de definir une application de $\mathbb{Z}/4\mathbb{Z}$ vers $\mathbb{C}$ donnee par

$$\iota_4^\bullet : a \,(\mathrm{mod}\, 4) \mapsto i^a$$

et que

$$\iota^\bullet = \iota_4^\bullet \circ \pi_4.$$

(resoudre d'abord la question 1. de l'exercice 2).

Solution 4. Vérifions que $i_4^\bullet$ est bien définie.
Soit $E \in \mathbb{Z}/4\mathbb{Z}$. Il existe un unique $e \in \mathbb{N}$ tel que $0 \leqslant e < 4$ et $E = e + 4\mathbb{Z}$. Si $a \in \mathbb{Z}$ est tel que $E = a + 4\mathbb{Z}$ alors il existe $m \in \mathbb{Z}$ tel que $a = e + 4m$ (car nous nous rappelons que $a + 4\mathbb{Z} = e + 4\mathbb{Z} \iff a \equiv e \,(\mathrm{mod}\, 4) \iff 4|(a - e)$).

$$i_4^\bullet(a + 4\mathbb{Z}) = i^{e+4m} = i^e(i^4)^m = i^e 1 = i^e = i_4^\bullet(e + 4\mathbb{Z})$$

Donc $i_4^\bullet$ est bien définie.

Montrons que $i^\bullet = i_4^\bullet \circ \pi_4$.
Soit $z \in \mathbb{Z}$. Il existe un unique $k \in \mathbb{Z}$ ainsi qu'un unique $e \in \mathbb{N}$ tel que $0 \leqslant e < 4$ et $z = e + 4k$. Alors :

$$i^\bullet(z) = i^z = i^e i^{k4} = i^e,$$

$$i_4^\bullet \circ \pi_4(z) = i_4^\bullet \circ \pi_4(e + 4k) = i_4^\bullet(e + 4\mathbb{Z}) = i^e.$$

Ainsi $i^\bullet = i_4^\bullet \circ \pi_4$. □

Exercice 5. On considere l'application

$$f : x \in \mathbb{R}_{\geqslant -2} \mapsto x^3 - x \in \mathbb{R}.$$

1. Que vaut $f([-2, +\infty[)$? Que vaut $f([0, +\infty[)$?
2. Que vaut $f^{-1}([0, +\infty[)$? Que vaut $f^{-1}([-2, +\infty[)$?
3. Cette application est elle injective ?
4. Cette application est elle surjective ?
5. Comment modifier l'espace d'arrivee pour la rendre surjective ?
6. Trouver x_0 le plus petit possible pour cette application avec l'espace de depart $\mathbb{R}_{\geqslant x_0}$ soit injective.

Solution 5.

1. On peut calculer les extremum $\pm\frac{1}{\sqrt{3}}$ et les valeurs $f(1/\sqrt{3}) = \frac{-2}{3\sqrt{3}}$ et $f(-1/\sqrt{3}) = \frac{2}{3\sqrt{3}}$. Donc on obtient $f([-2, +\infty[) = [-6, +\infty[$, $f([0, +\infty[) = [\frac{-2}{3\sqrt{3}}, +\infty[$.
2. $f^{-1}([0, +\infty[) = [-1/\sqrt{3}, 0] \cup [1/\sqrt{3}, +\infty[$ et $f^{-1}([-2, +\infty[) = [\alpha, \infty[$ où α est la solution réelle de l'équation $x^3 - x = 2$.
3. L'application n'est pas injective car par example $f(0) = 0 = f(1)$.
4. L'application n'est pas surjective puisque -11 n'a pas d'antécedent.
5. L'application n'est pas surjective puisque -11 n'a pas d'antécedent (puisque $f(-2) = -10$ et la fonction est strictement croissante).

6. Pour faire en sort que l'application soit injective on prend $f : \mathbb{R}_{\geqslant \frac{1}{\sqrt{3}}} \to \mathbb{R}$.

Exercice 6. Soit $f : X \mapsto Y$ une application entre ensembles.

1. Montrer que pour tous sous-ensembles $A, B \subset X$
$$f(A \cup B) = f(A) \cup f(B).$$
2. (a) Montrer que pour tout $A, B \subset X$ des sous-ensembles, on a
$$f(A \cap B) \subset f(A) \cap f(B);$$
(b) donner un exemple pour lequel $f(A \cap B) \neq f(A) \cap f(B)$.
(c) Montrer que si f est injective on a
$$f(A \cap B) = f(A) \cap f(B).$$
3. Montrer que pour tout sous-ensembles $C, D \subset Y$ de Y on a
$$f^{(-1)}(C \cup D) = f^{(-1)}(C) \cup f^{(-1)}(D).$$
4. Montrer que pour tout pour tout sous-ensembles $C, D \subset Y$ de Y, on a
$$f^{(-1)}(C \cap D) = f^{(-1)}(C) \cap f^{(-1)}(D).$$
5. Montrer que
$$f \text{ est injective } \iff \forall A \subset X,\ f^{(-1)}(f(A)) = A.$$
6. Montrer que
$$f \text{ est surjective } \iff \forall C \subset Y,\ f(f^{(-1)}(C)) = C.$$
7. Montrer que pour $A \subset X$, on a
$$A \subset f^{(-1)}(f(A)).$$
Montrer par un exemple on n'a pas forcement l'egalite
$$A = f^{(-1)}(f(A)).$$
Soit $B \subset Y$, existe-t-il (en general) une relation d'inclusion entre B et $f(f^{(-1)}(B))$?

Solution 6. Soit $f : X \to Y$ une application ainsi que $A, B \subset X$ et $C, D \subset Y$.
Disclaimer : la correction de cet exercice est volontairement un peu longue et détaillée avec des phrases pour que vous compreniez la logique. En soit, un simple raisonnement avec uniquement des symbôles logiques pourrait suffire.

1. Montrons l'égalité par double inclusion :
   - $\subseteq$: Soit $y \in f(A \cup B)$. Par définition, il existe $x \in A \cup B$ tel que $f(x) = y$. Comme $x \in A \cup B$, alors $x \in A$ ou $x \in B$. Sans perte de généralité on peut supposer que $x \in A$ (le cas $x \in B$ se traite de manière identique par symétrie de A et B). Alors $f(x) \in f(A)$ donc $f(x) \in f(A) \cup f(B)$. Ainsi $f(A \cup B) \subseteq (f(A) \cup f(B))$ ✓
   - $\supseteq$: Soit $y \in f(A) \cup f(B)$. Sans perte de généralité on peut supposer que $y \in f(A)$ (encore une fois l'autre cas se traite par symétrie). Il existe donc $x \in A$ tel que $f(x) = y$. Comme $x \in A \cup B$ alors $f(x) \in f(A \cup B)$. Ainsi $(f(A) \cup f(B)) \subseteq f(A \cup B)$ ✓
2. (a) Soit $y \in f(A \cap B)$. Par défintion il existe $x \in A \cap B$ tel que $f(x) = y$. Comme $x \in A \cap B$, alors $x \in A$ et $x \in B$. Comme $x \in A$ alors $f(x) \in f(A)$ et comme $x \in B$ alors $f(x) \in f(B)$. Ainsi $f(x) \in f(A) \cap f(B)$ et on conclut que $f(A \cap B) \subset (f(A) \cap f(B))$ ✓.

   (b) On pose $c : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. Cette application vérifie :

$$c(\mathbb{R}_- \cap \mathbb{R}_+) = c(\{0\}) = \{0\} \subsetneq \mathbb{R}_+ = c(\mathbb{R}_-) \cap c(\mathbb{R}_+)$$

   (c) Puisque l'inclusion $f(A \cap B) \subseteq f(A) \cap f(B)$ est toujours vraie, on n'a qu'à démontrer que $f(A) \cap f(B) \subseteq f(A \cap B)$.
   Soit $y \in f(A) \cap f(B)$. Alors il existe $a \in A$ et $b \in B$ tels que $y = f(a) = f(b)$. Or f est injective donc $f(a) = f(b) \implies a = b$. Pour que ce soit possible, on doit avoir $a = b \in A \cap B$ et donc $f(a) = f(b) = y \in f(A \cap B)$. Ainsi $f(A) \cap f(B) \subseteq f(A \cap B)$✓
3. - $\subseteq$: Soit $x \in f^{(-1)}(C \cup D)$. Par définition $f(x) \in C \cup D$, i.e. $f(x) \in C$ ou $f(x) \in D$. Sans perte de généralité on peut supposer que $f(x) \in C$. Alors $x \in f^{(-1)}(C)$ et même $x \in f^{(-1)}(C) \cup f^{1}(D)$. Ainsi $f^{(-1)}(C \cup D) \subset (f^{(-1)}(C) \cup f^{(-1)}(D))$✓
   - $\supseteq$: Soit $x \in (f^{(-1)}(C) \cup f^{(-1)}(D))$. Alors $x \in f^{(-1)}(C)$ ou $x \in f^{(-1)}(D)$ et sans perte de généralité on peut supposer que $x \in f^{(-1)}(C)$. Ainsi $f(x) \in C$ et donc $f(x) \in C \cup D$. Ainsi $x \in f^{(-1)}(C \cup D)$ et finalement, $(f^{(-1)}(C) \cup f^{(-1)}(D)) \subset f^{(-1)}(C \cup D)$.✓
4. - $\subseteq$: Soit $x \in f^{(-1)}(C \cap D)$. Alors $f(x) \in C \cap D$ i.e. $f(x) \in C$ et $f(x) \in D$. Ainsi, $x \in f^{(-1)}(C)$ et $x \in f^{(-1)}(C)$, donc $x \in f^{(-1)}(C) \cap f^{(-1)}(D)$ et enfin $f^{(-1)}(C \cap D) \subset f^{(-1)}(C) \cap f^{(-1)}(D)$✓
   - $\supseteq$: Soit $x \in f^{(-1)}(C) \cap f^{(-1)}(D)$. Alors $x \in f^{(-1)}(C)$ et $x \in f^{(-1)}(D)$, donc $f(x) \in C$ et $f(x) \in D$, i.e. $f(x) \in C \cap D$. Cela implque que $x \in f^{(-1)}(C \cap D)$ et ainsi que $f^{(-1)}(C) \cap f^{(-1)}(D) \subset f^{(-1)}(C \cap D)$✓
5. Montrons que : f est injective $\iff \forall A \subset X : f^{(-1)}(f(A)) = A$.
   - $\implies$: On suppose f injective et on montre l'égalit'e par double inclusion.

— $\subseteq$: Soient $A \subseteq X$ et $x \in A$. Par définition, $f(x) \in f(A)$ et donc $x \in f^{(-1)}(f(A))$. Cela étant vrai pour chaque $x \in A$, on conclut que $A \subseteq f^{(-1)}(f(A))$ ✓

— $\supseteq$: Soit $x \in f^{(-1)}(f(A))$. Alors $f(x) \in f(A)$ donc $\exists a \in A$ tel que $f(a) = f(x)$.
Par injectivité, $a = x$ et donc $x \in A$ et on conclut que $f^{(-1)}(f(A)) \subseteq A$ ✓

Ainsi on a bien $A = f^{(-1)}(f(A))$✓

- $\Longleftarrow$: Supposons que $\forall A \subseteq X,\ A = f^{(-1)}(f(A))$ et soient $x, x' \in X$ tels que $f(x) = f(x')$. Alors $f^{(-1)}(f(\{x\})) = \{x\}$ cependant $f(x') = f(x) \in f(\{x\})$ donc $x' \in f^{(-1)}(f(\{x\}))$ i.e. $x' \in \{x\}$ ainsi $x = x'$. Finalement f est injective. ✓

6. Montrons que : $f$est surjective $\Longleftrightarrow \forall C \subset Y : f(f^{(-1)}(C)) = C$. Raisonnons une dernière fois par double implication.
   - $\Longrightarrow$: Supposons f surjective et soit $C \subset Y$. Soit $c \in C$. Par surjectivité de f, $\exists x \in X$ tel que $f(x) = c$, i.e. $x \in f^{(-1)}(\{x\}) \subseteq f^{(-1)}(C)$. Ainsi $c = f(x) \in f(f^{(-1)}(C))$ et par arbitrarité de c on conclut que $C \subseteq f(f^{(-1)}(C))$. Soit maintenant $c \in f(f^{(-1)}(C))$. Par définition, $\exists x \in f^{(-1)}(C)$ tel que $f(x) = c$. Soit $c \in f(f^{(-1)}(C))$. Il existe $x \in f^{(-1)}(C)$ tel que $f(x) = c$. Or $x \in f^{(-1)}(C)$ donc $c = f(x) \in C$. Finalement $f(f^{(-1)}(C)) \subset C$. Ainsi on a bien $f(f^{(-1)}(C)) = C$✓
   - $\Longleftarrow$: Soit $y \in Y$. Comme $f(f^{(-1)}(Y)) = Y$ il existe $x \in f^{(-1)}(Y)$ tel que $y = f(x)$. Donc f est surjective. ✓

7. - Soit $a \in A$. Alors $f(a) \in f(A)$ et donc $a \in f^{(-1)}(f(A))$. Donc $A \subset f^{(-1)}(f(A))$.
   - On pose $h : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ et $A := \mathbb{R}_{\geqslant 0} = \{x \in \mathbb{R},\ x \geqslant 0\}$. On a $h(A) = \mathbb{R}_{\geqslant 0}$ et $h^{(-1)}(\mathbb{R}_{\geqslant 0}) = \mathbb{R}$. Donc par example $-2 \in h^{(-1)}(h(A))$ mais $-2 \notin A$.
   - Montrons que : $B \supset f(f^{(-1)}(B))$. Soit $y \in f(f^{(-1)}(B))$. Alors il existe $x \in f^{(-1)}(B)$ tel que $f(x) = y$. Comme $f(x)$ est unique, $x \in f^{(-1)}(B)$ implique que $y \in B$. Donc $B \supset f(f^{(-1)}(B))$. Pour montrer qu'on n'a pas forcément une égalité on considère la fonction h et $B = [-1, 1]$. On a $h(h^{(-1)}([-1, 1])) = h([0, 1]) = [0, 1]$, donc $-1 \in B$ mais $-1 \notin h(h^{(-1)}(B))$.

Exercice 7. Soient X, Y, Z des ensembles (pas forcement finis) et $\phi : X \to Y$ et $\psi : Y \to Z$ deux applications entre les ensembles X et Y et les ensembles Y et Z et $\varphi = \psi \circ \phi : X \to Z$ l'application composee.

1. Montrer que si φ est surjective alors ψ est surjective. Donner un exemple montrant que ϕ ne l'est pas forcement.

2. Montrer que si φ est injective alors ϕ est injective. Donner un exemple montrant que ψ ne l'est pas forcement.

Solution 7. Soient $\phi : X \to Y$ et $\psi : Y \to Z$ des applications et $\varphi = \psi \circ \phi$.

1. Supponsons φ surjective et montrons que ψ est surjective.
   Soit $z \in Z$. Par surjectivité de φ il existe $x \in X$ tel que $z = \varphi(x) = \psi(\phi(x))$. En posant $y = \phi(x)$ on a bien que $\psi(y) = \psi(\phi(x)) = \varphi(x) = z$. Donc ψ est bien surjective✓

   Cependant, l'application ϕ n'est pas nécessairement surjective.
   Dans le cas $X = Y = [-2, 2],\ Z = [-1, 1],\ \varphi(x) = \frac{x}{2}, \psi(x) = x$ On voit bien que ϕ (définie par $\phi(x) = \frac{x}{2}$) est une surjection (même une bijection) entre $[-2, 2]$ et $[-1, 1]$ alors que φ n'est pas surjective : -2 n'a pas d'antécedent.
2. Supposons φ injective et montrons que ϕ est injective.
   Soient $x, x' \in X$ tels que $\phi(x) = \phi(x')$. Alors $\psi(\phi(x)) = \psi(\phi(x'))$ i.e. $\varphi(x) = \varphi(x')$. Par injectivité de φ, on a $x = x'$. Ainsi ϕ bel et bien injective✓

   Cependant ψ ne l'est pas nécessairement. Par exemple, si $X = \mathbb{N}$, $Y = \mathbb{Z}$, $Z = \mathbb{N}$ avec pour tout $n \in \mathbb{N}$ on définit ϕ par $\phi(n) = -n$ et pour tout $z \in \mathbb{Z}$ on définit ψ par $\psi(z) = z^2$. Pour tout $n \in \mathbb{N}$ on a $\varphi(n) = n^2$ injective mais ψ non injective. En effet $\psi(-1) = 1 = \psi(1)$.

Exercice 8. ($\star$) On veut montrer le resultat de Cantor : l'application polynomiale (de Cantor)

$$C : (m, n) \mapsto ((m + n)^2 + m + 3n)/2$$

et une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$. Pour cela

1. Verifier que C est une application de $\mathbb{N}^2$ a valeurs vers $\mathbb{N}$.
2. Calculer les valeurs $C(m, n)$ pour $m + n \leqslant 3$ et les reporter sur les point $(, n) \in \mathbb{Z}^2$ d'une representation du quart de plan $\{(x, y),\ x, y \geqslant 0\}$.
3. Pour $k \geqslant 0$ un entier, on definit le sous-ensemble

   $$D_k = \{(m, n) \in \mathbb{N}^2,\ m + n = k\}.$$

   Quelles sont les valeurs prises par $C(m, n)$ quand (m, n) decrit D_k ?
4. En deduire l'injectivite et la surjectivite de C.

Remarque. Une autre application possible (obtenue par symetrie) est

$$C'(m, n) = ((m + n)^2 + 3m + n)/2.$$

On ne sait pas si il y a d'autre applications polynomiales etablissant une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$.

Solution 8.

1. Rappelons nous d'abord de quelques faits utiles. Pour $n, m \in \mathbb{N}$:
   - Si n et m sont tous les deux pairs ou tous les deux impairs alors $n+m$ est pair :
     Dans le premier cas on écrit $n = 2p$ et $m = 2q$ avec $p, q \in \mathbb{N}$, puis on voit facilement que $n + m = 2(\underbrace{p+q}_{\in\mathbb{N}})$ est pair.
     Dans le deuxième cas on écrit $n = 2p+1, m = 2q+1$ et alors $n+m = 2(\underbrace{p+q+1}_{\in\mathbb{N}})$, ce qui montre à nouveau la parité.
   - Si n est pair et m est impair alors $n+m$ est impair (par un raisonnement similaire au précédent).
   - Le carré d'un entier pair est pair :
     De même qu'avant, on écrit $n = 2p$ et alors $n^2 = 4p^2 = 2 \cdot \underbrace{2p^2}_{\in\mathbb{N}}$ donc n^2 est pair.
   - Le carré d'un entier impair est impair :
     De même qu'avant, on écrit $n = 2p+1$ et alors $n^2 = 4p^2 + 4p + 1 = 2 \cdot \underbrace{2p^2 + 2p}_{\in\mathbb{N}} + 1$ donc n^2 est impair.

   Maintenant on veut montrer que $(m+n)^2 + m + 3n$ est toujours pair en faisant une grande disjonction des cas sur la parité de n et m :
   - $\underline{n \text{ et } m \text{ pairs}}$: alors $m+n$ et $m+3n$ sont pairs, donc $(m+n)^2 + m + 3n$ est aussi pair et donc $C(m,n) \in \mathbb{N}$✓
   - $\underline{n \text{ et } m \text{ impairs}}$: pareil qu'au dessus✓
   - $\underline{n \text{ pair et } m \text{ impair}}$: alors $n+m$ est impair, $(n+m)^2$ aussi, et $m+3n$ aussi, donc $(m+n)^2 + m + 3n$ est pair et $C(m,n) \in \mathbb{N}$✓
   - $\underline{n \text{ impair et } m \text{ pair}}$: pareil qu'au dessus✓
2. Les paires possibles sont

   $$\{(m,n) \in \mathbb{N}^2 \mid n+l \leqslant 3\} = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(2,0),(2,1),(3,0)\}$$

   Les valeurs de $C(m,n)$ sont données par le tableau ci-dessous :

$n \backslash m$	0	1	2	3
0	0	1	3	6
1	2	4	7	
2	5	8		
3	9			

3. Remarquons tout d'abord qu'on peut ré-écrire $D_k = \{(m, k-m) \mid 0 \leqslant m \leqslant k\}$. Alors $\forall (m, k-m) \in D_k : C(m, k-m) = \frac{(m+k-m)^2+3m+k-m}{2} = \underbrace{\frac{k^2+k}{2}}_{=:c_k} + m$ et donc
$$C(D_k) = \{c_k + m \mid 0 \leqslant m \leqslant k\} = [\![c_k, c_k + k]\!]$$
(les doubles crochets symbolisent des intervalles d'entiers).
Nous avons défini la grandeur c_k pour pouvoir exprimer plus simplement la relation suivante : $\forall k \in \mathbb{N}, c_{k+1} = c_k + k + 1$. En effet $\frac{k^2+k}{2} + k + 1 = \frac{k^2+k+2k+2}{2} = \frac{(k+1)^2+(k+1)}{2}$.

   Ainsi, tous les intervalles $C(D_k)$ sont contigus, et ne se chevauchent pas (si l'intervalle $C(D_k)$ se termine à la borne a, alors l'intervalle $C(D_k)$ commence à la borne $a+1$). Comme ils commencent à 0 et leur taille ne fait qu'augmenter, ils couvrent tout $\mathbb{N}$ et ils en créent une partition :
$$\mathbb{N} = \bigsqcup_{k \in \mathbb{N}} C(D_k)$$
   On pourrait aussi le voir à partir du fait que la suite $\{c_k\}_{k\in\mathbb{N}}$ est strictement croissante et tend vers $+\infty$ donc
$$\mathbb{N} = \bigsqcup_{k \in \mathbb{N}} [\![c_k, c_{k+1}[\![= \bigsqcup_{k \in \mathbb{N}} C(D_k)$$

4. Tout d'abord, $\forall k \in \mathbb{N}$, la restriction $C_{|D_k} : D_k \to C(D_k)$ est bijective puisqu'elle est définie de maniére "affine" : $C(m, k-m) = c_k + m$. Ensuite, pour montrer que C elle-même est bijective on n'a qu'à montrer que chaque élément $y \in \mathbb{N}$ a un unique antécédent par C. C'est le cas puisque les ensembles $C(D_k), k \in \mathbb{N}$ forment une partition de $\mathbb{N}$, donc $\exists! k_y \in \mathbb{N} : y \in \mathbb{C}(D_{k_y})$. Mais alors comme C est bijective lorsque restreinte à D_{k_y}, y a un unique antécédent dans D_{k_y} et donc dans $\mathbb{N}^2$. S'il y en avait un autre dans $D_{k'}$ alors on aurait $\{y\} \subseteq C(D_{k_y}) \cap C(D_{k'})$ et donc l'intersection n'est pas vide comme on l'a montré dans la question précédente.
   Ainsi $C : \mathbb{N}^2 \to \mathbb{N}$ est bien bijective. □

Exercice 9. Dans la série prochaine

Exercice 10. Dans la série prochaine

Exercice 11. Soit X un ensemble et $\mathscr{P}(X)$ l'ensemble des sous-ensembles de X. La difference symetrique discutee dans l'exercice 1 defini une application
$$\Delta : \begin{array}{ccc} \mathscr{P}(X) \times \mathscr{P}(X) & \mapsto & \mathscr{P}(X) \\ (A, B) & \mapsto & A \Delta B \end{array}$$
et donc une loi de composition sur $\mathscr{P}(X)$.

1. Montrer que cette loi de composition est associative et commutative.
2. Trouver un element neutre $e_\Delta \in \mathscr{P}(X)$ et une application d'inversion

$$\bullet^{-1} : \mathscr{P}(X) \mapsto \mathscr{P}(X)$$

de sorte que $(\mathscr{P}(X), \Delta, e_\Delta, \bullet^{-1})$ forme un groupe commutatif.

Solution 11.

1. Pour la commuativité :

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

Pour l'associativité : On note que

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

et

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

On a

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

Pareil on obtient

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

2. On a $\emptyset\Delta A = A\Delta\emptyset = A$, alors $\emptyset = e_\Delta$ est l'élément neutre. De plus on a $A\Delta A = \emptyset$, 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 12. Dans la série prochaine