Mathématiques Discrètes : Janvier 2011
Corrigé

Les réponses présentées dans ce document sont plus complètes que celles attendues. Ces réponses contiennent parfois une explication intuitive (en plus de la réponse formelle) ou des informations complémentaires.

1. Décidez si les affirmations suivantes sont vraies ou fausses.

   (a) $\{b \in \mathbb{N} \mid \exists\, n \in \mathbb{N}\ \ b = (4^n \mod 7)\} = \{1, 2, 4\}$.

   Vrai. Posons $A := \{b \in \mathbb{N} \mid \exists\, n \in \mathbb{N}\ \ b = (4^n \mod 7)\}$. Notons que cet ensemble peut se ré-écrire de la façon suivante : $\{4^n \mod 7 \mid n \in \mathbb{N}\}$. En prenant quelques valeurs consécutives pour n, on constate que les valeurs correspondantes des $(4^n \mod 7)$ cyclent.

   Montrons d'abord que $\{1, 2, 4\} \subseteq A$. En prenant $n = 0 \in \mathbb{N}$, on a $(4^0 \mod 7) = 1 \in A$; en prenant $n = 2 \in \mathbb{N}$, on a $(4^2 \mod 7) = (16 \mod 7) = 2 \in A$; et en prenant $n = 1 \in \mathbb{N}$, on a $(4^1 \mod 7) = 4 \in A$. Pour montrer que $A \subseteq \{1, 2, 4\}$, prouvons par récurrence que pour tout $n \in \mathbb{N}$, $(4^n \mod 7) \in \{1, 2, 4\}$. Cas de base : $n = 0$, on a $4^0 \mod 7 = 1 \in \{1, 2, 4\}$. Hypothèse de récurrence : supposons que pour tout $0 \leq k \leq n$, on a $(4^k \mod 7) \in \{1, 2, 4\}$. Montrons que la propriété est encore vérifiée pour $k = n + 1$. On a

   $$\begin{aligned} 4^{n+1} \mod 7 &= (4^n \cdot 4) \mod 7 \\ &= ((4^n \mod 7) \cdot (4 \mod 7)) \mod 7 \ \text{(propriété du modulo)} \\ &= ((4^n \mod 7) \cdot 4) \mod 7. \end{aligned}$$

   Or, par hypothèse de récurrence, on sait que $(4^n \mod 7) \in \{1, 2, 4\}$. Considérons les trois cas possibles et montrons, en utilisant l'équation ci-dessus, que dans chacun des cas, $(4^{n+1} \mod 7)$ appartient bien à $\{1, 2, 4\}$.
   - Si $(4^n \mod 7) = 1$, on a $(4^{n+1} \mod 7) = ((1 \cdot 4) \mod 7) = 4 \in \{1, 2, 4\}$.
   - Si $(4^n \mod 7) = 2$, on a $(4^{n+1} \mod 7) = ((2 \cdot 4) \mod 7) = 1 \in \{1, 2, 4\}$.
   - Si $(4^n \mod 7) = 4$, on a $(4^{n+1} \mod 7) = ((4 \cdot 4) \mod 7) = 2 \in \{1, 2, 4\}$.

   (b) $\displaystyle\bigcap_{n \in \mathbb{N}} \left[0, 2 + \frac{(-1)^n}{2^n}\right] = [0, 1]$.

   Faux. Intuitivement, quand n est pair, $2 + \frac{(-1)^n}{2^n} = 2 + \frac{1}{2^n} > 2$ et quand n est impair, $2 + \frac{(-1)^n}{2^n} = 2 - \frac{1}{2^n} \geq \frac{3}{2}$ car la plus grande valeur que prend $\frac{1}{2^n}$ est $\frac{1}{2}$ pour $n = 1$. Nous en déduisons que la borne supérieure de chaque intervalle est supérieure ou égale à $\frac{3}{2}$.

   Montrons alors que $\frac{3}{2} \in \displaystyle\bigcap_{n \in \mathbb{N}} \left[0, 2 + \frac{(-1)^n}{2^n}\right]$, c'est-à-dire pour tout $n \in \mathbb{N}$, $\frac{3}{2} \in \left[0, 2 + \frac{(-1)^n}{2^n}\right]$. Soit $n \in \mathbb{N}$, on a $0 \leq \frac{3}{2}$, et $\frac{3}{2} \leq 2 + \frac{(-1)^n}{2^n}$ si et seulement si $\frac{-1}{2} \leq \frac{(-1)^n}{2^n}$. Pour les n pairs, l'inégalité à vérifier devient $\frac{-1}{2} \leq \frac{1}{2^n}$, qui est vraie car la quantité de gauche est négative et celle de droite positive (quel que soit n). Pour les n impairs, on doit avoir $\frac{-1}{2} \leq \frac{-1}{2^n}$, ce qui est équivalent à $2^n \geq 2$. Comme n est impair, n est supérieur ou égal à 1, donc l'inégalité est vérifiée.

   On a montré que $\frac{3}{2}$ appartient à l'intersection infinie et comme $\frac{3}{2} \notin [0, 1]$, l'égalité donnée dans l'énoncé est fausse.

(c) L'ensemble $\{n \in \mathbb{N} \mid n \text{ est premier } \Rightarrow n \text{ est pair}\}$ est fini.

Faux. L'implication (n est premier $\Rightarrow n$ est pair) est vraie en particulier si n n'est pas premier, or il existe une infinité de nombres non-premiers.

Montrons formellement que l'ensemble donné dans l'énoncé n'est pas fini. Notons cet ensemble B et montrons que $2\mathbb{N} \subseteq B$ par exemple. Comme $2\mathbb{N}$ n'est pas fini, B ne l'est pas non plus. Soit $2n \in 2\mathbb{N}$. Si $n = 1$, alors $2n = 2$ appartient à B car 2 est premier et pair ; et si $n \neq 1$, alors $2n \neq 2$ et 2 divise $2n$, donc $2n$ n'est pas premier (il a un diviseur qui n'est pas 1, ni lui-même) et appartient à B.

Remarquons que cet ensemble B contient exactement tous les nombres non-premiers et 2.

(d) Soit $n \in \mathbb{N}$, soit $F_n = \{f : \{0, 1, \ldots, n\} \to \{0, 1\}\}$. Il existe une bijection $\varphi : \mathcal{P}(\{0, 1, \ldots, n\}) \to F_n$.

Vrai. Une telle fonction φ doit envoyer un sous-ensemble X de $\{0, 1, \ldots, n\}$ sur une fonction f qui va de $\{0, 1, \ldots, n\}$ dans $\{0, 1\}$. L'idée est que cette fonction f décrive exactement l'ensemble X, c'est-à-dire si on prend x dans $\{0, 1, \ldots, n\}$, alors $f(x)$ nous dit si x appartient ou non à l'ensemble X ($f(x) = 1$ ou 0 respectivement).

Formellement, définissons la bijection φ de la façon suivante : soit $X \in \mathcal{P}(\{0, 1, \ldots, n\})$, posons $\varphi(X) = f$, où pour tout $x \in \{0, 1, \ldots, n\}$, $f(x) = 1$ si $x \in X$ et $f(x) = 0$ sinon. La fonction f appartient bien à F_n, donc φ est bien définie. Montrons maintenant que φ est une bijection.

- φ est injective si pour tout $X, Y \in \mathcal{P}(\{0, 1, \ldots, n\})$, on a $X \neq Y \Rightarrow \varphi(X) \neq \varphi(Y)$.
  Soient X, Y deux parties de $\{0, 1, \ldots, n\}$ telles que $X \neq Y$. Donc il existe x dans X et x n'appartient pas à Y (ou inversément). Posons $f_X := \varphi(X)$ et $f_Y := \varphi(Y)$. Comme $x \in X$ et $x \notin Y$, on a $f_X(x) = 1$ et $f_Y(x) = 0$ par définition des deux fonctions. Ainsi, $f_X \neq f_Y$.
- φ est surjective si pour tout $f \in F_n$, il existe $X \in \mathcal{P}(\{0, 1, \ldots, n\})$ tel que $\varphi(X) = f$.
  Soit f dans F_n. Construisons X de la façon suivante : soit $x \in \{0, 1, \ldots, n\}$, on a $x \in X$ si et seulement si $f(x) = 1$. Par définition de φ, on a bien que $\varphi(X) = f$.

(e) $\forall n \in \mathbb{Z}\ |n| \leq n^2$.

Vrai. Montrons d'abord que pour tout $n \in \mathbb{N}$, $|n| \leq n^2$. Soit $n \in \mathbb{N}$ tel que $n \neq 0$. Alors $|n| = n \leq n^2$ si et seulement si $1 \leq n$, ce qui est vrai puisque que n appartient à $\mathbb{N}_0$. L'inégalité est donc vérifiée pour les naturels non-nuls. Dans le cas où $n = 0$, on a bien $0 = |0| \leq 0^2 = 0$.

Montrons maintenant que la formule est vraie aussi pour les entiers négatifs. Soit $m \in \mathbb{Z}^-$, alors $-m$ est dans $\mathbb{N}$. Par ce que l'on vient de prouver, on a $|-m| \leq (-m)^2$. Or, $|-m| = |m|$ par définition de la valeur absolue, et $(-m)^2 = m^2$. On obtient alors $|m| \leq m^2$.

(f) $\forall a, b, c \in \mathbb{Z}$, $\forall m \in \mathbb{N}_0$, on a $(a + b \equiv_m a + c) \Rightarrow (b \equiv_m c)$.

Vrai. Soient $a, b, c \in \mathbb{Z}$ et $m \in \mathbb{N}_0$. Par définition du modulo, on a

$$a + b \equiv_m a + c \quad \Leftrightarrow \quad m \mid ((a + c) - (a + b)) \quad \Leftrightarrow \quad m \mid (c - b) \quad \Leftrightarrow \quad (b \equiv_m c).$$

(g) $\forall a, b, c, m \in \mathbb{N}_0$, tous premiers, on a $(a \cdot b \equiv_m a \cdot c) \Rightarrow (b \equiv_m c)$.

Faux. Prenons $a = 3$, $b = 2$, $c = 7$, et $m = 3$. Ils sont tous dans $\mathbb{N}_0$ et premiers. On a $a \cdot b = 6$ et $a \cdot c = 21$, donc $a \cdot b \equiv_m a \cdot c$ car $(6 \mod 3) = 0 = (21 \mod 3)$. Mais $b \not\equiv_m c$ puisque $(2 \mod 3) = 2$ et $(7 \mod 3) = 1$.

(h) $\forall x \in \mathbb{R}\ \exists n \in \mathbb{N}\ \ n \leq x \leq n+1.$

Faux. Cette formule est fausse pour tout réel strictement négatif car on ne peut pas trouver de nombre positif qui lui soit inférieur. Notons néanmoins qu'elle est vraie pour les réels positifs.

Plus formellement, montrons la négation de cette formule : $\exists\, x \in \mathbb{R}\ \forall n \in \mathbb{N}\ \ (n > x) \vee (x > n+1)$. Prenons $x = -1 \in \mathbb{R}$. Soit $n \in \mathbb{N}$. On a $n \geq 0 > -1 = x$, donc $n > x$.

(i) Le schéma $(\mathbf{B}, \mathbf{R})$ permet d'engendrer tous les multiples de 3 ; où $\mathbf{B} = \{2, 3\}$ et $\mathbf{R} = \{r_1, r_2\}$ avec :

$$x, y \xrightarrow{r_1} \text{pgcd}(x, y) \qquad ; \qquad x, y \xrightarrow{r_2} \text{ppcm}(x, y).$$

Faux. Montrons que ce schéma ne permet d'engendrer que les nombres 2, 3, 1 et 6. En particulier, il ne peut engendrer 9, qui est un multiple de 3. Appliquons les différentes règles sur les éléments de la base et appliquons-les encore sur les nouveaux éléments obtenus jusqu'à ce que l'on n'engendre plus aucun nombre supplémentaire.

$$\begin{aligned}
2, 3 &\xrightarrow{r_1} \text{pgcd}(2,3) = 1 \quad ; \quad 2, 3 \xrightarrow{r_2} \text{ppcm}(2,3) = 6 \\
1, 2 &\xrightarrow{r_1} \text{pgcd}(1,2) = 1 \quad ; \quad 1, 2 \xrightarrow{r_2} \text{ppcm}(1,2) = 2 \\
1, 3 &\xrightarrow{r_1} \text{pgcd}(1,3) = 1 \quad ; \quad 1, 3 \xrightarrow{r_2} \text{ppcm}(1,3) = 3 \\
2, 6 &\xrightarrow{r_1} \text{pgcd}(2,6) = 2 \quad ; \quad 2, 6 \xrightarrow{r_2} \text{ppcm}(2,6) = 6 \\
3, 6 &\xrightarrow{r_1} \text{pgcd}(3,6) = 3 \quad ; \quad 3, 6 \xrightarrow{r_2} \text{ppcm}(3,6) = 6 \\
1, 6 &\xrightarrow{r_1} \text{pgcd}(1,6) = 1 \quad ; \quad 1, 6 \xrightarrow{r_2} \text{ppcm}(1,6) = 6 \\
n, n &\xrightarrow{r_1} \text{pgcd}(n,n) = n \quad ; \quad n, n \xrightarrow{r_2} \text{ppcm}(n,n) = n \ \text{ pour tout } n \in \{1,2,3,6\}.
\end{aligned}$$

On a appliqué les deux règles sur toutes les paires possibles d'éléments engendrés et on n'obtient aucun nouveau élément. Le schéma $(\mathbf{B}, \mathbf{R})$ engendre donc exactement l'ensemble $\{1, 2, 3, 6\}$.

2. Un "truc" pour tester rapidement qu'un nombre naturel est divisible par 3 est de tester que la somme de ses digits dans son écriture en base 10 est divisible par 3. Par exemple, 123 est divisible par 3, car $1 + 2 + 3 = 6$ est divisible par 3. Le but de cet exercice est d'essayer de comprendre ce "truc".

(a) Quel que soit $k \in \mathbb{N}$, calculez le reste de la division de 10^k par 3.

Montrons par récurrence que $(10^k \mod 3) = 1$ pour tout $k \in \mathbb{N}$. Cas de base : $k = 0$. On a $10^0 = 1$ et $1 \mod 3 = 1$. Hypothèse de récurrence : supposons que pour tout $0 \leq n \leq k$, $(10^n \mod 3) = 1$. Montrons que la propriété est encore vraie pour $n = k + 1$. On a

$$\begin{aligned}
10^{k+1} \mod 3 &= (10^k \cdot 10) \mod 3 \\
&= ((10^k \mod 3) \cdot (10 \mod 3)) \mod 3 \quad \text{(propriété du modulo)} \\
&= (1 \cdot 1) \mod 3 \quad \text{(par hypothèse de récurrence et } 10 = 3 \cdot 3 + 1) \\
&= 1 \mod 3 \\
&= 1.
\end{aligned}$$

(b) Soit $n \in \mathbb{N}$, on sait que l'on peut écrire n en base 10 (vous ne devez pas le prouver) ; c'est-à-dire que l'on peut écrire n sous la forme suivante :

$$n = \sum_{k=0}^{K} a_k 10^k$$

pour un certain $K \in \mathbb{N}$, avec $a_k \in \{0, 1, \ldots, 9\}$. Par exemple, $123 = 1.10^2 + 2.10^1 + 3.10^0$. En utilisant cette écriture, formalisez (à l'aide d'une implication) qu'une condition nécessaire pour qu'un nombre naturel soit divisible par 3 est que la somme de ses digits dans son écriture en base 10 soit divisible par 3.

Rappel : soient P, Q deux propositions. Quand $P \Rightarrow Q$, on dit que P est une condition suffisante pour Q, et Q est une condition nécessaire pour avoir P (car si Q est faux, alors P aussi).
La formule demandée est donc la suivante :
$\forall n \in \mathbb{N}$ où $n = \sum_{k=0}^{K} a_k 10^k$ pour un certain $K \in \mathbb{N}$, avec $a_k \in \{0, 1, \ldots, 9\}$,

$$n \equiv_3 0 \quad \Rightarrow \quad \left(\sum_{k=0}^{K} a_k\right) \equiv_3 0\,.$$

(c) En utilisant le point (a), prouvez la propriété que vous avez formulée au point (b).

Soit $n \in \mathbb{N}$ tel que $n = \sum_{k=0}^{K} a_k 10^k$ pour un certain $K \in \mathbb{N}$, avec $a_k \in \{0, 1, \ldots, 9\}$. Par le point (a), on a $10^k \equiv_3 1$ pour tout $k \in \mathbb{N}$. En particulier, on a donc $a_k 10^k \equiv_3 a_k$ pour tout $k \in \{0, \ldots, K\}$, par la propriété suivante : $\forall a, b, c \in \mathbb{Z},\ \forall m \in \mathbb{N}_0 \quad (b \equiv_m c) \Rightarrow (a \cdot b \equiv_m a \cdot c)$. De même, en appliquant K fois la propriété : $\forall a, b, c, d \in \mathbb{Z},\ \forall m \in \mathbb{N}_0 \quad (a \equiv_m b \wedge c \equiv_m d) \Rightarrow (a + c \equiv_m b + d)$, on en déduit que

$$\left(\sum_{k=0}^{K} a_k 10^k\right) \equiv_3 \left(\sum_{k=0}^{K} a_k\right). \tag{1}$$

Par conséquent, on a bien que $n \equiv_3 0$ implique $\left(\sum_{k=0}^{K} a_k\right) \equiv_3 0$.

(d) Déterminez si la réciproque de la propriété que vous avez formulée au point (b) est vraie.

Par l'équation (1), la réciproque est vraie également : si $\left(\sum_{k=0}^{K} a_k\right) \equiv_3 0$, alors $n \equiv_3 0$.

(e) Ce "truc" est-il vrai pour tester la divisibilité d'un naturel par un autre nombre que 3 ? Expliquez votre raisonnement !

Oui. Cela marche aussi pour tester la divisibilité d'un naturel par 9. En effet, on a $10 \equiv_9 1$, donc on peut prouver que pour tout $k \in \mathbb{N}$, on a $10^k \equiv_9 1$ (de la même façon qu'au point (a)). De plus, les preuves des points (c) et (d) sont toujours correctes si on remplace $\equiv_3$ par $\equiv_9$. On a donc :
$\forall n \in \mathbb{N}$ où $n = \sum_{k=0}^{K} a_k 10^k$ pour un certain $K \in \mathbb{N}$, avec $a_k \in \{0, 1, \ldots, 9\}$,

$$n \equiv_9 0 \quad \Leftrightarrow \quad \left(\sum_{k=0}^{K} a_k\right) \equiv_9 0.$$

Remarquons que pour tout $n \in \mathbb{N}_0$ différent de 3 et 9, on a $10 \not\equiv_n 1$.

3. Soit $X \subseteq \mathbb{N}$, on note $|X|$ le nombre d'éléments de X. On considère le schéma d'induction (sur les parties de $\mathbb{N}$) $(\mathbf{B}, \mathbf{R})$ où $\mathbf{B} = \big\{\{0\}\big\}$ et $\mathbf{R} = \{r_1, r_2, r_3\}$ avec :

$$X \xrightarrow{r_1} X \cup \{|X|\} \quad ; \quad X \xrightarrow{r_2} X^c \quad ; \quad X, Y \xrightarrow{r_3} X \cap Y.$$

(a) Le schéma $(\mathbf{B}, \mathbf{R})$ permet-il d'engendrer les ensembles $\{0, 1, \ldots, n\}$ quel que soit $n \in \mathbb{N}$?

Oui. Montrons cela par récurrence sur $n \in \mathbb{N}$. Cas de base : $n = 0$, on a $\{0\} \in \mathbf{B}$, donc $\{0\}$ est engendré par le schéma. Hypothèse de récurrence : supposons que pour tout $0 \leq k \leq n$, l'ensemble $\{0, \ldots, k\}$ peut être engendré par le schéma. Prouvons que $\{0, \ldots, n+1\}$ peut être également engendré par $(\mathbf{B}, \mathbf{R})$. On a

$$\{0, \ldots, n\} \xrightarrow{r_1} \{0, \ldots, n\} \cup \{|\{0, \ldots, n\}|\} = \{0, \ldots, n\} \cup \{n+1\} = \{0, \ldots, n, n+1\}.$$

Comme $\{0, \ldots, n\}$ peut être engendré par le schéma (par hypothèse de récurrence), l'ensemble $\{0, \ldots, n, n+1\}$ aussi.

(b) Le schéma $(\mathbf{B}, \mathbf{R})$ permet-il d'engendrer l'ensemble $\{1\}$?

Oui. On a :

$$\begin{aligned} \{0\} &\xrightarrow{r_2} \{1, 2, \ldots\} \\ \{0, 1\}, \{1, 2, \ldots\} &\xrightarrow{r_3} \{1\}. \end{aligned}$$

Comme $\{0\}$ est dans la base et $\{0, 1\}$ est engendré par $(\mathbf{B}, \mathbf{R})$ (voir point (a)), le singleton $\{1\}$ peut être engendré par le schéma.

(c) Le schéma $(\mathbf{B}, \mathbf{R})$ permet-il d'engendrer les ensembles $\{n\}$ quel que soit $n \in \mathbb{N}$?

Oui. Le singleton $\{0\}$ est dans la base, donc engendré par le schéma. Soit $n \in \mathbb{N}_0$, on a

$$\begin{aligned} \{0, \ldots, n-1\} &\xrightarrow{r_2} \{n, n+1, \ldots\} \\ \{0, \ldots, n\}, \{n, n+1, \ldots\} &\xrightarrow{r_3} \{n\}. \end{aligned}$$

Par le point (a), les ensembles $\{0, \ldots, n-1\}$ et $\{0, \ldots, n\}$ sont engendrés par le schéma ($n > 0$), donc $\{n\}$ peut être engendré par $(\mathbf{B}, \mathbf{R})$.

Remarquons que grâce au point (a), une preuve par récurrence n'est pas nécessaire dans cet exercice.

(d) Le schéma $(\mathbf{B}, \mathbf{R})$ permet-il d'engendrer toutes les parties **finies** de $\mathbb{N}$?

Oui. Montrons cela par récurrence sur le cardinal des parties finies de $\mathbb{N}$. Cas de base : $|X| = 0$ où $X \in \mathcal{P}(\mathbb{N})$, alors $X = \emptyset$. On a :

$$\begin{aligned} \{0\} &\xrightarrow{r_2} \{1, 2, \ldots\} \\ \{0\}, \{1, 2, \ldots\} &\xrightarrow{r_3} \emptyset. \end{aligned}$$

Le schéma peut donc engendrer $X = \emptyset$ car $\{0\} \in \mathbf{B}$. Hypothèse de récurrence : supposons que pour tout $0 \leq k \leq n$, toute partie de $\mathbb{N}$ de cardinal k peut être engendrée par $(\mathbf{B}, \mathbf{R})$. Prouvons que le schéma peut engendrer toute partie de cardinal $k = n + 1$. Soit $X \in \mathcal{P}(\mathbb{N})$ tel que $|X| = n + 1$.

Alors on peut écrire X comme $Y \cup \{x\}$, où $|Y| = n$, $Y \subseteq X$, $x \in X$ et $x \notin Y$. Comme l'union ne fait pas partie des règles du schéma, utilisons des propriétés de la théorie des ensembles pour faire apparaître l'intersection et le complémentaire. Comme $(A^c)^c = A$ et $(A \cup B)^c = A^c \cap B^c$ pour tous ensembles A et B, on a :

$$X = Y \cup \{x\} = (Y^c \cap \{x\}^c)^c.$$

Montrons que $(Y^c \cap \{x\}^c)^c$ peut être engendré par le schéma :

$$\begin{aligned} Y &\xrightarrow{r_2} Y^c \\ \{x\} &\xrightarrow{r_2} \{x\}^c \\ Y^c, \{x\}^c &\xrightarrow{r_3} Y^c \cap \{x\}^c \\ Y^c \cap \{x\}^c &\xrightarrow{r_2} (Y^c \cap \{x\}^c)^c. \end{aligned}$$

Comme Y peut être engendré par le schéma par hypothèse de récurrence ($|Y| = n$) et que $\{x\}$ aussi par le point (c), le schéma $(\mathbf{B}, \mathbf{R})$ peut également engendrer $(Y^c \cap \{x\}^c)^c = X$.

4. Trouvez (si possible) un exemple dans chacune des situations suivantes. Dans le cas où il est impossible de trouver un exemple, justifiez pourquoi.

(a) Un ensemble $X \subseteq \mathbb{R}$ non-vide qui satisfait la formule suivante :

$$\big(\exists b \in \mathbb{R}\ \forall x \in X\ (x \leq b)\big)\ \wedge\ \big(\forall y \in X\ \exists z \in X\ (y < z)\big).$$

Intuitivement, la première partie de la formule signifie que l'ensemble X possède une borne supérieure, et la seconde que X n'a pas de maximum.

Prenons $X = [0, 1[\subseteq \mathbb{R}$ et prouvons que la formule est vérifiée. Prenons $b = 1 \in \mathbb{R}$. Soit $x \in [0, 1[$, on a bien $x \leq 1 = b$. Montrons maintenant la deuxième partie. Soit $y \in [0, 1[$. Prenons $z = \frac{1+y}{2}$ et assurons-nous que z appartient à $[0, 1[$. On a $0 \leq \frac{1+y}{2}$ si et seulement si $-1 \leq y$, ce qui est vrai car $y \in [0, 1[$. De plus, on a $\frac{1+y}{2} < 1$ si et seulement si $y < 1$, et cette inégalité est également satisfaite. Donc $z = \frac{1+y}{2}$ appartient bien à $[0, 1[$. Il reste à démontrer que $y < z$. Or,

$$y < \frac{1+y}{2} \quad \Leftrightarrow \quad 2y < 1 + y \quad \Leftrightarrow \quad y < 1\,.$$

Comme $y \in [0, 1[$, on a bien $y < z$.

(b) Une fonction $f : \{0, 1\} \to \{5, 7\}$ qui est injective sans être surjective, telle que $Dom(f) = \{0, 1\}$.

C'est impossible de trouver une telle fonction car pour toute fonction $f : A \to B$ où $|A| = |B|$ et A, B sont des ensembles finis, on a que f est injective si et seulement si elle est surjective si et seulement si elle est bijective. Or ici, on a $|\{0, 1\}| = |\{5, 7\}| = 2 < +\infty$.

Notez qu'il est également possible de montrer cela par l'absurde. Supposons qu'il existe une telle fonction. Par injectivité, on a $f(0) = 5$ et $f(1) = 7$ (ou inversement). Or cette fonction est surjective car tous les points de son ensemble d'arrivée sont atteints, ce qui amène à une contradiction.

(c) Un ensemble *dénombrable* X de nombres réels tel que $X \subseteq [0, 1]$.

Prenons $X = \{\frac{1}{n+1} \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$. Cet ensemble X est bien inclus à $[0, 1]$ car pour tout n, on a que $0 \leq \frac{1}{n+1}$, et $\frac{1}{n+1} \leq 1$ si et seulement si $0 \leq n$, ce qui est vrai. Montrons maintenant que X est dénombrable. Considérons la fonction $f : \mathbb{N} \to X : n \mapsto \frac{1}{n+1} \in X$ et montrons qu'elle est bijective.

– f est injective : soient $n_1, n_2 \in \mathbb{N}$ tels que $f(n_1) = f(n_2)$. Par définition de f, cela signifie que $\frac{1}{n_1+1} = \frac{1}{n_2+1}$, c'est-à-dire $n_2 + 1 = n_1 + 1$, ou encore $n_1 = n_2$.
– f est surjective : soit $y = \frac{1}{n+1} \in X$ où $n \in \mathbb{N}$. Prenons $x = n \in \mathbb{N}$. On a, par définition de f, que $f(x) = f(n) = \frac{1}{n+1} = y$.

(d)

Un polynôme, avec (au moins) une racine non entière, qui est engendré par le schéma $(\mathbf{B}, \mathbf{R})$ où $\mathbf{B} = \{1, x\}$ et $\mathbf{R} = \{r_1, r_2\}$ avec :

$$p(x), q(x) \xrightarrow{r_1} p(x) + q(x) \qquad ; \qquad p(x), q(x) \xrightarrow{r_2} p(x) \cdot q(x).$$

Prenons le polynôme $2x + 1$. Son unique racine est $-\frac{1}{2}$, et n'est pas entière. Montrons que ce polynôme peut être engendré par le schéma. On a

$$\begin{aligned} x, x &\xrightarrow{r_1} 2x \\ 2x, 1 &\xrightarrow{r_1} 2x + 1. \end{aligned}$$

Comme x et 1 sont dans la base, le schéma permet donc d'engendrer le polynôme $2x + 1$.

(e)

Un polynôme, avec (au moins) une racine non entière, qui est engendré par le schéma $(\mathbf{B}, \mathbf{R})$ où $\mathbf{B} = \{1, x\}$ et $\mathbf{R} = \{r_1, r_2\}$ avec :

$$p(x) \xrightarrow{r_1} p(x) \cdot (x - 3) \qquad ; \qquad p(x), q(x) \xrightarrow{r_2} p(x) \cdot q(x).$$

Montrons que c'est impossible de trouver un tel polynôme, c'est-à-dire que tout polynôme engendré par ce schéma ne possède que des racines entières, s'il en a. Prouvons cela par induction sur le schéma. Le polynôme 1 n'a pas de racine et le polynôme x n'a que $0 \in \mathbb{Z}$ comme racine. Pour les éléments de la base, la propriété est donc vérifiée. Soient $p(x)$ et $q(x)$ deux polynômes engendrés par le schéma qui n'ont que des racines entières. Montrons qu'en appliquant les deux règles de $\mathbf{R}$, on obtient deux polynômes qui satisfont encore la propriété.

$$\begin{aligned} p(x) &\xrightarrow{r_1} p(x) \cdot (x - 3) \\ p(x), q(x) &\xrightarrow{r_2} p(x) \cdot q(x). \end{aligned}$$

D'une part, les racines du polynôme $p(x) \cdot (x-3)$ sont exactement 3 et les racines de $p(x)$. Comme $3 \in \mathbb{Z}$ et les racines de $p(x)$ sont entières par hypothèse, on a bien que les racines de $p(x) \cdot (x - 3)$ sont entières. D'autre part, le polynôme $p(x) \cdot q(x)$ s'annule si et seulement $p(x)$ ou $q(x)$ s'annule. Or les racines de ces deux polynômes sont toutes entières par hypothèse, donc les racines de $p(x) \cdot q(x)$ sont entières.

(f) Une fonction $f : \mathbb{Q} \to \mathbb{R} \setminus \mathbb{Q}$ qui est injective. $(\mathbb{R} \setminus \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\})$

Prenons $f : \mathbb{Q} \to \mathbb{R} \setminus \mathbb{Q} : x \mapsto \pi + x$. Cette fonction f est bien définie car pour tout $x \in \mathbb{Q}$, on a que $f(x) \in \mathbb{R} \setminus \mathbb{Q}$. En effet, supposons par l'absurde que $f(x) = \pi + x$ appartient à $\mathbb{Q}$. Alors $\pi + x = q$ pour un certain q dans $\mathbb{Q}$. Comme la soustraction de deux rationnels donne un rationnel, $\pi = q - x$ serait dans $\mathbb{Q}$, ce qui amène à une contradiction vu que π est irrationnel.

La fonction f est injective. En effet, soient $x_1, x_2 \in \mathbb{Q}$ tels que $f(x_1) = f(x_2)$, alors on a, par définition de f, $\pi + x_1 = \pi + x_2$, ou encore $x_1 = x_2$.

(g) Une fonction $f : \mathbb{R} \to \mathbb{R}$ qui satisfait la formule suivante :

$$\big(\forall x, y \in \mathbb{R}\ (x < y) \Rightarrow f(x) > f(y)\big) \wedge \big(\exists p \in \mathbb{R}_0\ \forall z \in \mathbb{R}\ f(z) = f(z+p)\big).$$

Il est impossible de trouver une telle fonction f. Intuitivement, la première partie de la formule signifie que f est strictement décroissante. Or, la deuxième nous dit que pour tout z, la fonction a la même image en z et en $z + p$ (pour un p non-nul), i.e. f est périodique, ce qui contredit la stricte décroissance de la fonction.

Montrons cela par l'absurde et supposons qu'il existe une fonction f qui satisfait cela. Prenons un point z dans le domaine de f. Si $p < 0$ (respectivement $p > 0$), on a que $z + p < z$ (respectivement $z < z + p$) et donc, $f(z + p) > f(z)$ (respectivement $f(z) > f(z + p)$) par la première moitié de la formule. Or, on doit avoir que $f(z) = f(z + p)$ par la deuxième moitié, ce qui amène une contradiction.

(h) Une suite d'ensembles $(X_n)_{n\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $X_n \subseteq \mathbb{Q}$, qui satisfait la formule suivante :

$$\left(\forall k \in \mathbb{N} \bigcap_{n=0}^{k} X_n \neq \emptyset\right) \ \wedge \ \left(\bigcap_{n=0}^{+\infty} X_n = \emptyset\right).$$

Prenons $X_n = \{q \in \mathbb{Q} \mid 0 < q \leq \frac{1}{n+1}\} \subseteq \mathbb{Q}$ pour tout $n \in \mathbb{N}$. Montrons que cette suite d'ensembles satisfait la formule donnée. Pour tout naturel n, le fait que $\frac{1}{n+1} \leq \frac{1}{n}$ implique $X_n \subseteq X_{n-1}$. Par conséquent, pour tout $k \geq 0$, on a que $X_k \subseteq \ldots \subseteq X_0$, et donc, $\bigcap_{n=0}^{k} X_n = X_k$. Or, $\frac{1}{k+1}$ appartient à X_k (car c'est un rationnel strictement plus grand que 0). On en déduit alors que $\bigcap_{n=0}^{k} X_n \neq \emptyset$ pour tout $k \in \mathbb{N}$.

Prouvons maintenant que l'intersection infinie des X_n est vide. Supposons par l'absurde qu'il existe x dans $\bigcap_{n=0}^{+\infty} X_n$. Alors, on a $0 < x \leq 1$ puisque pour tout $n \in \mathbb{N}$, $0 < x \leq \frac{1}{n+1}$ et $\frac{1}{n+1} \leq 1$. Or nous pouvons montrer : $\forall y \in [1, +\infty[\ \ \exists m \in \mathbb{N}_0 \quad m \leq y < m + 1$, en prenant $m = \lfloor y \rfloor \in \mathbb{N}_0$ (car $y \geq 1$). Nous pouvons ré-écrire cette formule de la façon suivante :

$$\forall z \in]0, 1]\ \ \exists m \in \mathbb{N}_0 \quad \frac{1}{m+1} < z \leq \frac{1}{m}.$$

En effet, soit z dans $]0, 1]$, alors $\frac{1}{z}$ appartient à $[1, +\infty[$. Par la première formule, il existe $m \in \mathbb{N}_0$ tel que $m \leq \frac{1}{z} < m + 1$, qui est équivalent à $\frac{1}{m+1} < z \leq \frac{1}{m}$.

En appliquant cette propriété à x $(0 < x \leq 1)$, on sait qu'il existe $m \in \mathbb{N}_0$ tel que

$$\frac{1}{m+1} < x \quad \text{et} \quad x \leq \frac{1}{m}.$$

Par définition des ensembles X_n, cela signifie que x n'appartient pas à X_m (et x appartient à X_{m-1}). Or par hypothèse, x est dans $\bigcap_{n=0}^{+\infty} X_n$, ce qui amène à une contradiction.

(i) Une suite d'ensembles $(X_n)_{n\in\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, $X_n \subseteq \mathbb{Q}$, qui satisfait la formule suivante :

$$\left(\forall k \in \mathbb{N} \bigcup_{n=0}^{k} X_n \neq \emptyset\right) \ \wedge \ \left(\bigcup_{n=0}^{+\infty} X_n = \emptyset\right).$$

Il est impossible de trouver une suite d'ensembles $(X_n)_{n\in\mathbb{N}}$ qui satisfait cette formule. Pour montrer cela, supposons par l'absurde qu'il en existe une. En particulier, pour $k = 0$, on a que $\bigcup_{n=0}^{k} X_n = X_0 \neq \emptyset$. Or, $X_0 \subseteq \bigcup_{n=0}^{+\infty} X_n$, donc cette union infinie est non-vide également, ce qui contredit la deuxième partie de la formule.