Université Joseph Fourier, Grenoble I
Mathématiques, Informatique et Mathématiques Appliquées
Licence Sciences et Technologies 1e année

Langage mathématique

Eric Dumas, Emmanuel Peyre et Bernard Ycart

Ce chapitre vous explique la règle du jeu mathématique. Rien n'est vraiment nouveau ni compliqué. Pour donner des exemples d'énoncés, nous ferons appel à quelques notions de base sur les nombres entiers, que vous connaissez depuis longtemps.

Table des matières

1 Cours

1.1 Assertions

On peut voir le langage mathématique comme un jeu de construction, dont le but est de fabriquer des énoncés vrais. La règle de base de ce jeu est qu'un énoncé mathématique ne peut être que vrai ou faux. Il ne peut pas être « presque vrai » ou « à moitié faux ». Une des contraintes sera donc d'éviter toute ambiguïté et chaque mot devra avoir un sens mathématique précis.

Selon le cas, un énoncé mathématique pourra porter des noms différents.

- *assertion :* c'est le terme que nous utiliserons le plus souvent pour désigner une affirmation dont on peut dire si elle est vraie ou fausse.
- *théorème :* c'est un résultat important, dont on démontre ou on admet qu'il est vrai, et qui doit être connu par cœur.
- *proposition :* nous utiliserons ce terme pour désigner un résultat démontré, moins important qu'un théorème.
- *lemme :* c'est un résultat démontré, qui constitue une étape dans la démonstration d'un théorème.
- *corollaire :* c'est une conséquence facile d'un théorème ou d'une proposition.

Dans ce cours les démonstrations se terminent par un carré blanc, plutôt que par le célèbre CQFD (« ce qu'il fallait démontrer »). Pour écrire formellement des énoncés mathématiques, on utilise des lettres représentant des concepts (nombres, ensembles, fonctions, vecteurs, matrices, polynômes...) avec des symboles logiques et des relations.

Le but de ce chapitre étant d'illustrer la manipulation du langage, il ne comportera aucune difficulté mathématique. Nous en resterons à des énoncés très simples, que l'on prendra soin de toujours traduire en langage courant pour bien les comprendre. Dans ce qui suit les lettres m et n désignent des entiers naturels $(0, 1, 2, \ldots)$. Nous n'utiliserons que les symboles de comparaison $(<, >, \leqslant, \geqslant)$ et de divisibilité ($\mid$). Rappelons que $m \mid n$ (« m divise n ») si n est égal au produit km pour un certain entier k.

$n < 5$	l'entier n est strictement inférieur à 5
$n \geqslant 3$	l'entier n est supérieur ou égal à 3
$n \mid 12$	l'entier n divise 12
$2 \mid n$	l'entier n est divisible par 2 (il est pair)

Pour combiner entre elles des assertions, on utilise les connecteurs de base suivants :

- la *négation* (« non »), notée $\neg$
- la *conjonction* (« et »), notée $\wedge$
- la *disjonction* (« ou »), notée $\vee$.

Le tableau suivant est une *table de vérité*. Il décrit l'effet des connecteurs sur deux assertions A et B, selon qu'elles sont vraies (V) ou fausses (F), en disant dans chacun

des 4 cas si l'assertion composée est elle-même vraie ou fausse.

		négation non	conjonction et	disjonction ou
A	B	$\neg A$	$A \wedge B$	$A \vee B$
V	V	F	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	F

Le « ou » est toujours inclusif : A ou B signifie que l'une *au moins* des deux assertions est vraie (peut-être les deux). Par opposition, le « ou exclusif » est vrai quand l'une des deux assertions est vraie mais pas les deux. Voici quelques assertions composées et leur traduction.

$\neg(n < 5)$	l'entier n n'est pas strictement inférieur à 5.
$(n < 5) \wedge (2 \,\vert\, n)$	l'entier n est strictement inférieur à 5 et divisible par 2.
$(2 \,\vert\, n) \vee (3 \,\vert\, n)$	l'entier n est divisible par 2 ou par 3.

Observez l'usage des parenthèses qui permettent d'isoler des assertions simples au sein d'une assertion composée.

À partir des connecteurs de base, on en fabrique d'autres, dont les plus importants sont l'*implication* et l'*équivalence*. Par définition, l'implication $A \Longrightarrow B$ est vraie soit si A est fausse soit si A et B sont vraies toutes les deux. L'écriture $A \Longrightarrow B$ est donc une notation pour $(\neg A) \vee B$ (« non A ou B »). L'équivalence $A \Longleftrightarrow B$ est une double implication : $\Big((A \Longrightarrow B) \wedge (B \Longrightarrow A)\Big)$ (« A implique B et B implique A »). Voici les tables de vérité des implications et de l'équivalence entre deux assertions A et B. Constatez que l'équivalence $A \Longleftrightarrow B$ est vraie quand A et B sont toutes les deux vraies, ou bien toutes les deux fausses.

A	B	$A \Longrightarrow B$	$B \Longrightarrow A$	$A \Longleftrightarrow B$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

L'implication et l'équivalence sont les outils de base du raisonnement mathématique. Il est essentiel de bien les assimiler, et de comprendre toutes leurs formulations.

$A \implies B$
A implique B
A entraîne B
si A est vrai alors B est vrai
B est vrai si A est vrai
A est vrai seulement si B est vrai
pour que B soit vrai il suffit que A le soit
A est une condition suffisante pour B
pour que A soit vrai il faut que B le soit
B est une condition nécessaire pour A

Pour bien comprendre l'implication, reprenez chacune des formulations en remplaçant A par « $n > 3$ » et B par « $n > 2$ ».

$A \iff B$
A est équivalent à B
A équivaut à B
A entraîne B et réciproquement
si A est vrai alors B est vrai et réciproquement
A est vrai si et seulement si B est vrai
pour que A soit vrai il faut et il suffit que B le soit
A est une condition nécessaire et suffisante pour B

Pour bien comprendre l'équivalence, reprenez chacune des formulations en remplaçant A par « $n \geqslant 3$ » et B par « $n > 2$ ».

Les principales propriétés des connecteurs sont résumées dans le théorème suivant.

Théorème 1. *Soient A, B et C trois assertions. Les équivalences suivantes sont toujours vraies.*

- *Commutativité :*

$$\Big(A \wedge B\Big) \iff \Big(B \wedge A\Big)\,. \tag{1}$$

« A et B » équivaut à « B et A ».

$$\Big(A \vee B\Big) \iff \Big(B \vee A\Big)\,. \tag{2}$$

« A ou B » équivaut à « B ou A ».

- *Associativité :*

$$\Big(A \wedge (B \wedge C)\Big) \iff \Big((A \wedge B) \wedge C\Big)\,. \tag{3}$$

« A et (B et C) » équivaut à « (A et B) et C ».

$$\Big(A \vee (B \vee C)\Big) \iff \Big((A \vee B) \vee C\Big)\,. \tag{4}$$

« A ou (B ou C) » équivaut à « (A ou B) ou C ».

- *Distributivité :*

$$\Big(A \wedge (B \vee C)\Big) \Longleftrightarrow \Big((A \wedge B) \vee (A \wedge C)\Big) . \tag{5}$$

« A et (B ou C) » équivaut à « (A et B) ou (A et C) ».

$$\Big(A \vee (B \wedge C)\Big) \Longleftrightarrow \Big((A \vee B) \wedge (A \vee C)\Big) . \tag{6}$$

« A ou (B et C) » équivaut à « (A ou B) et (A ou C) ».

- *Négations :*

$$\Big(\neg(\neg A)\Big) \Longleftrightarrow A . \tag{7}$$

« non (non A) » équivaut à « A ».

$$\Big(\neg(A \vee B)\Big) \Longleftrightarrow \Big((\neg A) \wedge (\neg B)\Big) . \tag{8}$$

« non (A ou B) » équivaut à « (non A) et (non B) ».

$$\Big(\neg(A \wedge B)\Big) \Longleftrightarrow \Big((\neg A) \vee (\neg B)\Big) . \tag{9}$$

« non (A et B) » équivaut à « (non A) ou (non B) ».

Il est conseillé de remplacer A, B et C par des assertions sur les nombres entiers pour bien comprendre les énoncés de ce théorème (par exemple A par $(n \leqslant 6)$, B par $(2 \,|\, n)$, C par $(3 \,|\, n)$).

Démonstration : Pour démontrer l'équivalence de deux assertions, nous n'avons pas d'autre moyen pour l'instant que de vérifier que leurs tables de vérité coïncident : les deux assertions sont équivalentes si elles sont toujours soit toutes les deux vraies soit toutes les deux fausses. Voici la vérification pour (5).

$$A \wedge (B \vee C) \Longleftrightarrow (A \wedge B) \vee (A \wedge C) .$$

L'équivalence est vraie car dans la table ci-dessous, les colonnes correspondant aux deux assertions sont identiques.

A	B	C	$(B \vee C)$	$A \wedge (B \vee C)$	$(A \wedge B)$	$(A \wedge C)$	$(A \wedge B) \vee (A \wedge C)$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V
V	F	V	V	V	F	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

Nous laissons au lecteur le soin de vérifier de même chacune des autres équivalences. □

Rares sont les démonstrations mathématiques qui utilisent explicitement les tables de vérité. Une démonstration typique est un enchaînement d'implications ou d'équivalences, partant des hypothèses pour aboutir à la conclusion. Ces enchaînements utilisent la *transitivité* de l'implication et de l'équivalence.

Proposition 1. *Soient A, B et C trois assertions. L'énoncé suivant est toujours vrai.*

$$\Big((A \Longrightarrow B) \wedge (B \Longrightarrow C)\Big) \Longrightarrow (A \Longrightarrow C)\ . \tag{10}$$

Si A implique B et B implique C, alors A implique C.

On en déduit facilement la transitivité de l'équivalence :

Corollaire 1. *Soient A, B et C des assertions, l'énoncé suivant est toujours vrai.*

$$\Big((A \Longleftrightarrow B) \wedge (B \Longleftrightarrow C)\Big) \Longrightarrow (A \Longleftrightarrow C)\ .$$

Si A équivaut à B et B équivaut à C, alors A équivaut à C.

Démonstration : Nous utilisons (une dernière fois) les tables de vérité, pour vérifier que quelles que soient les valeurs de vérité de A, B et C, l'implication (10) est vraie. Notons

- I_1 l'assertion $A \Longrightarrow B$,
- I_2 l'assertion $B \Longrightarrow C$,
- I_3 l'assertion $A \Longrightarrow C$.

A	B	C	I_1	I_2	$I_1 \wedge I_2$	I_3	$(I_1 \wedge I_2) \Longrightarrow I_3$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

□

Nous utiliserons des enchaînements d'équivalences pour démontrer le résultat suivant, qui décrit le comportement de l'implication par rapport à la négation.

Proposition 2. *Soient A et B deux assertions. Les équivalences suivantes sont toujours vraies.*

1.
$$\Big(\neg(A \Longrightarrow B)\Big) \iff \Big(A \wedge (\neg B)\Big)\,. \tag{11}$$
« L'implication $A \Longrightarrow B$ est fausse si et seulement si A est vrai et B est faux ».

2.
$$\Big(A \Longrightarrow B\Big) \iff \Big(\neg B \Longrightarrow \neg A\Big)\,. \tag{12}$$
« A implique B » est équivalent à « non B implique non A ».

Démonstration : Nous pourrions démontrer ces équivalences directement à l'aide des tables de vérité (nous conseillons au lecteur de le faire). Nous allons plutôt les déduire du théorème 1. Voici la démonstration de la première équivalence.

$$\begin{array}{rcll} \neg(A \Longrightarrow B) & \iff & \neg((\neg A) \vee B) & \text{par définition de l'implication} \\ & \iff & \neg(\neg A) \wedge \neg B & \text{par (8)} \\ & \iff & A \wedge \neg B & \text{par (7).} \end{array}$$

Voici la démonstration de la seconde équivalence.

$$\begin{array}{rcll} \Big(A \Longrightarrow B\Big) & \iff & \Big((\neg A) \vee B\Big) & \text{par définition de l'implication} \\ & \iff & \Big((\neg A) \vee (\neg(\neg B))\Big) & \text{par (7)} \\ & \iff & \Big((\neg(\neg B)) \vee (\neg A)\Big) & \text{par (2)} \\ & \iff & \Big((\neg B) \Longrightarrow (\neg A)\Big) & \text{par définition de l'implication.} \end{array}$$

□

L'équivalence (11) est la méthode habituelle que l'on utilise pour démontrer qu'une implication est fausse : il suffit d'exhiber une situation où A est vraie et B fausse pour infirmer l'implication $A \Longrightarrow B$. Par exemple, l'implication « $(n \leqslant 3) \Longrightarrow (n \mid 3)$ » est fausse, car on peut trouver un entier n tel que $(n \leqslant 3)$ soit vrai et $(n|3)$ soit faux : 2 est inférieur ou égal à 3 mais ne divise pas 3. On appelle cela « trouver un contre-exemple ».

L'équivalence (12) est aussi une technique de démonstration classique. L'implication « $(\neg B) \Longrightarrow (\neg A)$ » (« non B implique non A ») s'appelle la *contraposée* de l'implication $A \Longrightarrow B$. Par exemple, la contraposée de « $(n > 3) \Longrightarrow (n > 2)$ » est « $(n \leqslant 2) \Longrightarrow (n \leqslant 3)$ ». Il est parfois plus facile pour démontrer une implication de démontrer sa contraposée, nous y reviendrons.

1.2 Ensembles

Un *ensemble* peut être vu comme une collection d'objets mathématiques, appelés *éléments*, comme l'ensemble $\mathbb{N}$ des entiers naturels. Contentez-vous pour l'instant de l'idée intuitive d'un paquet d'éléments possédant une propriété commune, sur lequel on

a mis une étiquette rappelant cette propriété. Un ensemble n'est bien défini que si on peut dire sans ambiguïté si un élément appartient ou non à l'ensemble. Les sommets des Alpes ne forment pas un ensemble (comment décider qu'un endroit particulier est un sommet ?). Par contre l'ensemble des sommets cotés sur une carte donnée est bien défini. Deux ensembles sont égaux si et seulement si ils contiennent les mêmes éléments.

Le fait qu'un élément x appartienne à un ensemble A se note $x \in A$, et son contraire $x \notin A$ (« x n'appartient pas à A »). Par exemple $2 \in \mathbb{N}$ (2 appartient à $\mathbb{N}$) et $\sqrt{2} \notin \mathbb{N}$ (racine de 2 n'appartient pas à $\mathbb{N}$). Certains ensembles souvent utilisés ont une notation propre, comme l'ensemble $\mathbb{N}$ des entiers naturels, l'ensemble $\mathbb{R}$ des nombres réels, l'ensemble $\mathbb{C}$ des nombres complexes. Pour les autres, on utilise une définition, que l'on écrit entre accolades pour dire qu'il s'agit de l'ensemble des éléments vérifiant cette définition. On peut écrire un ensemble *en extension*, en donnant la liste de ses éléments. Voici deux définitions de l'ensemble des entiers naturels strictement inférieurs à 5.

$$\{\, n \in \mathbb{N} \,;\quad n < 5 \,\} = \{\, 0, 1, 2, 3, 4 \,\}\,.$$

Cet énoncé se lit « ensemble des n appartenant à $\mathbb{N}$ tels que $n < 5$ » ou « ensemble des entiers strictement inférieurs à 5 ». Voici deux définitions de l'ensemble des diviseurs de 12.

$$\{\, n \in \mathbb{N} \,;\quad n \,|\, 12 \,\} = \{\, 1, 2, 3, 4, 6, 12 \,\}\,.$$

On peut aussi définir des ensembles en extension par une liste infinie. Le plus souvent, celle-ci se déduit de $\mathbb{N}$. Par exemple l'ensemble des entiers supérieurs ou égaux à 5 :

$$\{\, n \in \mathbb{N} \,;\quad n \geqslant 5 \,\} = \{\, n + 5 \,;\quad n \in \mathbb{N} \,\}\,,$$

et l'ensemble des entiers pairs :

$$\{\, n \in \mathbb{N} \,;\quad 2 \,|\, n \,\} = \{\, 2n \,;\quad n \in \mathbb{N} \,\}\,,$$

Les ensembles que nous définirons seront des *sous-ensembles* ou *parties* d'un ensemble plus grand (comme l'ensemble des entiers $\mathbb{N}$ dans les exemples précédents).

Définition 1. *On dit qu'un ensemble A est un* sous-ensemble *ou une partie d'un ensemble E si tout élément de A est aussi élément de E.*

Si E est l'ensemble de référence (l'ensemble des entiers dans nos exemples), l'ensemble des parties de E se note $\mathcal{P}(E)$. Il contient toujours E lui-même, ainsi que l'ensemble vide, noté $\emptyset$. Si A est un sous-ensemble (une partie) de E, on dit aussi que A est *inclus* dans E, et on note $A \subset E$. On note aussi $E \supset A$ pour « E contient A ». Voici l'écriture en extension de $\mathcal{P}(\{0, 1, 2\})$, qui est l'ensemble des parties de l'ensemble à trois éléments $\{0, 1, 2\}$.

$$\mathcal{P}(\{0, 1, 2\}) = \Big\{\, \emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\} \,\Big\}\,.$$

Un ensemble qui ne contient qu'un seul élément, comme $\{0\}$, est un *singleton*. L'ensemble $\mathcal{P}(\{0,1,2\})$ contient 8 éléments, dont chacun est lui-même un ensemble.

Il est fréquent (et souvent utile) de passer d'un ensemble A à l'assertion $x \in A$ (vraie ou fausse). Les connecteurs logiques entre assertions (« non », « et », « ou ») se traduisent par des opérations ensemblistes : complémentaire, intersection, réunion. Nous utiliserons cette correspondance comme définition des opérations ensemblistes.

ensembles A, B	assertions $(x \in A), (x \in B)$
complémentaire ${}^cA$	négation (« non ») $x \in {}^cA \iff \neg(x \in A) \iff x \notin A$
intersection (« inter ») $A \cap B$	conjonction (« et ») $(x \in A \cap B) \iff \Big((x \in A) \wedge (x \in B)\Big)$
réunion (« union ») $A \cup B$	disjonction (« ou ») $(x \in A \cup B) \iff \Big((x \in A) \vee (x \in B)\Big)$

Au travers de ce dictionnaire l'implication

$$(x \in A) \Longrightarrow (x \in B), \text{ soit } (\neg(x \in A)) \vee (x \in B) \ ,$$

devient $x \in ({}^cA \cup B)$. Elle est toujours vraie si et seulement si le complémentaire de $({}^cA \cup B)$, est vide, c'est-à-dire si A est inclus dans B. Les propriétés $(x \in A)$ et $(x \in B)$ sont équivalentes si les deux inclusions $A \subset B$ et $B \subset A$ sont vraies, c'est-à-dire si les deux ensembles contiennent les mêmes éléments. On dit qu'ils sont égaux, et on note simplement $A = B$. Pour démontrer que deux ensembles sont égaux, on doit montrer que chacun est inclus dans l'autre (tout comme pour démontrer une équivalence, on doit montrer les deux implications).

On déduit du théorème 1 les propriétés suivantes des opérations ensemblistes. Les démonstrations constituent un bon exercice de traduction, que nous laissons au lecteur. Nous conseillons aussi de remplacer A par $\{n \in \mathbb{N}\,;\ n \leqslant 6\}$, B par $\{n \in \mathbb{N}\,;\ 2 \,|\, n\}$ et C par $\{n \in \mathbb{N}\,;\ 3 \,|\, n\}$ et d'écrire en extension tous les ensembles du théorème.

Théorème 2. *Soient A, B et C trois ensembles. Les égalités ensemblistes suivantes sont toujours vraies.*

- *Commutativité :*

$$\Big(A \cap B\Big) = \Big(B \cap A\Big) \ . \tag{13}$$

$$\Big(A \cup B\Big) = \Big(B \cup A\Big) \ . \tag{14}$$

- *Associativité :*

$$\Big(A \cap (B \cap C)\Big) = \Big((A \cap B) \cap C\Big) \ . \tag{15}$$

$$\Big(A \cup (B \cup C)\Big) = \Big((A \cup B) \cup C\Big) \ . \tag{16}$$

- *Distributivité :*

$$\Big(A \cap (B \cup C)\Big) = \Big((A \cap B) \cup (A \cap C)\Big) \,. \tag{17}$$

$$\Big(A \cup (B \cap C)\Big) = \Big((A \cup B) \cap (A \cup C)\Big) \,. \tag{18}$$

- *Complémentaires : soient A et B des parties d'un ensemble E. Alors :*

$$E \setminus (E \setminus A) = A \,, \tag{19}$$

$$E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B) \,, \tag{20}$$

$$E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B) \,. \tag{21}$$

Nous nous placerons toujours dans le cas où tous les ensembles considérés sont des parties d'un ensemble de référence E. Le complémentaire d'une partie A est alors implicitement défini comme l'ensemble des éléments de E qui n'appartiennent pas à A. Moyennant cette convention, le résultat d'une opération ensembliste quelconque sur des parties de E est encore une partie de E. Il est commode de visualiser E par un rectangle et les sous-ensembles de E par des « patates » hachurées dessinées dans ce rectangle. Le résultat s'appelle un *diagramme de Venn*, plutôt qu'un sac de patates (figure 1). Nous conseillons au lecteur de visualiser les égalités ensemblistes du théorème 2 sur des diagrammes de Venn.

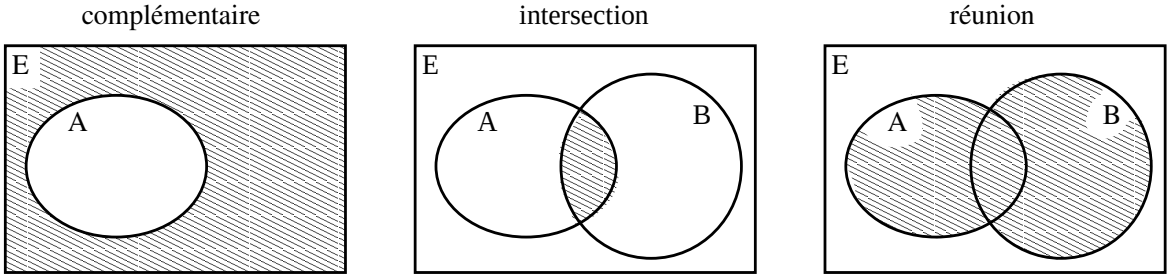

FIG. 1 – Diagrammes de Venn pour le complémentaire, l'intersection et la réunion.

Il existe d'autres manières utiles de combiner des ensembles entre eux pour en former de nouveaux. Nous utiliserons plusieurs fois le *produit cartésien*.

Définition 2. *Soient A et B deux ensembles. On appelle* produit cartésien *de A par B et on note $A \times B$ l'ensemble des couples formés d'un élément de A et un de B.*

$$A \times B = \{\, (a, b) \;;\quad a \in A \text{ et } b \in B \,\} \,.$$

Le produit cartésien de A par lui-même se note A^2. On le généralise à plus de deux copies de A en définissant A^n comme l'ensemble des n-uplets formés d'éléments de A.

$$A^n = \{\, (a_1, \ldots, a_n) \,,\ (a_1 \in A) \wedge \ldots \wedge (a_n \in A) \,\} \,.$$

Attention, dans un n-uplet, certaines coordonnées peuvent être identiques et l'ordre est important. Par exemple, si a et b sont deux éléments distincts de A, les triplets (a, b, a) et (a, a, b) sont des éléments distincts de A^3.

1.3 Quantificateurs

Les quantificateurs sont les deux symboles $\forall$ « quel que soit » et $\exists$ « il existe ». On les utilise pour des énoncés du type :

$$\forall n \in \mathbb{N}\,,\ \exists m \in \mathbb{N}\,;\quad n < m\,. \tag{22}$$

Cette formule se lit : quel que soit n appartenant à $\mathbb{N}$, il existe m appartenant à $\mathbb{N}$ tel que $n < m$. Soit encore : pour tout entier n, il existe un entier m strictement plus grand que n. Il est crucial de retenir que dans ce cas l'entier m peut dépendre de l'entier n. Cette assertion est vraie : pour tout n, le nombre $m = n + 1$ vérifie bien $n < m$.

L'ordre dans lequel on écrit les quantificateurs est très important. Echangeons dans (22) les deux quantificateurs.

$$\exists m \in \mathbb{N}\,;\quad \forall n \in \mathbb{N}\,,\quad n < m\,.$$

Cette assertion se lit : il existe un entier m tel que tout entier n vérifie $n < m$ (ce qui est faux).

Pour écrire la négation d'une assertion comportant des quantificateurs on change les $\forall$ en $\exists$ et les $\exists$ en $\forall$, puis on écrit la négation de l'assertion qui suit la liste des quantificateurs. Ceci est tout à fait conforme à l'intuition. La négation de « tout les x vérifient A » est bien « il existe un x qui ne vérifie pas A ». La négation de « il existe un x qui vérifie A » est bien « aucun x ne vérifie A » soit encore « tous les x vérifient $\neg A$ ». Ecrivons par exemple la négation de l'assertion (22).

$$\exists n \in \mathbb{N}\ ;\quad \forall m \in \mathbb{N}\,,\ (n \geqslant m)\,.$$

Il existe un entier n supérieur ou égal à tout entier m (ce qui est faux).

Attention, les quantificateurs ne sont pas toujours distributifs par rapport à « et » et « ou ». Par exemple, « il existe un entier supérieur à 7 et inférieur à 6 » (faux) n'est pas équivalent à « il existe un entier supérieur à 7 et il existe un entier inférieur à 6 » (vrai). De même « tout entier est inférieur ou égal à 6, ou bien supérieur ou égal à 7 » (vrai) n'est pas équivalent à « tout entier est inférieur ou égal à 6 ou tout entier est supérieur ou égal à 7 » (faux).

Nous commettrons souvent l'abus de notation consistant à regrouper des quantificateurs de même nature. Par exemple :

$$\forall n \in \mathbb{N}\,,\ \forall m \in \mathbb{N}\,,\quad m + n \in \mathbb{N}\,,$$

que l'on pourrait aussi écrire

$$\forall (n, m) \in \mathbb{N}^2\,,\quad m + n \in \mathbb{N}\,,$$

sera plutôt écrit :

$$\forall n, m \in \mathbb{N}\,,\quad m + n \in \mathbb{N}\,.$$

(La somme de deux entiers naturels est un entier naturel.)

Ou encore,

$$\exists n \in \mathbb{N}\,,\ \exists m \in \mathbb{N}\ ;\quad n+m<10\,,$$

deviendra :

$$\exists n, m \in \mathbb{N}\ ;\quad n+m<10\,.$$

(Il existe deux entiers dont la somme est inférieure à 10.)

Constatez en la lisant à haute voix que la formule suivante définit bien la divisibilité.

$$\forall m, n \in \mathbb{N}\,,\ (m\,|\,n) \iff \Big(\exists k \in \mathbb{N}\ ;\quad n = km\Big)\,.$$

1.4 Applications

Les fonctions et les applications sont des correspondances entre ensembles. Pour définir une fonction f, il faut d'abord un ensemble de départ E (la *source*) et un ensemble d'arrivée F (le *but*). Il faut ensuite un sous-ensemble Γ du produit cartésien de $E \times F$, c'est-à-dire un ensemble de couples (x, y) où $x \in E$ et $y \in F$. L'ensemble Γ s'appelle le *graphe* de la fonction. La règle de base est qu'un élément de E ne peut pas correspondre à deux éléments de F. Ceci s'écrit :

$$\Big(((x,y) \in \Gamma) \wedge ((x,z) \in \Gamma)\Big) \implies y = z\,.$$

La donnée de l'ensemble de départ, de l'ensemble d'arrivée et du graphe définit la fonction f. Si $(x, y) \in \Gamma$, on dit que y est l'*image* de x : $y = f(x)$. La notation standard pour une fonction est la suivante.

$$\begin{array}{ccc} & f & \\ E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array}$$

Elle se lit « fonction f de E vers F qui à x associe $f(x)$ ».

On utilise le plus souvent *fonction* et *application* comme des synonymes. En toute rigueur une application est une fonction telle que tout élément de l'ensemble de départ admet une image (et une seule). Pour une fonction, le sous-ensemble de l'ensemble de départ formé des éléments qui ont effectivement une image s'appelle le *domaine de définition*. Dans ce chapitre, nous nous limiterons aux applications.

Définition 3. *Soient E et F deux ensembles et f une application de E dans F.*

1. *Soit A un sous-ensemble de E. On appelle* image de A par f *et on note $f(A)$ l'ensemble des images des éléments de A.*

$$f(A) = \{\, y \in F\ ;\quad \exists x \in A\,,\ f(x) = y\,\}\,.$$

2. *Soit B un sous-ensemble de F. On appelle* image réciproque de B par f *et on note $f^{-1}(B)$ l'ensemble des éléments de E dont l'image appartient à B.*

$$f^{-1}(B) = \{\, x \in E \,;\quad f(x) \in B \,\}\ .$$

Attention à la notation f^{-1} : elle ne signifie pas que f est inversée. C'est une convention pour désigner un sous-ensemble de l'espace de départ. Un élément x de E tel que $f(x) = y$ s'appelle un *antécédent* de y. D'après la définition 3, l'ensemble des antécédents de y est $f^{-1}(\{y\})$.

Soit $E = \{0, 1, 2, 3\}$ et $F = \{0, 1, 2\}$. Considérons l'application qui à un nombre associe le reste de sa division euclidienne par 2 : 0 s'il est pair, 1 s'il est impair. Le graphe de cette application est :

$$\Gamma = \{\, (0,0), (1,1), (2,0), (3,1) \,\}\ .$$

Il est parfois commode de représenter un graphe par un ensemble de flèches entre deux diagrammes de Venn (figure 2). L'image de $\{0, 2\}$ est le singleton $\{0\}$. L'image réciproque de $\{1\}$ est $\{1, 3\}$. L'image réciproque de $\{2\}$ est l'ensemble vide.

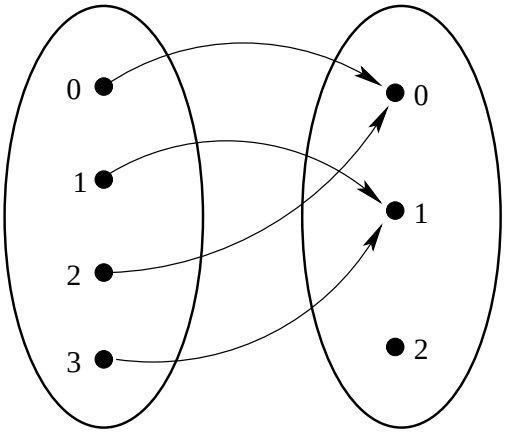

FIG. 2 – Représentation graphique d'une application de $\{0, 1, 2, 3\}$ vers $\{0, 1, 2\}$.

Soient E, F, et G trois ensembles, f une application de E vers F et g une application de F vers G. On définit la *composée* de f par g , notée $g \circ f$, comme l'application de E vers G qui à x associe $g \circ f(x) = g(f(x))$. Attention à l'ordre des applications dans l'écriture $g \circ f$: c'est l'ordre inverse des flèches dans le schéma ci-dessous.

$$\begin{array}{ccccc} & & f & & g & \\ E & \longrightarrow & F & \longrightarrow & G & \\ x & \longmapsto & f(x) & \longmapsto & g \circ f(x) = g(f(x)) \ . \end{array}$$

Définition 4. *Soient E et F deux ensembles et f une application de E vers F. On dit que f est :*

1. injective *si tout élément de l'ensemble d'arrivée possède* au plus *un antécédent dans l'ensemble de départ.*

$$\forall x_1, x_2 \in E\ , \quad \Big(f(x_1) = f(x_2)\Big) \implies x_1 = x_2\ .$$

2. surjective *si tout élément de l'ensemble d'arrivée possède* au moins *un antécédent dans l'ensemble de départ.*

$$\forall y \in F\ ,\ \exists x \in E\ ; \quad f(x) = y\ .$$

3. bijective *si tout élément de l'ensemble d'arrivée possède* exactement *un antécédent dans l'ensemble de départ.*

Une application bijective, ou *bijection*, est donc à la fois injective et surjective (voir figure 3).

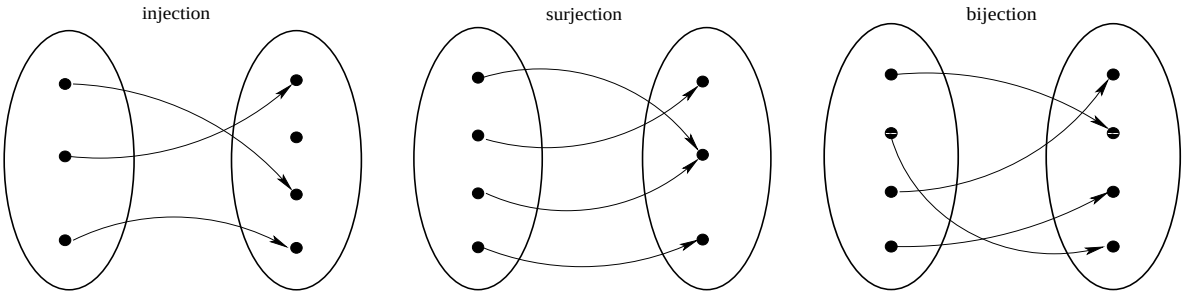

FIG. 3 – Représentations graphiques d'une injection, d'une surjection et d'une bijection.

Voici comment les applications injectives, surjectives et bijectives se comportent vis-à-vis de la composition. La démonstration de cette assertion est laissée au lecteur à titre d'exercice.

Proposition 3. *Soient E, F, et G trois ensembles, f une application de E vers F et g une application de F vers G.*

1. *Si f et g sont injectives alors $g \circ f$ est injective.*
2. *Si f et g sont surjectives alors $g \circ f$ est surjective.*
3. *Si f et g sont bijectives alors $g \circ f$ est bijective.*
4. *Si $g \circ f$ est injective alors f est injective.*
5. *Si $g \circ f$ est surjective alors g est surjective.*

Si une application de E vers F est bijective, tout élément de F a un antécédent et un seul. On peut alors définir *l'application réciproque* de f, notée f^{-1} :

$$f(x) = y \iff x = f^{-1}(y)\ .$$

Si f est bijective, la composée de f par son application réciproque f^{-1} est l'application qui à x associe x, de E vers E. On l'appelle *application identique*, ou *identité*.

$$\begin{array}{ccccc} & f & & f^{-1} & \\ E & \longrightarrow & F & \longrightarrow & E \\ x & \longmapsto & f(x) & \longmapsto & f^{-1}\circ f(x) = f^{-1}(f(x)) = x\ . \end{array}$$

Les notations pour l'application réciproque et pour l'image réciproque d'une partie de l'ensemble d'arrivée F sont liées par la relation :

$$f^{-1}(\{y\}) = \{f^{-1}(y)\}\ .$$

On prendra garde au fait que si l'image réciproque d'une partie est définie pour toute application, l'application réciproque, quant à elle, n'est définie que pour une application bijective.

1.5 Cardinaux

Nous allons utiliser la notion de bijection pour définir le cardinal d'un ensemble fini. Intuitivement, deux ensembles ont le même nombre d'éléments si et seulement si on peut définir une bijection entre ces ensembles. Les définitions qui suivent formalisent cette intuition.

Définition 5. *Soient E et F des ensembles. On dit que E* et F ont le même cardinal *s'il existe une bijection de E sur F.*

Soient E un ensemble et n un entier. On dit que E est de cardinal n *si E et $\{1,\dots,n\}$ ont le même cardinal.*

Soit E un ensemble. On dit que E est fini *s'il existe un entier n tel que E soit de cardinal n.*

Proposition 4. *Soient m et n des entiers. S'il existe une injection*

$$f : \{1,\dots,m\} \longrightarrow \{1,\dots,n\}\ ,$$

alors $m \leqslant n$.

Démonstration : On raisonne par récurrence sur m. Si $m = 0$, la conclusion est vérifiée. Supposons le résultat vrai pour $m-1$. Soit

$$f : \{1,\dots,m\} \longrightarrow \{1,\dots,n\}\ ,$$

une application injective. Comme f est injective, on a

$$\forall i \in \{1,\dots,m\},\quad i \neq m \Rightarrow f(i) \neq f(m)\ .$$

On peut donc définir

$$\begin{array}{rcl} g : \{1, \ldots, m-1\} & \longrightarrow & \{1, \ldots, n-1\} \\ i & \longmapsto & \begin{cases} f(i) \text{ si } f(i) < f(m), \\ f(i) - 1 \text{ si } f(i) > f(m). \end{cases} \end{array}$$

L'application ainsi définie est injective. Donc, par hypothèse de récurrence, $m - 1 \leqslant n - 1$. D'où $m \leqslant n$. □

Corollaire 2. *Soient m et n des entiers. S'il existe une bijection de $\{1, \ldots, m\}$ sur $\{1, \ldots, n\}$, alors $m = n$.*

Démonstration : Notons f une telle bijection. Alors f et f^{-1} sont injectives et on applique la proposition précédente. □

Ce corollaire montre que si E est un ensemble de cardinal m et de cardinal n, alors $m = n$. En effet, dans ce cas il existe une bijection f de E sur $\{1, \ldots, m\}$ et g de E sur $\{1, \ldots, n\}$ et $g \circ f^{-1}$ fournit une bijection de $\{1, \ldots, m\}$ sur $\{1, \ldots, n\}$.

Définition 6. *Soit E un ensemble fini. On appelle* cardinal de E *et on note* $\mathrm{Card}(E)$ *l'unique entier n tel que E soit de cardinal n.*

Exemple 1. *Si a, $b \in \mathbb{Z}$, avec $a \leqslant b$, alors*

$$\mathrm{Card}(\{a, a+1, \ldots, b-1, b\} = b - a + 1 \, .$$

En effet l'application

$$\begin{array}{rcl} f : \{a, \ldots, b\} & \longrightarrow & \{1, \ldots, b-a+1\} \\ x & \longmapsto & x - a + 1 \end{array}$$

est bijective.

Proposition 5. *Soit E un ensemble fini et X une partie de E. Alors*

a) *L'ensemble X est fini ;*

b) $\mathrm{Card}(X) \leq \mathrm{Card}(E)$ *;*

c) *Si* $\mathrm{Card}(X) = \mathrm{Card}(E)$*, alors $X = E$.*

Démonstration : Soit n le cardinal de E. Il existe donc une bijection Φ de E sur $\{1, \ldots, n\}$. L'application obtenue par restriction à X :

$$\begin{array}{rcl} X & \longrightarrow & \Phi(X) \\ x & \longmapsto & \Phi(x) \, , \end{array}$$

est également bijective. Quitte à remplacer X par $\Phi(X)$, il suffit de traiter le cas où $E = \{1, \ldots, n\}$.

On raisonne alors par récurrence sur le cardinal de E. Si $n = 0$, alors $E = X = \emptyset$ et le résultat est valide. Supposons le résultat démontré pour les ensembles de cardinal $n-1$, et montrons le pour $E = \{1, \ldots, n\}$. Si $X = E$, alors $\mathrm{Card}(X) = \mathrm{Card}(E)$ et les assertions a), b) et c) sont vérifiées. Si $X \neq E$, il nous suffit de montrer que X est fini de cardinal inférieur ou égal à $n-1$. Mais dans ce cas, il existe $i \in \{1, \ldots, n\}$ tel que $i \notin X$. On considère alors l'application

$$\begin{array}{rcl} f : \{x \in E\,; \quad x \neq i\} & \longrightarrow & \{1, \ldots, n-1\} \\ x & \longmapsto & \begin{cases} x \text{ si } x < i, \\ x - 1 \text{ si } x > i. \end{cases} \end{array}$$

f est bijective, donc $\mathrm{Card}(\{x \in E\,;\ x \neq i\}) = n-1$ et par hypothèse de récurrence X est fini et

$$\mathrm{Card}(X) \leqslant n - 1 < \mathrm{Card}(E).$$

ce qui montre les assertions dans ce cas. □

Corollaire 3. *Soient E et F des ensembles et $f : E \to F$ une application.*
Si F est fini et si f est injective, alors

a) *E est fini ;*

b) $\mathrm{Card}(E) \leq \mathrm{Card}(F)$ *;*

c) *f est bijective si et seulement si* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Si E est fini et si f est surjective, alors

a) *F est fini ;*

b) $\mathrm{Card}(F) \leq \mathrm{Card}(E)$ *;*

c) *f est bijective si et seulement si* $\mathrm{Card}(E) = \mathrm{Card}(F)$.

Démonstration : Si f est injective, on considère l'application

$$\begin{array}{rcl} g : E & \longrightarrow & f(E) \\ x & \longmapsto & f(x) \end{array}$$

g est bijective. Donc E et $f(E)$ ont même cardinal. Donc $\mathrm{Card}(E) = \mathrm{Card}(f(E)) \leqslant \mathrm{Card}(F)$. L'application f est bijective si et seulement si $f(E) = F$ ce qui est équivalent à $\mathrm{Card}(E) = \mathrm{Card}(F)$ par ce qui précède.

Supposons f surjective, c'est-à-dire telle que

$$\forall y \in F,\ \exists x \in E, \quad f(x) = y.$$

Donc il existe une application $g : E \to F$ telle que

$$\forall y \in F, \quad f(g(y)) = y.$$

La composée $f \circ g$ est l'appication identique de F, donc g est injective. On applique alors le cas injectif à g. □

Rappelons la définition du complémentaire :

Définition 7. *Soient A et B des ensembles, on note*

$$A \setminus B = \{x \in A\,;\ x \notin B\}.$$

Si $B \subset A$, $A \setminus B$ est appelé le complémentaire de B dans A.

Proposition 6. *Si A est fini et $B \subset A$, alors*

$$\mathrm{Card}(A) = \mathrm{Card}(B) + \mathrm{Card}(A \setminus B).$$

Démonstration : Par la proposition 5, on sait que B et $A \setminus B$ sont finis. Notons p le cardinal de B et q le cardinal de $A \setminus B$. Il existe donc des bijections

$$\Phi_1 : B \longrightarrow \{1, \ldots, p\}$$

et

$$\Phi_2 : A \setminus B \longrightarrow \{p+1, \ldots, p+q\}$$

L'application

$$\begin{array}{rcl} \Phi : A & \longrightarrow & \{1, \ldots, p+q\} \\ x & \longmapsto & \begin{cases} \Phi_1(x) \text{ si } x \in B, \\ \Phi_2(x) \text{ si } x \in A \setminus B \end{cases} \end{array}$$

est bijective donc $\mathrm{Card}(A) = p + q$. □

Proposition 7. *Soient A un ensemble fini, r un entier et $(A_i)_{i \in \{1,\ldots,r\}}$ une famille de parties de A telle que*

i. $A = A_1 \cup \cdots \cup A_r$;

ii. $\forall i, j \in \{1, \ldots, r\}, \quad i \neq j \Rightarrow A_i \cap A_j = \emptyset$

Alors

$$\mathrm{Card}(A) = \sum_{i=1}^{r} \mathrm{Card}(A_i).$$

Démonstration : On raisonne par récurrence sur r.

Si $r = 1$, $A = A_1$ et le résultat est vrai. Si c'est vrai pour $r - 1$, par hypothèse de récurrence, appliquée à l'ensemble $A_1 \cup \cdots \cup A_{r-1}$, on a

$$\mathrm{Card}(A_1 \cup \cdots \cup A_{r-1}) = \sum_{i=1}^{r-1} \mathrm{Card}(A_i).$$

Mais $A_r = A \setminus (A_1 \cup \cdots \cup A_{r-1})$. Donc

$$\mathrm{Card}(A) = \mathrm{Card}(A_r) + \sum_{i=1}^{r-1} \mathrm{Card}(A_i)$$

ce qui prouve le résultat pour r. □

Définition 8. *Soit E un ensemble fini et soit $(\lambda_e)_{e\in E}$ une famille de nombres réels (ou complexes) Soit $\Phi : \{1,\dots,n\} \to E$ une bijection. La somme*

$$\sum_{i=1}^{n} \lambda_{\Phi(i)}$$

ne dépend pas du choix de Φ, on la note $\sum_{e\in E} \lambda_e$.

Exemple 2. *Ainsi* $\mathrm{Card}(E) = \sum_{e\in E} 1$.

On peut définir de même le produit $\prod_{e\in E} \lambda_e$.

Corollaire 4 (Principe des bergers)**.** *Soient E un ensemble fini et F un ensemble. Soit $f : E \to F$ une application, alors $f(E)$ est fini et :*

$$\mathrm{Card}(E) = \sum_{y\in f(E)} \mathrm{Card}(f^{-1}(\{y\}))\ .$$

Démonstration : L'application $g : E \to f(E)$ définie par $g(x) = f(x)$ pour tout x de E est surjective. Par conséquent, $f(E)$ est fini. Soit $m = \mathrm{Card}(f(E))$. On fixe donc une bijection

$$\Phi : \{1,\dots,m\} \longrightarrow f(E).$$

On applique alors la proposition à la famille $(f^{-1}(\{\Phi(i)\}))_{i\in\{1,\dots,n\}}$ de parties de E. □

Proposition 8. *Soient E et F des ensembles finis, alors :*

a) $\mathrm{Card}(E \times F) = \mathrm{Card}(E)\mathrm{Card}(F)$ *;*

b) $\mathrm{Card}(E^F) = \mathrm{Card}(E)^{\mathrm{Card}(F)}$ *;*

c) $\mathrm{Card}(\mathcal{P}(E)) = 2^{\mathrm{Card}(E)}$.

Démonstration : Pour a), on considère l'application surjective $f : E \times F \to F$ qui applique (x, y) sur y et on applique la proposition précédente, en notant que pour tout y de F, l'application

$$\begin{array}{rcl} E & \longrightarrow & f^{-1}(\{y\}) \\ x & \longmapsto & (x, y) \end{array}$$

est bijective.

Pour b), on raisonne par récurrence sur $\mathrm{Card}(F)$ en considérant pour tout $x \in F$ l'application

$$\begin{array}{rcl} E^F & \longrightarrow & E^{F-\{x\}} \\ g & \longmapsto & g_{|F-\{x\}}. \end{array}$$

Pour c), on vérifie que l'application de $\mathcal{P}(E)$ sur $\{0,1\}^E$ qui envoie une partie A sur l'application

$$\begin{array}{rcl} \mathbb{I}_A : E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} 1 \text{ si } x \in A, \\ 0 \text{ sinon.} \end{cases} \end{array}$$

est bijective. □

1.6 Relations

Dans ce cours, une *relation* $\mathcal{R}$ établit une correspondance entre deux éléments d'un même ensemble. Elle est définie par l'ensemble E sur lequel elle opère, et par son graphe Γ, qui est un sous-ensemble du produit cartésien $E \times E$. Le fait qu'un couple (x, y) appartienne au graphe Γ est noté $x\mathcal{R}y$ (x est en relation avec y). Considérons par exemple la relation « divise » sur l'ensemble $E = \{1, 2, 3, 4, 5, 6\}$. Son graphe est :

$$\Gamma = \{\, (1,1), (1,2), (1,3), (1,4), (1,5), (1,6), \\ (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6) \,\} .$$

Ses éléments sont visualisés par des flèches sur la figure 4.

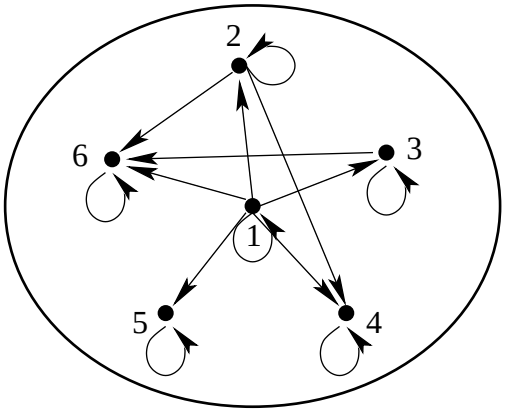

FIG. 4 – Représentation graphique de la relation « divise » sur $\{1, 2, 3, 4, 5, 6\}$.

Les propriétés intéressantes que l'on attend d'une relation sont les suivantes.

Définition 9. *On dit qu'une relation $\mathcal{R}$ sur un ensemble E est :*

1. réflexive *si tout élément est relié à lui-même*

$$\forall x \in E\,,\ x\mathcal{R}x\ ;$$

2. symétrique *si x relié à y entraîne que y est relié à x*

$$\forall x, y \in E\,,\ (x\mathcal{R}y) \Longrightarrow (y\mathcal{R}x)\ ;$$

3. anti-symétrique *si x relié à y et y relié à x entraînent $x = y$*

$$\forall x, y \in E\,,\ \Big((x\mathcal{R}y) \wedge (y\mathcal{R}x)\Big) \Longrightarrow x = y\ ;$$

4. transitive *si quand x est relié à y et y à z alors x est relié à z*

$$\forall x, y, z \in E\,,\ \Big((x\mathcal{R}y) \wedge (y\mathcal{R}z)\Big) \Longrightarrow x\mathcal{R}z\ .$$

Les relations servent à traduire mathématiquement des comparaisons entre éléments d'un même ensemble. Ces comparaisons peuvent être de deux types.

- x a le même ... que y (la même valeur, la même image par une fonction...) : c'est une relation *d'équivalence*.
- x est plus ... que y (plus petit, plus grand, plus tôt...) : c'est une relation *d'ordre*.

Définition 10. *Soit $\mathcal{R}$ une relation sur un ensemble E.*

1. *On dit que $\mathcal{R}$ est une* relation d'équivalence *si elle est à la fois* réflexive, symétrique et transitive*.*
2. *On dit que $\mathcal{R}$ est une* relation d'ordre *si elle est à la fois* réflexive, antisymétrique et transitive*.*

Voici des exemples de chacun des deux types de relations.

Notre premier exemple de relation d'équivalence est la congruence des entiers. Soit p un entier strictement positif fixé. Définissons la relation $\mathcal{R}$ sur $\mathbb{N}$ par :

$$\forall m, n \in \mathbb{N}\,, \quad \Big(m\mathcal{R}n\Big) \iff \Big(p \,|\, (m-n)\Big)$$

On dit que m et n sont congrus modulo p et on note « $m \equiv n$ modulo p ». Il est facile de vérifier que la congruence modulo p est réflexive, symétrique et transitive. Les nombres pairs sont tous congrus à 0 modulo 2, les nombres impairs sont congrus à 1. Vérifiez sur votre agenda, où les jours de l'année sont numérotés, que tous les lundis sont congrus entre eux modulo 7.

Pour notre deuxième exemple de relation d'équivalence, nous allons revenir sur la notion de cardinal d'un ensemble. Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble de ses parties. Définissons la relation $\mathcal{R}$ sur $\mathcal{P}(E)$ qui relie deux parties A et B s'il existe une bijection de A vers B. Cette relation est :

- réflexive : l'application identique est une bijection de E vers lui-même,
- symétrique : si f est une bijection de A vers B alors l'application réciproque f^{-1} est une bijection de B vers A,
- transitive : si f est une bijection de A vers B et g est une bijection de B vers C, alors $g \circ f$ est une bijection de A vers C.

Le *cardinal* est la propriété commune que possèdent deux parties reliées par cette relation d'équivalence. Il caractérise leur *classe d'équivalence*.

Définition 11. *Soit E un ensemble et $\mathcal{R}$ une relation d'équivalence sur E. Pour tout élément x de E, la* classe d'équivalence *de x pour $\mathcal{R}$ est l'ensemble, noté $\mathfrak{cl}_{\mathcal{R}}(x)$ de tous les éléments de E auxquels x est relié.*

$$\mathfrak{cl}_{\mathcal{R}}(x) = \{\, y \in E\,, x\mathcal{R}y \,\}\,.$$

L'ensemble des classes d'équivalence s'appelle ensemble quotient *de E par $\mathcal{R}$, et il est noté $E/\mathcal{R}$.*

Théorème 3. *Deux classes d'équivalence sont égales ou bien disjointes.*

Démonstration : Soient x et y deux éléments de E. Ces deux éléments sont reliés ou ils ne le sont pas : nous distinguons les deux cas.

1. *Si x est relié à y.*
   Nous allons démontrer que les deux classes sont égales. Soit z un élément de $\mathfrak{cl}_{\mathcal{R}}(y)$. Par définition d'une classe d'équivalence, $y\mathcal{R}z$. Comme $x\mathcal{R}y$ et $y\mathcal{R}z$, d'après la transitivité, $x\mathcal{R}z$. Nous venons de montrer que tout élément de $\mathfrak{cl}_{\mathcal{R}}(y)$ appartient aussi à $\mathfrak{cl}_{\mathcal{R}}(x)$. Donc $\mathfrak{cl}_{\mathcal{R}}(y) \subset \mathfrak{cl}_{\mathcal{R}}(x)$. Comme la relation est symétrique, y est relié à x. Donc ce qui précède s'applique en permutant x et y. Donc $\mathfrak{cl}_{\mathcal{R}}(x) \subset \mathfrak{cl}_{\mathcal{R}}(y)$. Comme les deux inclusions sont vraies, les deux classes sont égales.
2. *Si x n'est pas relié à y.*
   Nous allons démontrer que l'intersection des deux classes est vide. D'après la transitivité, pour tout $z \in E$, l'implication suivante est vraie.

   $$\Big((x\mathcal{R}z) \wedge (z\mathcal{R}y)\Big) \Longrightarrow (x\mathcal{R}y)\ .$$

   Donc si $x\mathcal{R}y$ est fausse, alors l'une des deux relations $x\mathcal{R}z$, $z\mathcal{R}y$ est fausse. Donc un élément z de E ne peut pas appartenir à la fois à $\mathfrak{cl}_{\mathcal{R}}(x)$ et à $\mathfrak{cl}_{\mathcal{R}}(y)$: leur intersection est vide.

□

Tout élément de E appartient à sa propre classe d'équivalence car la relation est réflexive, et à aucune autre d'après le théorème précédent. On dit que l'ensemble des classes d'équivalences constitue une *partition* de E (figure 5).

Définition 12. *Soit E un ensemble et $P \subset \mathcal{P}(E)$ un ensemble de parties de E. On dit que P est une* partition *de E si tout élément de E appartient à un et un seul des éléments de P.*

Considérons la relation de congruence modulo p sur $\mathbb{Z}$. La classe d'équivalence de 0 est l'ensemble des multiples de p, la classe d'équivalence de 1 est l'ensemble de tous les entiers n tels que $n-1$ est un multiple de $p\ldots$:

$$\forall i \in \{0,\ldots,p-1\}\ ,\quad \mathfrak{cl}_{\mathcal{R}}(i) = \{i+np\,,\ n \in \mathbb{N}\}\ .$$

L'ensemble quotient est formé de ces p classes d'équivalence.

Considérons maintenant la relation d'équivalence $\mathcal{R}$ sur $\mathcal{P}(\mathbb{N})$ qui relie deux ensembles d'entiers s'il existe une bijection de l'un vers l'autre. La classe d'équivalence de $\{1,\ldots,n\}$ contient toutes les parties de $\mathbb{N}$ qui ont n éléments. Pour $m \neq n$ les classes de $\{1,\ldots,m\}$ et $\{1,\ldots,n\}$ sont disjointes, car il n'existe pas de bijection entre $\{1,\ldots,m\}$ et $\{1,\ldots,n\}$. L'ensemble quotient de $\mathcal{P}(\mathbb{N})$ par la relation $\mathcal{R}$ est en bijection avec $\mathbb{N}$.

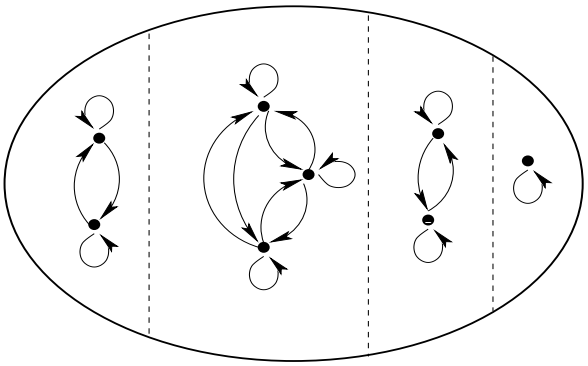

FIG. 5 – Représentation graphique d'une relation d'équivalence. Partition en classes d'équivalence.

Passons maintenant aux relations d'ordre. L'ordre le plus naturel est celui des nombres entre eux. Observons que « $<$ » et « $>$ » ne sont pas réflexives. Par contre « $\leqslant$ » et « $\geqslant$ » sont bien des relations d'ordre. Si deux éléments sont reliés par une relation d'ordre, on dit qu'ils sont comparables. Si tous les éléments sont comparables deux à deux, on dit que l'ordre est *total*. C'est le cas pour « $\leqslant$ » et « $\geqslant$ » mais pas pour la relation « divise » sur $\mathbb{N}$, qui est une relation d'ordre *partiel*. Si E est un ensemble, l'inclusion est une relation d'ordre partiel sur $\mathcal{P}(E)$.

Voici un autre exemple. Supposons que E soit un alphabet, pour lequel on a choisi un ordre total, noté $\leqslant$: l'alphabet latin dont les lettres sont rangées de « A » à « Z », $E = \{0, 1\}$ avec $0 \leqslant 1$, etc... Les éléments de E^n sont des n-uplets de lettres, donc des mots de longueur n. Comment les ranger ? On peut bien sûr définir une relation d'ordre coordonnée par coordonnée :

$$(x_1, \ldots, x_n)\mathcal{R}(y_1, \ldots, y_n) \iff \Big((x_1 \leqslant y_1) \wedge \ldots \wedge (x_n \leqslant y_n)\Big) .$$

C'est bien une relation d'ordre, mais il n'est que partiel. On obtient un ordre total en donnant la précédence à la première coordonnée, puis à la seconde en cas d'égalité sur la première, etc...

$$\begin{aligned}(x_1, \ldots, x_n)\mathcal{R}(y_1, \ldots, y_n) \iff & \\ & \Big((x_1 < y_1) \vee ((x_1 = y_1) \wedge (x_2 < y_2)) \vee \ldots \vee \\ & ((x_1 = y_1) \wedge \ldots \wedge (x_{n-1} = y_{n-1}) \wedge (x_n < y_n)) \\ & ((x_1 = y_1) \wedge \ldots \wedge (x_n = y_n))\Big) .\end{aligned}$$

L'ordre est maintenant total. Compliqué ? Pas tellement : c'est l'ordre dans lequel les mots sont rangés dans un dictionnaire : on l'appelle *ordre lexicographique*.

1.7 Raisonnements

Il ne s'agit pas de proposer ici une théorie du raisonnement mathématique. Nous allons simplement donner quelques exemples de démonstrations, pour illustrer trois types de raisonnements : par contraposée, par l'absurde et par récurrence.

Raisonnement par contraposée
Il consiste, plutôt que de démontrer l'implication $A \Longrightarrow B$, à démontrer sa contraposée $(\neg B) \Longrightarrow (\neg A)$. Il est difficile de donner une règle générale d'utilisation de ce raisonnement. Un bon conseil avant de se lancer dans la démonstration d'une implication, est d'écrire d'abord sa contraposée. Avec un peu d'expérience, on arrive vite à sentir laquelle des deux est la plus facile à démontrer. Si le résultat désiré est B, on cherche les conséquences de $\neg B$ pour arriver aux bonnes hypothèses. Notre premier exemple est un résultat facile, mais très utile.

Proposition 9. *Soit x un nombre réel tel que pour tout $\varepsilon > 0$, $x \leqslant \varepsilon$. Alors $x \leqslant 0$.*

Démonstration : Nous devons démontrer l'implication :

$$\Big(\forall \varepsilon > 0\ , \quad x \leqslant \varepsilon\Big) \implies (x \leqslant 0)\ .$$

Ecrivons sa contraposée :

$$(x > 0) \implies \Big(\exists \varepsilon > 0\ ; \qquad x > \varepsilon\Big)\ .$$

« Si x est strictement positif, alors il existe $\varepsilon > 0$ tel que $x > \varepsilon$ ». C'est vrai : il suffit de choisir $\varepsilon = x/2$. □

Comme deuxième exemple, nous allons reprendre un des points de la démonstration du théorème 3.

Proposition 10. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Soient x et y deux éléments de E qui ne sont pas reliés. Alors l'intersection des deux classes d'équivalence de x et y est vide.*

Démonstration : L'implication que nous devons démontrer s'écrit formellement :

$$\neg(x \mathcal{R} y) \implies (\mathfrak{cl}_{\mathcal{R}}(x) \cap \mathfrak{cl}_{\mathcal{R}}(y) = \emptyset)\ .$$

Sa contraposée est :

$$(\mathfrak{cl}_{\mathcal{R}}(x) \cap \mathfrak{cl}_{\mathcal{R}}(y) \neq \emptyset) \implies (x \mathcal{R} y)\ .$$

Soit z un élément de $\mathfrak{cl}_{\mathcal{R}}(x) \cap \mathfrak{cl}_{\mathcal{R}}(y)$ (il y en a au moins un car l'intersection est non vide. Par définition des classes d'équivalence, x est relié à z, et z est relié à y. Par transitivité, x est relié à y. □

Raisonnement par l'absurde
Il consiste à démontrer une assertion en vérifiant que sa négation conduit à une contradiction avec les hypothèses. Dans certains cas il se distingue mal du raisonnement par contraposée : si A désigne la conjonction des hypothèses et B la conclusion, nier B et aboutir à une contradiction, revient à démontrer $\neg A$ à partir de $\neg B$, ce qui est la contraposée de $A \Longrightarrow B$.

Notre premier exemple est dû à Euclide.

Proposition 11. *Il existe une infinité de nombres premiers.*

Démonstration : Supposons qu'il n'en existe qu'un nombre fini, et soit N le plus grand d'entre eux. Considérons le nombre $P = N! + 1$. Il est strictement supérieur à N, donc il n'est pas premier, par définition de N. Si on effectue la division euclidienne de P par un nombre quelconque entre 2 et N, le reste est 1, par définition de la factorielle (produit de tous les entiers de 1 à N). Donc le nombre P n'est divisible par aucun nombre entre 2 et N donc par aucun nombre premier : il est donc premier, d'où la contradiction. □

Voici un autre résultat classique.

Proposition 12. *Le nombre $\sqrt{2}$ est irrationnel.*

Démonstration : Un nombre rationnel est le quotient de deux entiers ; un nombre irrationnel n'est pas rationnel. Nous devons donc démontrer que $\sqrt{2}$ n'est pas le quotient de deux entiers. Supposons le contraire : il existe deux entiers p et q tels que $\sqrt{2} = p/q$. Quitte à simplifier la fraction, nous pouvons supposer que p et q n'ont pas de facteur commun. Multiplions par q et élevons au carré :

$$2q^2 = p^2 \ .$$

Le nombre $p^2 = 2q^2$ est pair, donc p est également pair. Mais si p est pair, alors p^2 est multiple de 4. Donc q^2 est multiple de 2, donc q est pair. Mais alors 2 est un facteur commun à p et q, ce qui est une contradiction. □

Pour notre troisième exemple, nous revenons encore une fois sur :

Deux classes d'équivalence sont égales ou bien disjointes.

Comparez la démonstration qui suit avec celle du théorème 3 et de la proposition 10.

Démonstration : L'assertion A est l'hypothèse : $\mathcal{R}$ est une relation d'équivalence. L'assertion B est la conclusion, que l'on peut écrire de manière formelle comme suit.

$$\forall x, y \in E \ , \quad (\mathfrak{cl}_{\mathcal{R}}(x) = \mathfrak{cl}_{\mathcal{R}}(y)) \vee (\mathfrak{cl}_{\mathcal{R}}(x) \cap \mathfrak{cl}_{\mathcal{R}}(y) = \emptyset) \ .$$

La négation de B s'écrit :

$$\exists x, y \in E \ , \quad (\mathfrak{cl}_{\mathcal{R}}(x) \neq \mathfrak{cl}_{\mathcal{R}}(y)) \wedge (\mathfrak{cl}_{\mathcal{R}}(x) \cap \mathfrak{cl}_{\mathcal{R}}(y) \neq \emptyset) \ .$$

Soit encore : il existe deux éléments x et y tels que les classes $\mathfrak{cl}_{\mathcal{R}}(x)$ et $\mathfrak{cl}_{\mathcal{R}}(y)$ ne soient ni égales ni disjointes. Si c'est le cas, il existe un élément z qui est dans l'une et pas dans l'autre, et un élément t qui est dans les deux. Supposons que z soit dans $\mathfrak{cl}_{\mathcal{R}}(x)$, mais pas dans $\mathfrak{cl}_{\mathcal{R}}(y)$. Donc $x\mathcal{R}z$, donc $z\mathcal{R}x$, car $\mathcal{R}$ est symétrique. Mais aussi $x\mathcal{R}t$ et $t\mathcal{R}y$ car t appartient aux deux classes de x et y. Donc puisque $\mathcal{R}$ est transitive, $z\mathcal{R}y$. Donc z est dans la classe de y, ce qui est une contradiction. □

Raisonnement par récurrence

Pour démontrer qu'une assertion $H(n)$ dépendant d'un entier n est vraie pour tout $n \in \mathbb{N}$, on démontre :

1. $H(0)$ « initialisation »,
2. $\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+1)$ « hérédité ».

L'assertion $H(n)$ est *l'hypothèse de récurrence*. Il peut se faire qu'elle ne soit vraie que pour $n \geqslant 1$ ou $n \geqslant 2$, auquel cas, on la démontre pour la plus petite valeur pour laquelle elle est vraie. Voici la démonstration d'une formule à connaître :

Proposition 13. *Pour tout entier $n \geqslant 1$, la somme des entiers de 1 à n vaut $n(n+1)/2$.*

Démonstration : L'hypothèse de récurrence est :

$$H(n)\ :\qquad \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\ .$$

1. *Initialisation.* Pour $n = 1$:
$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}\ .$$
2. *Hérédité.* Soit n un entier quelconque. Supposons que $H(n)$ est vraie. Ecrivons :
$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + (n+1)\ .$$
En appliquant $H(n)$, on obtient
$$\left(\sum_{k=1}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)\ ,$$
Le membre de droite s'écrit
$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}\ ,$$
Nous avons donc démontré que
$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}\ ,$$
c'est-à-dire que $H(n+1)$ est vraie.

□

On peut être amené, pour démontrer $H(n+1)$ à utiliser $H(m)$ pour $m \in \{0, \ldots, n\}$, ce qui ne change rien au principe de la récurrence.

$$\forall n \in \mathbb{N}\,,\ \Big((\forall m \in \{0, \ldots, n\}\,, \quad H(m)\,) \implies H(n+1) \Big)\,.$$

Pour deviner quelle est la bonne hypothèse $H(n)$, on doit souvent essayer plusieurs valeurs successives de n : $n = 0$, puis $n = 1$, $n = 2$,... C'est parfaitement inutile pour la démonstration. Attention, ce n'est pas parce qu'une propriété est vraie pour quelques valeurs de n qu'elle est vraie pour tout n. Voici deux exemples.

1. Les nombres 31, 331, 3 331,..., 33 333 331 sont tous premiers. Mais $333\,333\,331 = 17 \times 19\,607\,843$ ne l'est pas.
2. Pour toutes les valeurs de n allant de 0 à 39, le nombre $n^2 + n + 41$ est premier. Mais le nombre $40^2 + 40 + 41 = 41^2$ ne l'est pas.

2 Entraînement

2.1 Vrai ou faux

Vrai-Faux 1. Parmi les assertions suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ $(2 < 3) \wedge (2 \,|\, 4)$.
2. ☐ $(2 < 3) \wedge (2 \,|\, 5)$.
3. ☒ $(2 < 3) \vee (2 \,|\, 5)$.
4. ☒ $(2 < 3) \wedge (\neg(2 \,|\, 5))$.
5. ☐ $(\neg(2 < 3)) \vee (2 \,|\, 5)$.
6. ☒ $\Big((2 < 3) \wedge (2 \,|\, 4)\Big) \vee (3 \,|\, 6)$.
7. ☒ $\Big((2 < 3) \wedge (2 \,|\, 4)\Big) \vee (3 \,|\, 5)$.
8. ☐ $\Big((2 < 3) \wedge (2 \,|\, 4)\Big) \wedge (3 \,|\, 5)$.
9. ☒ $\Big((2 < 3) \wedge (2 \,|\, 5)\Big) \vee \Big((3 \,|\, 6) \wedge (3 < 6)\Big)$.
10. ☐ $\Big((2 < 3) \wedge (2 \,|\, 5)\Big) \vee \Big((3 \,|\, 6) \wedge (3 > 6)\Big)$.

Vrai-Faux 2. Soit n un entier naturel quelconque. Parmi les implications suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ $(n \geqslant 5) \implies (n > 3)$.
2. ☐ $(n \geqslant 5) \implies (n > 6)$.
3. ☐ $(n \geqslant 5) \implies (n \leqslant 6)$.
4. ☒ $(n < 1) \implies (2 \,|\, n)$.
5. ☐ $(n < 1) \implies (n \,|\, 2)$.
6. ☒ $(n < 2) \implies (n^2 = n)$.
7. ☒ $(n > 0) \implies (2n > n)$.
8. ☐ $(n \geqslant 0) \implies (2n > n)$.
9. ☒ $(n \geqslant 0) \implies ((n + 1) > n)$.

Vrai-Faux 3. Soit n un entier naturel quelconque. Parmi les équivalences suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ $(n \geqslant 5) \iff (n > 4)$.
2. ☐ $(n \geqslant 5) \iff (n \geqslant 4)$.
3. ☐ $((n > 5) \wedge (n \,|\, 12)) \iff (n = 6)$.
4. ☒ $((n > 6) \wedge (n \,|\, 12)) \iff (n = 12)$.
5. ☒ $((3 \,|\, n) \wedge (4 \,|\, n)) \iff (12 \,|\, n)$.

6. ☐ $((3 \mid n) \wedge (4 \mid n)) \iff (n \mid 12)$.
7. ☐ $((n \mid 3) \vee (n \mid 4)) \iff (n \mid 12)$.

Vrai-Faux 4. Parmi les assertions suivantes, portant sur un entier naturel n, lesquelles sont des conditions suffisantes pour que n soit pair, lesquelles ne le sont pas et pourquoi ?

1. ☐ $n \leqslant 2$.
2. ☒ $(n \leqslant 2) \wedge (\neg(n = 1))$.
3. ☒ $12 \mid n$.
4. ☐ $n \mid 12$.
5. ☒ $(n \mid 12) \wedge (n > 3)$.
6. ☐ $(n \mid 12) \vee (n \mid 10)$.
7. ☐ $(n \mid 12) \wedge (n \mid 10)$.
8. ☒ $(n \mid 16) \wedge (n > 1)$.
9. ☒ $(n \mid 16) \wedge (\neg(n^2 = n))$.

Vrai-Faux 5. Soit n un entier quelconque. Parmi les phrases suivantes, lequelles traduisent correctement l'implication

$$(4 \mid n) \implies (2 \mid n)\ ,$$

lesquelles ne la traduisent pas et pourquoi ?

1. ☒ Si 4 divise n alors 2 divise n.
2. ☐ 2 divise n seulement si 4 divise n.
3. ☐ Pour que 2 divise n il faut que 4 divise n.
4. ☒ Pour que 2 divise n il suffit que 4 divise n.
5. ☒ la condition « 2 divise n » est nécessaire pour que 4 divise n.
6. ☐ la condition « 4 divise n » est nécessaire pour que 2 divise n.
7. ☒ la condition « 4 divise n » est suffisante pour que 2 divise n.

Vrai-Faux 6. Parmi les phrases suivantes, lesquelles traduisent correctement l'équivalence

$$((3 \mid n) \wedge (4 \mid n)) \iff (12 \mid n)\ ,$$

lesquelles ne la traduisent pas et pourquoi ?

1. ☒ Si 3 et 4 divisent n alors 12 divise n et réciproquement.
2. ☐ Pour que 12 divise n il faut que 3 et 4 divisent n.
3. ☒ Pour que 12 divise n il faut et il suffit que 3 et 4 divisent n.
4. ☒ Pour que 12 divise n il est nécessaire et suffisant que 3 et 4 divisent n.
5. ☐ 12 divise n seulement si 3 et 4 divisent n.

6. ☒ 12 divise n si et seulement si 3 et 4 divisent n.

Vrai-Faux 7. Si je mange, alors je bois et je ne parle pas. Si je ne parle pas alors je m'ennuie. Je ne m'ennuie pas. Je peux en déduire que (oui ou non et pourquoi) :

1. ☒ je parle.
2. ☐ je ne parle pas.
3. ☐ je ne bois pas.
4. ☒ je ne mange pas.
5. ☐ je ne bois pas et je ne mange pas.

Vrai-Faux 8. Parmi les assertions suivantes lesquelles sont vraies, lesquelles sont fausses, et pourquoi ?

1. ☒ Si Napoléon était chinois, alors $3 - 2 = 2$.
2. ☐ Soit Cléopâtre était chinoise, soit les grenouilles aboient.
3. ☒ Soit les roses sont des animaux, soit les chiens ont 4 pattes.
4. ☒ Si l'homme est un quadrupède, alors il aboie.
5. ☐ Les roses ne sont ni des animaux, ni des fleurs.
6. ☒ Paris est en France ou Madrid est en Chine.
7. ☒ La pierre ponce est un homme si et seulement si les femmes sont des sardines.
8. ☒ Les poiriers ne donnent pas des melons, et Cléopâtre n'était pas chinoise.
9. ☒ Il est faux que si les grenouilles n'aboient pas alors $3 \times 2 = 7$.
10. ☐ Si les champignons sont des animaux ou le Cid était espagnol, alors la longueur d'une circonférence est le double de son rayon.
11. ☒ Une condition nécessaire et suffisante pour que dans un jeu de 40 cartes il y ait 45 as est que le cuir soit végétal.

Vrai-Faux 9. Soient A, B, C trois sous-ensembles d'un ensemble E. L'ensemble $((A \cup B) \cap C) \cup ((A \cap B) \cap \complement C)$ est-il (oui ou non et pourquoi) ?

1. ☐ égal à E.
2. ☐ inclus dans $A \cap B$.
3. ☒ inclus dans $A \cup B$.
4. ☒ inclus dans $A \cup C$.
5. ☐ inclus dans $A \cap C$.
6. ☒ inclus dans $(A \cap C) \cup B$.
7. ☐ inclus dans $(A \cap \complement C) \cup B$.
8. ☒ égal à $(A \cap B) \cup (B \cap C) \cup (A \cap C)$.

Vrai-Faux 10. Parmi les ensembles d'entiers suivants, lesquels sont égaux au singleton $\{0\}$, lesquels sont différents et pourquoi ?

1. ☐ $\{\, n \in \mathbb{N} \,;\quad n \leqslant 1 \,\}$.
2. ☒ $\{\, n \in \mathbb{N} \,;\quad n < 1 \,\}$.
3. ☒ $\{\, n \in \mathbb{N} \,;\quad (n \leqslant 1) \wedge (2 \,|\, n) \,\}$.
4. ☐ $\{\, n \in \mathbb{N} \,;\quad 1 + n > 0 \,\}$.
5. ☒ $\{\, n \in \mathbb{N} \,;\quad 1 + n = 1 \,\}$.
6. ☒ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ n \leqslant m \,\}$.
7. ☐ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ n < m \,\}$.
8. ☐ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ n \,|\, m \,\}$.
9. ☒ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ m \,|\, n \,\}$.

Vrai-Faux 11. Un entier est un nombre premier s'il est non nul et divisible seulement par 1 et par lui-même. Parmi les ensembles suivants, lesquels sont égaux à l'ensemble des nombres premiers, lesquels sont différents et pourquoi ?

1. ☐ $\{\, n \in \mathbb{N} \,;\quad (n > 0) \wedge ((m \,|\, n) \Longrightarrow (m = n)) \,\}$.
2. ☒ $\{\, n \in \mathbb{N} \,;\quad (m \,|\, n) \Longrightarrow (m \in \{1, n\}) \,\}$.
3. ☐ $\{\, n \in \mathbb{N} \,;\quad (m \,|\, n) \Longrightarrow (1 \leqslant m \leqslant n) \,\}$.
4. ☐ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ ((m = 1) \vee (m = n)) \wedge (\neg(m \,|\, n)) \,\}$.
5. ☒ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ ((m = 1) \vee (m = n)) \vee (\neg(m \,|\, n)) \,\}$.
6. ☐ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ (1 < m < n) \Longrightarrow (\neg(m \,|\, n)) \,\}$.
7. ☒ $\{\, n \in \mathbb{N} \,;\quad \forall m \in \mathbb{N},\ (n > 0) \wedge ((1 < m < n) \Longrightarrow (\neg(m \,|\, n))) \,\}$.

Vrai-Faux 12. Soient E et F deux ensembles et f une application de E vers F. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si f est injective alors tout élément de E a plus d'une image dans F.
2. ☒ Si f est injective alors tout élément de F a au plus un antécédent dans E.
3. ☐ Si f est surjective alors tout élément de F a plus d'un antécédent dans F.
4. ☐ Si f n'est pas bijective alors au moins un élément de F n'a pas d'antécédent.
5. ☒ Si f n'est pas injective alors il existe deux éléments distincts de E ayant la même image.

Vrai-Faux 13. Soient E et F deux ensembles finis et f une application de E vers F. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si $\mathrm{Card}(E) > \mathrm{Card}(F)$ alors f est surjective.
2. ☒ Si $\mathrm{Card}(E) > \mathrm{Card}(F)$ alors f n'est pas injective.

3. ☐ Si $\mathrm{Card}(E) = \mathrm{Card}(F)$ alors f est bijective.
4. ☒ Si $\mathrm{Card}(E) = \mathrm{Card}(F)$ et si f est surjective, alors f est bijective.
5. ☐ Si $\mathrm{Card}(E) \neq \mathrm{Card}(F)$ alors f est injective ou surjective.
6. ☒ Si $\mathrm{Card}(E) = \mathrm{Card}(F)$ et si f n'est pas surjective, alors f n'est pas injective.
7. ☒ Si $\mathrm{Card}(E) = \mathrm{Card}(F)$ et si f n'est pas injective, alors f n'est pas surjective.

Vrai-Faux 14. Soit $E = \{0, 1, 2\}$. Les graphes suivants définissent-ils une relation d'équivalence sur E (oui ou non et pourquoi) ?

1. ☐ $\Gamma = \{\,(0,0), (0,1), (1,0), (1,1)\,\}$.
2. ☒ $\Gamma = \{\,(0,0), (0,1), (1,0), (1,1), (2,2)\,\}$.
3. ☐ $\Gamma = \{\,(0,0), (0,1), (1,0), (1,1), (1,2), (2,2)\,\}$.
4. ☐ $\Gamma = \{\,(0,0), (0,1), (1,0), (1,1), (1,2), (2,1), (2,2)\,\}$.
5. ☒ $\Gamma = \{\,(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\,\}$.

Vrai-Faux 15. Soit $E = \{0, 1, 2\}$. Les graphes suivants définissent-ils une relation d'ordre sur E (oui ou non et pourquoi) ?

1. ☒ $\Gamma = \{\,(0,0), (0,1), (1,1), (2,2)\,\}$.
2. ☐ $\Gamma = \{\,(0,0), (0,1), (1,0), (1,1), (2,2)\,\}$.
3. ☒ $\Gamma = \{\,(0,0), (0,1), (0,2), (1,1), (2,2)\,\}$.
4. ☐ $\Gamma = \{\,(0,0), (0,1), (1,1), (1,2), (2,2)\,\}$.
5. ☒ $\Gamma = \{\,(0,0), (0,1), (0,2), (1,1), (1,2), (2,2)\,\}$.

Vrai-Faux 16. Soient E un ensemble fini non vide et x un élément fixé de E. Les relations $\mathcal{R}$ définies par les assertions suivantes sont-elles des relations d'équivalence sur $\mathcal{P}(E)$ (oui ou non et pourquoi) ?

1. ☒ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff A = B.$
2. ☐ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff A \subset B.$
3. ☐ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff (A \cap B = \emptyset).$
4. ☒ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((A \cap B = \emptyset) \vee (A \cup B \neq \emptyset)\Big).$
5. ☐ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff (x \in A \cup B).$
6. ☒ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((x \in A \cap B) \vee (x \in {}^cA \cap {}^cB)\Big).$

Vrai-Faux 17. Soient E un ensemble fini contenant au moins deux éléments, et x un élément fixé de E. Les relations $\mathcal{R}$ définies par les assertions suivantes sont-elles des relations d'ordre sur $\mathcal{P}(E)$ (oui ou non et pourquoi) ?

1. ☒ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff A = B.$
2. ☒ $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff A \subset B.$

3. $\square\ \forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff (x \in (A \cap {}^cB))$.
4. $\square\ \forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff (x \in (A \cup {}^cB))$.
5. $\boxtimes\ \forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((A = B) \vee (x \in A \cap {}^cB)\Big)$.

Vrai-Faux 18. Soit $H(n)$ un énoncé dépendant de l'entier n. Les assertions suivantes entraînent-elles que $H(n)$ est vraie pour tout $n \in \mathbb{N}$ (oui ou non et pourquoi) ?

1. $\boxtimes\ H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+1)\Big)$.
2. $\square\ H(1) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+1)\Big)$.
3. $\square\ H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
4. $\square\ H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+2)\Big)$.
5. $\boxtimes\ H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+2)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
6. $\square\ H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
7. $\boxtimes\ (H(0) \wedge H(1)) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.

2.2 Exercices

Exercice 1. Soient A, B, C trois assertions. Pour chacune des assertions suivantes :

$$\begin{array}{cc}
\Big(A \wedge (\neg B)\Big) & \Big(A \vee (\neg B)\Big) \\
\Big(A \vee (B \wedge C)\Big) & \Big(A \wedge (B \vee C)\Big) \\
\Big(A \Longrightarrow (\neg B)\Big) & \Big(A \Longleftrightarrow B\Big) \\
\Big((\neg(A \vee B)) \Longrightarrow C\Big) & \Big((A \wedge B) \Longleftrightarrow (\neg C)\Big) \\
\Big((A \wedge (\neg B)) \Longrightarrow C\Big) & \Big(A \vee (\neg B) \Longrightarrow (\neg C)\Big)
\end{array}$$

1. Ecrire sa négation.
2. Traduire l'assertion et sa négation en langage courant, en remplaçant A par « je mange », B par « je bois » et C par « je fume ».

Exercice 2. Soient A, B et C trois assertions. Démontrer que les équivalences suivantes sont toujours vraies, d'abord à l'aide des tables de vérité, ensuite en utilisant le théorème 1. Traduire chacune des assertions en langage courant, en remplaçant A par « je mange », B par « je bois » et C par « je fume ».

1. $\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \iff \Big((A \wedge B) \Longrightarrow C\Big)$.
2. $\Big((A \vee B) \Longrightarrow C\Big) \iff \Big((A \Longrightarrow C) \wedge (B \Longrightarrow C)\Big)$.
3. $\Big((A \wedge B) \Longrightarrow C\Big) \iff \Big((A \Longrightarrow C) \vee (B \Longrightarrow C)\Big)$.
4. $\Big(A \Longrightarrow (B \wedge C)\Big) \iff \Big((A \Longrightarrow B) \wedge (A \Longrightarrow C)\Big)$.
5. $\Big(A \Longrightarrow (B \vee C)\Big) \iff \Big((A \Longrightarrow B) \vee (A \Longrightarrow C)\Big)$.

Exercice 3. On considère les quatre assertions suivantes :
- F : je fume,
- B : je bois,
- J : je mange du jambon,
- M : j'ai des moustaches.

Exprimer sous forme symbolique les phrases suivantes :

1. Je fume et je bois, mais je n'ai pas de moustache.
2. Quand je fume, je ne bois pas.
3. Chaque fois que je mange du jambon, je ne fume pas mais je bois.
4. Si je mange du jambon ou si je bois, alors je ne fume pas.
5. Il suffit que j'aie des moustaches pour que je mange du jambon.
6. Il faut que je mange du jambon et que je boive pour que je fume.
7. Une condition nécessaire pour que je boive et que je fume est que je mange du jambon.
8. Je fume et je bois, si et seulement si je mange du jambon ou j'ai des moustaches.
9. De deux choses l'une : soit je bois et je mange du jambon, soit si j'ai une moustache alors je ne fume pas.

En supposant que les valeurs de vérité respectives de F, B, J, M sont V, V, F, V, trouver les valeurs de vérité des phrases précédentes.

Exercice 4. Exprimer sous forme symbolique les raisonnements suivants et vérifier qu'ils sont corrects.

1. Si je vais à Londres, j'irai aussi à Oxford. Soit je vais à Londres, soit je dépense mon argent à autre chose. Si je vais à Oxford, je verrai John. Si je dépense mon argent à autre chose, je verrai John. Donc je verrai John.
2. Si j'ai de l'argent ou si je bois du vin alors je chante en me rasant et je suis content. Donc je n'ai pas d'argent ou bien je chante en me rasant.
3. Soit je mange, soit je bois, et si je mange je ne fume pas. Comme je ne bois pas, je ne fume pas.

4. Si Pierre est marié, alors Jean est marié, et si Jean est marié, alors Louis l'est aussi. De plus, soit Jean est célibataire, soit il est marié et Louis est célibataire. Donc Pierre est célibataire.
5. Si on ne danse pas, je m'asseois. Si je m'asseois, je bois et je fume. Si on danse je m'amuse. Or je m'ennuie. Donc je fume.
6. Si je ne m'asseois pas, je bois. Si je bois, on danse et de plus je fume. Si je m'asseois, je m'amuse. Or je m'ennuie. Donc je fume.
7. Si je marche, je sue. Si je ne me fatigue pas, je ne sue pas. Or je ne me fatigue pas. Donc je ne marche pas.
8. Si A dit la vérité, B ment. Si B ment, C ment. Si C ment, D dit la vérité. D ment ou bien E ment. A ne ment pas. Donc E ment.

Exercice 5. Trois commerçants habitent dans 3 maisons situées aux numéros 21, 23 et 25 de la même rue. Le boucher habite dans la maison jaune, qui est à côté de la rouge mais qui n'est pas à côté de la verte. L'épicier, qui n'est pas suisse, habite à côté du Français. L'Italien habite au numéro 21 et sa maison n'est pas jaune. Quelle est la nationalité du pharmacien, quelle est la couleur de sa maison, et où habite-t-il ?

Exercice 6. Trois personnes, un policier un berger et un assassin, habitent dans 3 maisons situées aux numéros 19, 21 et 23 de la même rue. Le policier habite au numéro 23 et sa maison n'est pas rouge. La maison rouge est à côté de la maison bleue mais pas à côté de la maison jaune. L'Italien habite dans la maison rouge. Le Français, qui n'est pas berger, habite à côté de l'assassin. Quelle est la couleur de la maison de l'assassin et où habite-t-il ?

Exercice 7. (Pour les courageux).

- Alice dit que si Bernard est coupable, Charles l'est aussi.
- Bernard dit que Alice est coupable et que Charles ne l'est pas.
- Charles dit qu'il n'est pas coupable mais que au moins l'un des deux autres l'est.

Soit A (respectivement B, C) l'assertion « Alice (respectivement : Bernard, Charles) est coupable ».

1. Ecrire sous forme logique les affirmations de Alice, Bernard et Charles.
2. On sait que chacune des trois personnes ment si et seulement si elle est coupable. Déduire de la question précédente trois assertions vraies. Simplifier leur expression.
3. Contruire la table de vérité de chacune des trois assertions de la question précédente.
4. Déduire de ces tables de vérité que Alice est innocente, Bernard et Charles sont coupables.

Exercice 8. Définir les ensembles suivants en extension.

1. $\{\, n \in \mathbb{N}\,; \quad (n > 3) \wedge (n \leqslant 7)\,\}$.
2. $\{\, n \in \mathbb{N}\,; \quad (2 \mid n) \wedge (n \leqslant 7)\,\}$.
3. $\{\, n \in \mathbb{N}\,; \quad (n \mid 12) \vee (n \geqslant 7)\,\}$.
4. $\{\, n \in \mathbb{N}\,; \quad (\neg(n \mid 12)) \wedge (n \leqslant 7)\,\}$.
5. $\{\, n \in \mathbb{N}\,; \quad (n > 3) \wedge ((n \mid 12) \vee (n \leqslant 7))\,\}$.

Exercice 9. Soient A, B et C trois sous-ensembles d'un ensemble E. Ecrire en fonction de A, B, C les ensembles correspondant aux assertions suivantes.

1. x appartient aux trois.
2. x appartient au moins à l'un d'entre eux.
3. x appartient à deux d'entre eux au plus.
4. x appartient à l'un d'entre eux exactement.
5. x appartient à deux d'entre eux au moins.
6. x appartient à l'un d'entre eux au plus.

Exercice 10. Soit E un ensemble. Soient A et B deux sous-ensembles de E. On appelle :

- différence de B dans A et on note $A \setminus B$ l'ensemble $A \cap {}^cB$,
- différence symétrique de A et B et on note $A\Delta B$ l'ensemble $(A \setminus B) \cup (B \setminus A)$.

1. Ecrire sous forme logique les propriétés « $x \in A \setminus B$ » et « $x \in A\Delta B$ » à l'aide des propriétés « $x \in A$ » et « $x \in B$ ». Démontrer les égalités ensemblistes suivantes.
2. $A \setminus \emptyset = A\Delta\emptyset = A$.
3. $A \setminus A = A\Delta A = \emptyset$.
4. $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.
5. $(A\Delta B) \cup (A\Delta C) = (A \cup B \cup C) \setminus (A \cap B \cap C)$.
6. Donner une représentation sous forme de diagramme de Venn de tous les ensembles définis dans cet exercice.

Exercice 11. Soient A, B et C trois sous-ensembles d'un ensemble E.

1. Simplifier l'expression $(A \cap B \cap C) \cup ({}^cA \cap B \cap C) \cup {}^cB \cup \mathcal{C}$.
2. Démontrer que $(A \cap {}^cB) \cap \mathcal{C} = A \cap {}^c(B \cup C) = (A \cap \mathcal{C}) \cap {}^cB$.
3. Démontrer que $(A \cup B \subset \mathcal{C}) \wedge (A \cup C \subset B) \Longleftrightarrow (A \subset B) \wedge (C = \emptyset)$.

Exercice 12. (D'après Lewis Caroll). Parmi les combattants d'une grande bataille, au moins 70% ont perdu un œil, au moins 75% une oreille, au moins 80% un bras, et au moins 85% une jambe. Quelle est la proportion minimale des combattants qui ont perdu les 4 ?

Exercice 13. Un centre de langue propose des cours d'Albanais, de Bantou et de Chinois. Sur 93 élèves, 54 étudient l'Albanais, 51 le Bantou ou le Chinois, 27 le Chinois mais pas le Bantou, 3 ni l'Albanais ni le Chinois, et 12 étudient les 3 langues.

1. Combien d'élèves étudient à la fois le Bantou et le Chinois ?
2. Combien d'élèves étudient l'Albanais ou le Bantou mais pas le Chinois ?
3. Combien d'élèves n'étudient ni le Bantou ni le Chinois ?
4. Combien d'élèves étudient une seule langue ?
5. Combien d'élèves étudient exactement deux langues ?

Exercice 14. Pour chacune des assertions suivantes :

- $\forall n \in \mathbb{N}\,,\ \exists m \in \mathbb{N}\ ;\quad (m \,|\, n)$,
- $\exists n \in \mathbb{N}\ ;\quad \forall m \in \mathbb{N}\,,\ (m \,|\, n)$,
- $\exists n \in \mathbb{N}\ ;\quad \forall m \in \mathbb{N}\,,\ (n \,|\, m)$,
- $\forall n \in \mathbb{N}\,,\ \forall m \in \mathbb{N}\,,\ \Big((m \,|\, n) \vee (n \,|\, m)\Big)$,
- $\forall n \in \mathbb{N}\,,\ \forall m \in \mathbb{N}\,,\ \Big(((m \,|\, n) \wedge (n \,|\, m)) \Longrightarrow (m = n)\Big)$,
- $\forall n \in \mathbb{N}\,,\ \forall m \in \mathbb{N}\,,\ \exists k \in \mathbb{N}\ ;\quad \Big((n \,|\, k) \wedge (m \,|\, k)\Big)$.

1. Lire à haute voix et comprendre.
2. Dire si l'assertion est vraie ou fausse et le démontrer.
3. Ecrire la négation, lire à haute voix et comprendre.

Exercice 15. On note $\mathbb{N}$ l'ensemble des entiers naturels, A l'ensemble des nombres pairs, et B l'ensemble des nombres premiers. Exprimer sous forme symbolique les phrases suivantes.

1. Tout nombre pair est divisible par 2.
2. Aucun nombre impair n'est divisible par 2.
3. Il n'existe pas de nombre premier pair distinct de 2.
4. Tout nombre premier distinct de 2 est impair.
5. Il existe un nombre pair qui divise tout nombre pair.
6. Tout nombre premier divise au moins un nombre pair

Exercice 16. On note $\mathbb{N}$ l'ensemble des entiers naturels, A l'ensemble des nombres pairs, et B l'ensemble des nombres premiers. Ecrire en langage courant et comprendre la signification des expressions logiques suivantes.

1. $\exists n \in A\ ;\quad n \in B$.
2. $\forall n \in A\,,\ \exists m \in B\ ;\quad m \,|\, n$.
3. $\forall n \in \mathbb{N}\,,\ n \in A \Longrightarrow \Big((n \notin B) \vee (n = 2)\Big)$.
4. $\forall n \in A\,,\ \Big((n = 2) \vee \Big(\exists (m,p) \in A \times B\ ;\quad n = mp\Big)\Big)$.
5. $\exists n \in \mathbb{N}\ ;\quad \forall (m,p) \in A \times B\,,\ (n \neq m) \wedge (n \neq p)$.

6. $\forall n \in \mathbb{N}\,,\ \Big(\exists m \in A\ ;\quad m \,|\, n\Big) \implies (n \in A)$.
7. $\forall n \in \mathbb{N}\,,\ (n \in A) \vee \Big(\exists m \in A\ ;\quad m+1 = n\Big)$.

Exercice 17. Représenter sur un diagramme de Venn les ensembles suivants.

- Ensemble Q des quadrilatères.
- Ensemble T des trapèzes.
- Ensemble P des parallélogrammes.
- Ensemble R des rectangles.
- Ensemble L des losanges.
- Ensemble C des carrés.

Exprimer sous forme logique, puis ensembliste, les phrases suivantes.

1. Tout carré est un rectangle.
2. Tout rectangle qui est aussi un losange est un carré.
3. Il existe des parallélogrammes qui ne sont pas des rectangles.
4. Si un losange est un rectangle alors c'est un carré.
5. Une condition nécessaire pour qu'un trapèze soit un carré est que ce soit un rectangle.
6. Pour qu'un trapèze soit un rectangle il suffit que ce soit un carré.
7. Il existe des quadrilatères qui ne sont ni des rectangles, ni des losanges.
8. Il existe des parallélogrammes qui ne sont ni des rectangles, ni des losanges.

Exercice 18. Si n est un entier, on note « n modulo 5 » le reste de la division euclidienne de n par 5. Les applications suivantes sont définies sur $\{0,1,2,3,4\}$, à valeurs dans lui-même. Représentez-les sur un diagramme. Sont-elles injectives ? surjectives ? bijectives ? Représentez le diagramme de $f \circ f$.

1. $f\ :\ n \mapsto n+1$ modulo 5.
2. $f\ :\ n \mapsto n+3$ modulo 5.
3. $f\ :\ n \mapsto n+10$ modulo 5.
4. $f\ :\ n \mapsto 2n$ modulo 5.
5. $f\ :\ n \mapsto 3n$ modulo 5.
6. $f\ :\ n \mapsto 10n$ modulo 5.

Exercice 19. Si n est un entier, on note « n modulo 6 » le reste de la division euclidienne de n par 6. Les applications f suivantes sont définies sur $\{0,1,2,3,4,5\}$, à valeurs dans lui-même. Représentez-les sur un diagramme. Sont-elles injectives ? surjectives ? bijectives ? Représentez le diagramme de $f \circ f$.

1. $f\ :\ n \mapsto n+1$ modulo 6.
2. $f\ :\ n \mapsto n+3$ modulo 6.

3. $f \ : \ n \mapsto n+10$ modulo 6.
4. $f \ : \ n \mapsto 2n$ modulo 6.
5. $f \ : \ n \mapsto 3n$ modulo 6.
6. $f \ : \ n \mapsto 10n$ modulo 6.

Exercice 20. On considère les applications suivantes, de $\mathbb{N}$ vers $\mathbb{N}$. Sont-elles injectives ? surjectives ? bijectives ?

1. $f \ : \ n \mapsto n+1$.
2. $f \ : \ n \mapsto 2n$.
3. $f \ : \ n \mapsto n^2$.
4. $f \ : \ n \mapsto \begin{cases} n+1 & \text{si } n \text{ est pair} \\ 2n & \text{si } n \text{ est impair.} \end{cases}$
5. $f \ : \ n \mapsto \begin{cases} 2n & \text{si } n \text{ est pair} \\ n-1 & \text{si } n \text{ est impair.} \end{cases}$
6. $f \ : \ n \mapsto \begin{cases} n+1 & \text{si } n \text{ est pair} \\ n-1 & \text{si } n \text{ est impair.} \end{cases}$
7. $f \ : \ n \mapsto \begin{cases} n/2 & \text{si } n \text{ est pair} \\ (n-1)/2 & \text{si } n \text{ est impair.} \end{cases}$

Exercice 21. On considère les applications suivantes, de $\mathbb{R}$ vers $\mathbb{R}$. Sont-elles injectives ? surjectives ? bijectives ?

1. $f \ : \ x \mapsto x+1$.
2. $f \ : \ x \mapsto 2x$.
3. $f \ : \ x \mapsto x^2$.
4. $f \ : \ x \mapsto x^3$.
5. $f \ : \ x \mapsto \sqrt{|x|}$.
6. $f \ : \ x \mapsto \frac{x}{\sqrt{|x|}}$ si $x \neq 0$, $f(0) = 0$.
7. $f \ : \ x \mapsto \mathrm{e}^x$.
8. $f \ : \ x \mapsto x^3 - 3x$.

Exercice 22. Soit E un ensemble et A un sous-ensemble de E. On appelle « fonction indicatrice de A » et on note $\mathbb{I}_A$ l'application de E vers $\{0,1\}$ qui à $x \in E$ associe 1 si $x \in A$, 0 si $x \notin A$. Soient A et B deux sous-ensembles de E. Démontrer les assertions suivantes.

1. $\forall x \in E \, , \ \mathbb{I}_{\complement A}(x) = 1 - \mathbb{I}_A(x)$.
2. $\forall x \in E \, , \ \mathbb{I}_{A \cap B}(x) = \min\{\mathbb{I}_A(x), \mathbb{I}_B(x)\} = \mathbb{I}_A(x)\, \mathbb{I}_B(x)$.
3. $\forall x \in E \, , \ \mathbb{I}_{A \cup B}(x) = \max\{\mathbb{I}_A(x), \mathbb{I}_B(x)\} = \mathbb{I}_A(x) + \mathbb{I}_B(x) - \mathbb{I}_A(x)\, \mathbb{I}_B(x)$.

Exercice 23. Soient E et F deux ensembles, f une application de E vers F. Soient A et A' deux sous-ensembles de E. Soient B et B' deux sous-ensembles de F. Démontrer les assertions suivantes.

1. $(A \subset A') \implies (f(A) \subset f(A'))$.
2. $(B \subset B') \implies (f^{-1}(B) \subset f^{-1}(B'))$.
3. $f(A \cup A') = (f(A) \cup f(A'))$.
4. $f^{-1}(B \cup B') = (f^{-1}(B) \cup f^{-1}(B'))$.
5. $f(A \cap A') \subset (f(A) \cap f(A'))$.
6. $f^{-1}(B \cap B') = (f^{-1}(B) \cap f^{-1}(B'))$.
7. $f^{-1}(f(A)) \supset A$.
8. $f(f^{-1}(B)) \subset B$.
9. $f(A \cap f^{-1}(B)) = (f(A) \cap B)$.
10. $f(A \cup f^{-1}(B)) \subset (f(A) \cup B)$.

Exercice 24. Ecrire chacune des assertions suivantes comme une implication.
Ecrire et démontrer sa contraposée.

1. Aucun nombre impair n'est la somme de deux nombres impairs.
2. Tout nombre premier strictement supérieur à 2 est impair.
3. Soient m et n deux entiers impairs tels que m divise $2n$. Alors m divise n.
4. Soient m et n deux entiers tels que m divise n. Alors m et $n+1$ sont premiers entre eux (ils n'ont aucun diviseur commun autre que 1).
5. Si le produit de deux entiers strictement supérieurs à 1 est le carré d'un entier alors chacun des deux est le carré d'un entier ou bien ils ont un diviseur commun autre que 1.

Exercice 25. Démontrer par récurrence les assertions suivantes.

1. $\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n}(k+1) = (n+1)(n+2)/2.$
2. $\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n} k^2 = n(n+1)(2n+1)/6.$
3. $\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n} k^3 = n^2(n+1)^2/4.$
4. $\forall n \in \mathbb{N}\ , \quad 3|(n^3 - n).$
5. $\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n} 2^k = 2^{n+1} - 1.$
6. $\forall n \in \mathbb{N}\ , \quad \sum_{k=0}^{n} k2^k = (n-1)2^{n+1} + 2.$

Exercice 26. Soient E un ensemble fini non vide et x un élément fixé de E. On considère les relations $\mathcal{R}$ définies par les assertions suivantes.

- $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff A = B.$
- $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((A \cap B = \emptyset) \vee (A \cup B \neq \emptyset)\Big).$
- $\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((x \in A \cap B) \vee (x \in {}^cA \cap {}^cB)\Big).$

Pour chacune de ces relations.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathcal{P}(E)$.
2. Décrire l'ensemble quotient $\mathcal{P}(E)/\mathcal{R}$.

Exercice 27. Soit E un ensemble non vide et x un élément fixé de E. On définit la relation $\mathcal{R}$ sur l'ensemble $\mathcal{P}(E)$ des parties de E par :

$$\forall A, B \in \mathcal{P}(E)\ , \quad A\mathcal{R}B \iff \Big((x \in A \cap B) \vee (x \in {}^cA \cap {}^cB)\Big)\ .$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Montrer que la classe d'équivalence de $\emptyset$ est $\mathcal{P}(E \setminus \{x\})$ (ensemble des parties du complémentaire de $\{x\}$ dans E).
3. Montrer que l'ensemble quotient $\mathcal{P}(E)/\mathcal{R}$ a deux éléments :
$$\mathcal{P}(E)/\mathcal{R} = \{\mathfrak{cl}_{\mathcal{R}}(\emptyset), \mathfrak{cl}_{\mathcal{R}}(\{x\})\}\ .$$
4. On définit l'application f_x, de $\mathcal{P}(E)$ vers $\mathcal{P}(E)$, qui à un sous-ensemble A associe $A \cup \{x\}$. L'application f est-elle injective ? surjective ?
5. Vérifier que l'image par f_x d'un élément de $\mathfrak{cl}_{\mathcal{R}}(\emptyset)$ appartient à $\mathfrak{cl}_{\mathcal{R}}(\{x\})$.
6. Montrer que tout élément de $\mathfrak{cl}_{\mathcal{R}}(\{x\})$ a un antécédent et un seul dans $\mathfrak{cl}_{\mathcal{R}}(\emptyset)$.
7. En déduire que :
$$\mathrm{Card}(\mathfrak{cl}_{\mathcal{R}}(\emptyset)) = \mathrm{Card}(\mathfrak{cl}_{\mathcal{R}}(\{x\}))$$
8. Déduire des questions précédentes que :
$$\mathrm{Card}(\mathcal{P}(E)) = 2\mathrm{Card}(\mathcal{P}(E \setminus \{x\}))\ .$$
9. Démontrer par récurrence que le cardinal de l'ensemble des parties d'un ensemble à n éléments est 2^n.

2.3 QCM

Donnez-vous une heure pour répondre à ce questionnaire. Les 10 questions sont indépendantes. Pour chaque question 5 affirmations sont proposées, parmi lesquelles 2 sont vraies et 3 sont fausses. Pour chaque question, cochez les 2 affirmations que vous pensez vraies. Chaque question pour laquelle les 2 affirmations vraies sont cochées rapporte 2 points.

Question 1.

A $\Big((4<2)\wedge(2\,|\,4)\Big)\wedge\Big((4\,|\,8)\wedge(4<8)\Big)$.

B $\Big((4<2)\vee(2\,|\,4)\Big)\wedge\Big((4\,|\,8)\wedge(8<4)\Big)$.

C $\Big((4<2)\wedge(2\,|\,4)\Big)\vee\Big((4\,|\,8)\wedge(4<8)\Big)$.

D $\Big((4<2)\vee(2\,|\,4)\Big)\wedge\Big((4\,|\,8)\vee(4<8)\Big)$.

E $\Big((8<2)\wedge(2\,|\,8)\Big)\vee\Big((2\,|\,4)\wedge(4<2)\Big)$.

Question 2. Soit n un entier naturel quelconque.

A $(n^2=n)\Longrightarrow(n<2)$.

B $(n^2=16)\Longrightarrow(2|n)$.

C $(n\leqslant 2)\Longrightarrow(2n>n)$.

D $(n^2\leqslant n)\Longrightarrow(2n>n)$.

E $(2|n)\Longrightarrow(2<n)$.

Question 3. Soit n un entier quelconque. L'implication $(6\,|\,n)\implies(3\,|\,n)$, peut se traduire par :

A Pour que n soit multiple de 3, il faut que n soit multiple de 6.

B Pour que n soit multiple de 3, il suffit que n soit multiple de 6.

C L'entier n est multiple de 3, seulement s'il est multiple de 6.

D Une condition nécessaire pour que n soit multiple de 6 est que n soit multiple de 3.

E Une condition suffisante pour que n soit multiple de 6 est que n soit multiple de 3.

Question 4. Si je mange, alors je bois. Si je bois, alors je ne parle pas et je suis content. Je ne suis pas content. Vous pouvez en déduire que :

A je ne mange pas.

B je parle.

C je ne parle pas et je ne mange pas.

D je mange.

E je ne bois pas.

Question 5. Soient A, B, C trois sous-ensembles quelconques d'un ensemble E. L'ensemble $\Big((A\cup{}^cB)\cap\mathcal{C}\Big)\cup\Big(({}^cA\cup\mathcal{C})\cap B\Big)$ est :

A inclus dans $\mathcal{C}\cup B$.

B égal à E.

C disjoint de B.

D égal à $\mathcal{C}\cup({}^cA\cap B)$.

E inclus dans $A\cup B$.

Question 6. L' ensemble A est égal au singleton $\{1\}$.

A $A = \{\, n \in \mathbb{N},\ (n^2 = n)\,\}$.
B $A = \{\, n \in \mathbb{N},\ (\forall m > n,\ n|m)\,\}$.
C $A = \{\, n \in \mathbb{N},\ (n|3)\,\}$.
D $A = \{\, n \in \mathbb{N},\ (n|2) \vee (n|3)\,\}$.
E $A = \{\, n \in \mathbb{N},\ (n|2) \wedge (n|3)\,\}$.

Question 7.
A $\forall n \in \mathbb{N},\ \exists m \in \mathbb{N}\,;\quad m \leqslant n$.
B $\forall n \in \mathbb{N},\ \forall m \in \mathbb{N}\,;\quad m \leqslant n$.
C $\exists n \in \mathbb{N},\ \forall m \in \mathbb{N}\,;\quad n \leqslant m$.
D $\exists n \in \mathbb{N},\ \forall m \in \mathbb{N}\,;\quad m \leqslant n$.
E $\exists n \in \mathbb{N},\ \exists m \in \mathbb{N}\,;\quad n + m + 1 = 0$.

Question 8. Soit $E = \{1, 2, 3, 4\}$. On note f l'application de E dans E dont le graphe Γ est le suivant.

$$\Gamma = \{\, (1, 2)\,,\ (2, 3)\,,\ (3, 3)\,,\ (4, 1)\,\}\ .$$

A L'application f est surjective.
B $f(\{2, 3\})$ est un singleton.
C $f^{-1}(\{2, 3\})$ est un singleton.
D L'image réciproque par f de tout singleton est non vide.
E 4 n'a pas d'antécédent pour f.

Question 9. La relation $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{N}$.
A $\forall n, m \in \mathbb{N},\quad n\mathcal{R}m \iff n|m$.
B $\forall n, m \in \mathbb{N},\quad n\mathcal{R}m \iff n^2 = m^2$.
C $\forall n, m \in \mathbb{N},\quad n\mathcal{R}m \iff n^2 + m^2 = -2nm$.
D $\forall n, m \in \mathbb{N},\quad n\mathcal{R}m \iff n^2 - m^2 = 2nm + 2n$.
E $\forall n, m \in \mathbb{N},\quad n\mathcal{R}m \iff n^2 + m^2 = 2nm$.

Question 10. Soit $H(n)$ un énoncé dépendant de l'entier n. L'assertion entraîne que $H(n)$ est vraie pour tout $n \geqslant 1$.
A $H(1) \wedge \Big(\forall n \geqslant 1,\ H(n) \Longrightarrow H(n+1)\Big)$.
B $H(1) \wedge \Big(\forall n \geqslant 1,\ H(n) \Longrightarrow H(n+2)\Big)$.
C $H(1) \wedge \Big(\forall n \geqslant 2,\ H(n) \Longrightarrow H(n+1)\Big)$.
D $H(1) \wedge \Big(\forall n \geqslant 1,\ H(n+1) \Longrightarrow H(n)\Big)$.
E $H(1) \wedge \Big(\forall n \geqslant 1,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \geqslant 4,\ H(n) \Longrightarrow H(n-1)\Big)$.

Réponses : 1–CD 2–AB 3–BD 4–AE 5–AD 6–BE 7–AC 8–BE 9–BE 10–AE

2.4 Devoir

Essayez de bien rédiger vos réponses, sans vous reporter ni au cours, ni au corrigé. Si vous souhaitez vous évaluer, donnez-vous deux heures ; puis comparez vos réponses avec le corrigé et comptez un point pour chaque question à laquelle vous aurez correctement répondu.

Questions de cours : Soient E et F deux ensembles. Soit f une application de E dans F. Soit A un sous-ensemble de E et B un sous-ensemble de F.

1. Définir l'image $f(A)$ de A et l'image réciproque $f^{-1}(B)$ de B.
2. Démontrer que $A \subset f^{-1}(f(A))$ et que $f(f^{-1}(B)) \subset B$.
3. Quand dit-on que f est injective ? surjective ?
4. Démontrer que si f est injective, alors $A = f^{-1}(f(A))$. Démontrer que si f est surjective, alors $B = f(f^{-1}(B))$.
5. Soit $E = F = \{-1, 0, 1\}$ et soit f l'application de E dans F qui à x associe x^2. L'application f est-elle injective ? surjective ? Soit $A = \{1\}$ et $B = \{-1, 1\}$. Ecrire en extension les ensembles $f^{-1}(f(A))$ et $f(f^{-1}(B))$.

Exercice 1 : Soient A, B et C trois assertions.

1. Ecrire la table de vérité de l'assertion :
$$(A \vee B) \implies (A \vee C) \, .$$
2. Ecrire la table de vérité de l'assertion :
$$(A \wedge B) \implies (A \wedge C) \, .$$
3. Utiliser les tables de vérité des deux questions précédentes pour démontrer que l'équivalence suivante est toujours vraie.
$$\Big(\big((A \vee B) \implies (A \vee C) \big) \wedge (A \wedge B) \implies (A \wedge C) \big) \Big) \iff \big(B \implies C \big) \, .$$
4. En utilisant les assertions A : « je suis une fille », B : « je fais du sport » et C : « je garde la forme », exprimer en langage courant l'équivalence de la question précédente.
5. Soit $\mathbf{E}$ un ensemble, $\mathbf{A}, \mathbf{B}, \mathbf{C}$ trois sous-ensembles de E. Représenter dans trois diagrammes de Venn différents les ensembles $\mathbf{E}, \mathbf{A}, \mathbf{B}, \mathbf{C}$, dans les trois cas suivants.
   - $\mathbf{B} \subset \mathbf{C}$.
   - $\mathbf{B} \not\subset \mathbf{C}$, $(\mathbf{A} \cup \mathbf{B}) \subset (\mathbf{A} \cup \mathbf{C})$, $(\mathbf{A} \cap \mathbf{B}) \not\subset (\mathbf{A} \cap \mathbf{C})$.
   - $\mathbf{B} \not\subset \mathbf{C}$, $(\mathbf{A} \cup \mathbf{B}) \not\subset (\mathbf{A} \cup \mathbf{C})$, $(\mathbf{A} \cap \mathbf{B}) \subset (\mathbf{A} \cap \mathbf{C})$.

6. Démontrer que l'équivalence suivante est toujours vraie.

$$\Big(\big((\mathbf{A}\cup\mathbf{B})\subset(\mathbf{A}\cup\mathbf{C})\big)\wedge(\mathbf{A}\cap\mathbf{B})\subset(\mathbf{A}\cap\mathbf{C})\big)\Big)\iff\big(\mathbf{B}\subset\mathbf{C}\big)\,.$$

Exercice 2 :

1. Soient A_1 et A_2 deux assertions. Ecrire à l'aide des symboles $\wedge, \vee, \neg$ l'assertion : « de deux choses l'une, soit A_1 est vraie, soit A_2 est vraie, mais pas les deux ». On notera désormais (A_1 Xor A_2) cette assertion.
2. Démontrer à l'aide des tables de vérité que l'implication suivante est toujours vraie.
$$\big(A_1 \text{ Xor } A_2\big)\wedge\big(\neg A_1\big)\implies A_2\,.$$
3. On considère les propositions suivantes : B : « je bois », C :« je conduis », F : « je vais voir un film », M : « je marche », R : « je vais au restaurant ». Ecrire sous forme symbolique les assertions suivantes.
   A_1 : « de deux choses l'une, soit je conduis, soit je marche ».
   A_2 : « de deux choses l'une, soit je vais voir un film, soit je vais au restaurant, et dans ce cas je bois ».
   A_3 : « si je conduis, alors je ne bois pas ».
   A_4 : « je ne marche pas ».
4. On suppose que les assertions A_1, A_2, A_3, A_4 sont vraies. Démontrer que l'assertion F est vraie. Vous écrirez votre raisonnement sous forme symbolique, et en langage courant.

Exercice 3 : Soit $\mathcal{R}$ la relation définie sur l'ensemble des réels $\mathbb{R}$ par :

$$\forall x,y\in\mathbb{R}\,,\quad\big(x\mathcal{R}y\big)\iff\big(x^2-y^2=x-y\big)\,.$$

Soit $\mathcal{S}$ la relation définie sur l'ensemble des réels $\mathbb{R}$ par :

$$\forall x,y\in\mathbb{R}\,,\quad\big(x\mathcal{S}y\big)\iff\big(x^2-y^2\leqslant x-y\big)\,.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Démontrer que pour tout $x\in\mathbb{R}$,
$$\mathfrak{cl}_{\mathcal{R}}(x)=\{x,1-x\}\,.$$
3. Démontrer que la relation $\mathcal{S}$ est réflexive, transitive, mais qu'elle n'est ni symétrique ni anti-symétrique.
4. Soit I l'ensemble des réels supérieurs ou égaux à $1/2$. Soit $\mathcal{S}'$ la relation définie sur I par :
$$\forall x,y\in I\,,\quad\big(x\mathcal{S}'y\big)\iff\big(x^2-y^2\leqslant x-y\big)\,.$$
   Montrer que $\mathcal{S}'$ est une relation d'ordre sur I.
5. Démontrer que :
$$\forall x,y\in I\,,\quad\big(x\mathcal{S}'y\big)\iff\big(x\leqslant y\big)\,.$$

2.5 Corrigé du devoir

Questions de cours :

1. L'image de A est l'ensemble des images par f des éléments de A.

$$f(A) = \{\, f(x)\,,\ x \in A\,\} = \{\, y \in B\,,\ \exists x \in A\,,\ y = f(x)\,\}\,.$$

L'image réciproque de B est l'ensemble des éléments de E dont l'image appartient à B.

$$f^{-1}(B) = \{\, x \in E\,,\ f(x) \in B\,\}\,.$$

2. Soit x un élément quelconque de A. Posons $y = f(x)$. Alors $y \in f(A)$ car $x \in A$. Donc x est un élément de E dont l'image par f appartient à $f(A)$. Par définition de l'image réciproque, x appartient à $f^{-1}(f(A))$. Tout élement de A appartient à $f^{-1}(f(A))$, donc $A \subset f^{-1}(f(A))$.

   Soit y un élément quelconque de $f(f^{-1}(B))$. Par définition de l'image, il existe $x \in f^{-1}(B)$ tel que $f(x) = y$. Puisque $x \in f^{-1}(B)$, l'image de x est dans B, donc $y \in B$. Tout élement de $f(f^{-1}(B))$ appartient à B, donc $f^{-1}(f(B)) \subset B$.

3. On dit que f est injective si tout élément de F a *au plus* un antécédent dans l'ensemble de départ.

$$\forall x_1, x_2 \in E\,,\quad \Big(f(x_1) = f(x_2)\Big) \implies x_1 = x_2\,.$$

   On dit que f est surjective si tout élément de l'ensemble d'arrivée a *au moins* un antécédent dans l'ensemble de départ.

$$\forall y \in F\,,\ \exists x \in E\ ;\quad f(x) = y\,.$$

4. Nous allons montrer que si f est injective, alors $f^{-1}(f(A)) \subset A$. Soit x un élément de $f^{-1}(f(A))$. Par définition de l'image réciproque, $f(x) \in f(A)$. Donc il existe un élément de A dont l'image est égale à celle de x. Mais comme f est injective, cet élément ne peut être que x lui-même. Donc $x \in A$. Tout élément de $f^{-1}(f(A))$ appartient à A, donc $f^{-1}(f(A)) \subset A$. Comme d'après la question 2, $A \subset f^{-1}(f(A))$, nous avons bien démontré que $A = f^{-1}(f(A))$, si f est injective.

   Nous allons maintenant montrer que si f est surjective, alors $B \subset f(f^{-1}(B))$. Soit y un élément de B. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Par définition de l'image réciproque, puisque $y \in B$, $x \in f^{-1}(B)$, et donc $y = f(x) \in f(f^{-1}(B))$. Tout élément de B appartient à $f(f^{-1}(B))$, donc $B \subset f(f^{-1}(B))$. Comme d'après la question 2, $f(f^{-1}(B)) \subset B$, nous avons bien démontré que $B = f(f^{-1}(B))$.

5. Le graphe de f est :

$$\{\, (-1, 1)\,,\ (0, 0)\,,\ (1, 1)\,\}\,.$$

L'application f n'est pas injective car -1 et 1 ont la même image. Elle n'est pas surjective car -1 n'a pas d'antécédent.

$$f^{-1}(f(A)) = \{-1, 1\} \neq A \quad \text{et} \quad f(f^{-1}(B)) = \{1\} \neq B\ .$$

Exercice 1 :

1. Notons I l'assertion proposée.

$$I = \Big((A \vee B) \implies (A \vee C) \Big)\ .$$

Voici sa table de vérité.

A	B	C	$A \vee B$	$A \vee C$	I
V	V	V	V	V	V
V	V	F	V	V	V
V	F	V	V	V	V
V	F	F	V	V	V
F	V	V	V	V	V
F	V	F	V	F	F
F	F	V	F	V	V
F	F	F	F	F	V

2. Notons J l'assertion proposée.

$$J = \Big((A \wedge B) \implies (A \wedge C) \Big)\ .$$

Voici sa table de vérité.

A	B	C	$A \wedge B$	$A \wedge C$	J
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	V	V
V	F	F	F	F	V
F	V	V	F	F	V
F	V	F	F	F	V
F	F	V	F	F	V
F	F	F	F	F	V

3. Voici les tables de vérité des assertions $I \wedge J$ et $B \Longrightarrow C$.

A	B	C	I	J	$I \wedge J$	$B \Longrightarrow C$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	V	V	V	V
V	F	F	V	V	V	V
F	V	V	V	V	V	V
F	V	F	F	V	F	F
F	F	V	V	V	V	V
F	F	F	V	V	V	V

On constate que les tables de vérité des assertions $I \wedge J$ et $B \Longrightarrow C$ sont les mêmes. L'équivalence entre les deux assertions est donc toujours vraie.

4. • $(A \vee B) \Longrightarrow (A \vee C)$: Si je suis une fille ou je fais du sport, alors je suis une fille ou je garde la forme.
   • $(A \vee B) \Longrightarrow (A \vee C)$: Si je suis une fille et je fais du sport, alors je suis une fille et je garde la forme.
   • $B \Longrightarrow C$: Si je fais du sport, alors je garde la forme.

   De deux choses l'une : soit je ne suis pas une fille, soit j'en suis une. Si je ne suis pas une fille (A est faux), la première implication dit que faire du sport est une condition suffisante pour garder la forme. La seconde implication dit que faire du sport est une condition suffisante pour garder la forme, aussi pour les filles. Affirmer les deux premières implications revient à dire que faire du sport est suffisant pour garder la forme, qu'on soit une fille ou non.

5. Voir figure 6.

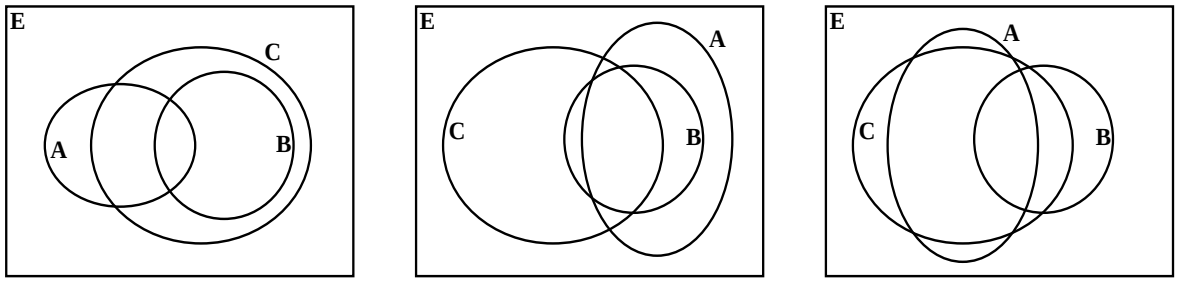

FIG. 6 – Diagrammes de Venn de trois sous-ensembles.

6. Notons respectivement A, B et C les assertions « $x \in \mathbf{A}$ », « $x \in \mathbf{B}$ » et « $x \in \mathbf{C}$ ». Les inclusions de l'énoncé se traduisent comme suit.

$$\Big(\big((\mathbf{A} \cup \mathbf{B}) \subset (\mathbf{A} \cup \mathbf{C}) \big) \iff \Big(\big(A \vee B \big) \Longrightarrow \big(A \vee C \big) \Big) \Big) ,$$

$$\Big(\big((\mathbf{A} \cap \mathbf{B}) \subset (\mathbf{A} \cap \mathbf{C}) \big) \Big) \iff \Big(\big(A \wedge B \big) \Longrightarrow \big(A \wedge C \big) \Big) ,$$
$$\Big(\mathbf{B} \subset \mathbf{C} \Big) \iff \Big(B \Longrightarrow C \Big) .$$

L'équivalence demandée est celle de la question 3.

Exercice 2 :

1. $$A_1 \text{ Xor } A_2 = \big(\neg A_1 \wedge A_2 \big) \vee \big(A_1 \wedge \neg A_2 \big) .$$

2.

A_1	A_2	A_1 Xor A_2	$\big(A_1$ Xor $A_2\big) \wedge (\neg A_1)$	$\big(A_1$ Xor $A_2\big) \wedge (\neg A_1) \Longrightarrow A_2$
V	V	F	F	V
V	F	V	F	V
F	V	V	V	V
F	F	F	F	V

3. A_1 : C Xor M
   A_2 : F Xor $(R \wedge B)$
   A_3 : $C \Longrightarrow (\neg B)$
   A_4 : $\neg M$

4. $$\begin{aligned} (C \text{ Xor } M) \wedge (\neg M) &\Longrightarrow C \\ C &\Longrightarrow (\neg B) \\ (\neg B) &\Longrightarrow \big(\neg (R \wedge B \big) \\ \Big(F \text{ Xor } (R \wedge B) \Big) \wedge \big(\neg (R \wedge B) \big) &\Longrightarrow F . \end{aligned}$$

   Soit je conduis, soit je marche. Puisque je ne marche pas, je conduis ; donc je ne bois pas. Puisque je ne bois pas, je ne suis pas au restaurant en train de boire. Donc je vais voir un film.

Exercice 3 :

1. La relation $\mathcal{R}$ est :
   - *réflexive :*
   $$\forall x \in \mathbb{R} , \quad x^2 - x^2 = x - x ,$$
   - *symétrique :*
   $$\forall x, y \in \mathbb{R} , \quad \big(x^2 - y^2 = x - y \big) \Longrightarrow \big(y^2 - x^2 = y - x \big) ,$$

- *transitive :*

$$\forall x, y, z \in \mathbb{R}\ , \quad \Big(\big(x^2 - y^2 = x - y\big) \wedge \big(y^2 - z^2 = y - z\big)\Big) \Longrightarrow \big(x^2 - z^2 = x - z\big)\ .$$

Donc c'est une relation d'équivalence.

2.

$$\begin{aligned} \forall x, y \in \mathbb{R}^2\ , \quad x\mathcal{R}y &\iff \big(x^2 - y^2 = x - y\big) \\ &\iff (x-y)(x+y-1) = 0 \\ &\iff \Big((x - y = 0) \vee (x + y - 1 = 0)\Big) \\ &\iff \Big((y = x) \vee (y = 1 - x)\Big)\ . \end{aligned}$$

3. La relation $\mathcal{S}$ est :
   - *réflexive :*

$$\forall x \in \mathbb{R}\ , \quad x^2 - x^2 \leqslant x - x\ ,$$

   - *transitive :*

$$\forall x, y, z \in \mathbb{R}\ , \quad \Big(\big(x^2 - y^2 \leqslant x - y\big) \wedge \big(y^2 - z^2 \leqslant y - z\big) \Longrightarrow \big(x^2 - z^2 \leqslant x - z\big)\ ,$$

   - *non symétrique :*

$$0^2 - 2^2 \leqslant 0 - 2 \quad \text{mais} \quad 2^2 - 0^2 > 2 - 0\ ,$$

   - *non anti-symétrique :*

$$0^2 - 1^2 \leqslant 0 - 1 \quad \text{et} \quad 1^2 - 0^2 \leqslant 1 - 0\ .$$

4. La relation $\mathcal{S}'$ est réflexive et transitive, comme la relation $\mathcal{S}$ (car ce qui est vrai sur $\mathbb{R}$ reste vrai sur un sous-ensemble de $\mathbb{R}$). Nous devons démontrer qu'elle est anti-symétrique. Soit I l'ensemble des réels supérieurs ou égaux à $1/2$.

$$\begin{aligned} \forall x, y \in I\ , \quad \Big(x\mathcal{S}'y\Big) \wedge \Big(y\mathcal{S}'x\Big) &\Longrightarrow x^2 - y^2 = x - y \\ &\Longrightarrow (y = x) \vee (y = 1 - x)\ , \end{aligned}$$

d'après la question 2. Or si $x > 1/2$, alors $1 - x < 1/2$, et si $x = 1/2$, alors $1 - x = 1/2$. Donc si x et y sont à la fois éléments de I et tels que $\Big(x\mathcal{S}'y\Big) \wedge \Big(y\mathcal{S}'x\Big)$, alors $x = y$: la relation $\mathcal{S}'$ est anti-symétrique.

5. Soient x et y deux éléments de I. Si $x = y = 1/2$, on a la fois $x\mathcal{S}'y$ et $x \leqslant y$. Si x ou y est strictement supérieur à $1/2$, alors $x + y - 1$ est strictement positif. Dans ce cas :

$$\begin{aligned} (x^2 - y^2) \leqslant (x - y) &\iff (x-y)(x+y-1) \leqslant 0 \\ &\iff x - y \leqslant 0 \\ &\iff x \leqslant y\ . \end{aligned}$$

3 Compléments

3.1 Ces longues chaînes de raisons

Voici cinq textes célèbres à propos de l'universalité et de la perfection du langage mathématique.

Platon (428-348 av. J.-C.), *La République*

> Tu n'ignores pas, je pense, que ceux qui s'occupent de géométrie, d'arithmétique et autres sciences du même genre, supposent le pair et l'impair, les figures, trois espèces d'angles et autres choses analogues suivant l'objet de leur recherche : qu'ils les traitent comme choses connues, et que quand ils en ont fait des hypothèses, ils estiment qu'ils n'ont plus à en rendre aucun compte ni à eux-mêmes ni aux autres, attendu qu'elles sont évidentes à tous les esprits ; qu'enfin, partant de ces hypothèses et passant par tous les échelons, ils aboutissent par voie de conséquences à la démonstration qu'ils s'étaient mis en tête de chercher.

Galilée (1564-1642), *L'Essayeur*

> La philosophie est écrite dans ce très vaste livre qui est éternellement ouvert devant nos yeux – je veux dire l'Univers – mais on ne peut le lire avant d'avoir appris la langue et s'être familiarisé avec les caractères dans lesquels elle est écrite. Elle est écrite en langue mathématique et ses lettres sont des triangles, des cercles et d'autres figures géométriques, moyens sans lesquels il est humainement impossible de comprendre un seul mot, sans lesquels on erre en vain dans un obscur labyrinthe.

Descartes (1596-1650), *Discours de la méthode*

> Ces longues chaînes de raisons, toutes simples et faciles, dont les géomètres ont coutume de se servir pour parvenir à leurs plus difficiles démonstrations, m'avaient donné occasion de m'imaginer que toutes les choses, qui peuvent tomber sous la connaissance des hommes, s'entre-suivent en même façon, et que, pourvu seulement qu'on s'abstienne d'en recevoir aucune pour vraie qui ne le soit, et qu'on garde toujours l'ordre qu'il faut pour les déduire les unes des autres, il n'y en peut avoir de si éloignées auxquelles enfin on ne parvienne, ni de si cachées qu'on ne découvre. Et je ne fus pas beaucoup en peine de chercher par lesquelles il était besoin de commencer : car je savais déjà que c'était par les plus simples et les plus aisées à connaître ; et considérant qu'entre tous ceux qui ont ci-devant recherché la vérité dans les sciences, il n'y a eu que les seuls mathématiciens qui ont pu trouver quelques démonstrations, c'est-à-dire quelques raisons certaines et évidentes, je ne doutais point que ce ne fût par les mêmes qu'ils ont examinées ; bien que je n'en espérasse aucune autre utilité, sinon qu'elles accoutumeraient mon esprit à se repaître de vérités et ne se point contenter de fausses raisons.

Pascal (1623-1662), *De l'esprit géométrique*

> Je ne puis faire entendre la conduite qu'on doit garder pour rendre les démonstrations convaincantes, qu'en expliquant celle que la géométrie observe, et je n'ai choisi cette science pour y arriver que parce qu'elle seule sait les véritables règles du raisonnement, et, sans s'arrêter aux règles des syllogismes qui sont tellement naturelles qu'on ne peut les ignorer, s'arrête et se fonde sur la véritable méthode de conduire le raisonnement en toutes choses, que presque tout le monde ignore, et qu'il est si avantageux de savoir, que nous voyons par expérience qu'entre esprits égaux et toutes choses pareilles, celui qui a de la géométrie l'emporte et acquiert une vigueur toute nouvelle.
>
> Je veux donc faire entendre ce que c'est que démonstrations par l'exemple de celles de géométrie, qui est presque la seule des sciences humaines qui en produise d'infaillibles, parce qu'elle seule observe la véritable méthode, au lieu que toutes les autres sont par une nécessité naturelle dans quelque sorte de confusion que seuls les géomètres savent extrêmement connaître.

Condillac (1715-1780), *La langue des calculs*

> L'algèbre est une langue bien faite, et c'est la seule : rien n'y paraît arbitraire. L'analogie qui n'échappe jamais, conduit sensiblement d'expression en expression. L'usage n'a ici aucune autorité. Il ne s'agit pas de parler comme les autres, il faut parler d'après la plus grande analogie pour arriver à la plus grande précision ; et ceux qui ont fait cette langue, ont senti que la simplicité du style en fait toute l'élégance : vérité peu connue dans nos langues vulgaires.

3.2 Démonstrations non constructives

L'assertion $\exists x \in \emptyset$ est fausse (par définition l'ensemble vide ne contient aucun élément). Toute implication qui commence par $\exists x \in \emptyset$ est forcément vraie, par définition de l'implication. Il est donc indispensable, avant de se lancer dans la démonstration d'une implication, de vérifier que les hypothèses ne sont pas vides, c'est-à-dire qu'elles sont satisfaites par au moins un objet. Sans cela, on pourrait en déduire tout et n'importe quoi. Par exemple l'assertion suivante est mathématiquement correcte, même si nous ne vous conseillons pas de l'apprendre par cœur :

$$\text{Soit } n \text{ un entier tel que } \forall m \in \mathbb{N},\ n \geqslant m. \text{ Alors } 1 = 0.$$

L'hypothèse est vide : aucun entier n'est supérieur à tous les autres.

Une grande partie de l'activité mathématique consiste à démontrer que des hypothèses ne sont pas vides, c'est-à-dire qu'il existe au moins un objet qui les vérifie. On appelle cela un « théorème d'existence ». Il est très possible de démontrer l'existence

d'un objet sans être capable de l'exhiber, ni même de donner un algorithme permettant de le calculer. Voici un exemple célèbre.

Proposition 14. *Il existe deux nombres irrationnels x et y tels que x^y soit rationnel.*

Démonstration : Nous avons vu que le nombre $\sqrt{2}$ est irrationnel. Essayons $\sqrt{2}^{\sqrt{2}}$: il est soit rationnel, soit irrationnel.

- Si $\sqrt{2}^{\sqrt{2}}$ est rationnel, la proposition est démontrée, puisque $x = y = \sqrt{2}$ convient.
- Si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, posons $x = \sqrt{2}^{\sqrt{2}}$, et $y = \sqrt{2}$. Alors

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}\,,$$

et la proposition est également démontrée.

□

Rien dans cette démonstration ne permet de savoir si $\sqrt{2}^{\sqrt{2}}$ est ou non rationnel, et donc l'existence de x et y est démontrée sans qu'on puisse exhiber un seul exemple. On dit que la démonstration est « non constructive ».

Certains mathématiciens, à la suite de Luitzen Brouwer (1881–1966), affirment qu'il n'est pas acceptable de démontrer un théorème d'existence sans être capable de construire au moins un objet vérifiant la propriété. Ils considèrent que cela revient à peu près à affirmer que les licornes existent parce qu'on trouve la définition du mot « licorne » dans les dictionnaires. À vous de juger...

3.3 L'ensemble de tous les ensembles

... n'existe pas ! Un ensemble E n'est défini que si pour tout objet x l'énoncé $(x \in E) \wedge \neg(x \in E)$ est faux.

Proposition 15. *L'ensemble de tous les ensembles n'existe pas.*

Démonstration : C'est un exemple de démonstration par l'absurde. Supposons que l'ensemble de tous les ensembles existe, et notons-le E. Notons A l'ensemble

$$A = \{\, x \in E\,; \quad x \notin x \,\}\,.$$

Comme E contient tous les ensembles, A appartient à E. Est-ce que A appartient à A ?

- si $A \in A$ alors par définition de A, $A \notin A$,
- si $A \notin A$ alors par définition de A, $A \in A$.

L'assertion $A \in A$ ne peut pas être vraie et fausse en même temps, c'est donc que l'hypothèse de départ (E existe) était fausse. □

Des versions plus prosaïques de ce paradoxe sont connues depuis l'antiquité. Par exemple :

Epiménide le Crétois a dit : tous les Crétois sont des menteurs

ou bien

Le barbier rase tous ceux qui ne se rasent pas eux-mêmes.

D'autres notions, apparemment claires, ne sont pas définies parce qu'elles conduisent à une contradiction. Par exemple :

Le plus petit nombre qu'on ne puisse pas définir en moins de vingt mots

(la phrase ci-dessus comporte quinze mots).

3.4 Le rêve de Hilbert

Durant l'été 1900 un congrès international de mathématiques se tenait à Paris. Le 8 août, David Hilbert (1862–1943) y donne une conférence mémorable ; selon Charles Hermite, « on n'entendra plus jamais dans les congrès de conférences pareilles ». Qu'a-t-il donc raconté ? Un théorème exceptionnel que lui seul pouvait démontrer ? Une nouvelle théorie ? Pas du tout. Il s'était contenté d'énoncer 23 problèmes, ceux qui selon lui feraient progresser la recherche en mathématiques durant le siècle qui allait commencer. Le plus impressionnant est que le siècle en question, qui vient de s'achever, lui a très largement donné raison !

Dans plusieurs de ces problèmes, et en particulier dans le dixième, Hilbert pose la question du fondement même du raisonnement mathématique. Il souhaitait rendre explicite un système axiomatique formel « universel ». En ces temps de scientisme triomphant, personne ne doutait que ce soit possible, et que les mathématiques finiraient bien, après tant de victoires sur la nature, par réussir à s'expliquer elles-mêmes.

Hilbert recherchait un système comportant des axiomes et des règles de déduction. Un axiome est une assertion que l'on déclare vraie a priori : par exemple $0 < 1$. Nous avons vu les règles de déduction de la logique, et le moyen de déclarer vraie ou fausse une assertion composée, en utilisant les tables de vérité. Hilbert souhaitait un système :

- *consistant :* aucune assertion ne peut être à la fois vraie et fausse ;
- *complet :* toute assertion est soit vraie soit fausse ;
- *décidable :* il existe une procédure finie qui permet de vérifier si une assertion donnée est vraie ou fausse.

On peut démontrer qu'un système consistant et complet est forcément décidable. Une procédure de décision consiste à ranger toutes les formules possibles d'abord par ordre de longueur, puis par ordre lexicographique pour les formules de même longueur. Si on doit vérifier l'assertion A, on parcourt les formules une par une en vérifiant pour chacune si elle est valide et si elle entraîne A ou bien $\neg A$. Ce n'est pas très efficace, mais cela conduira forcément au résultat !

En 1931 Kurt Gödel (1906–1978) ruine le rêve de Hilbert : il démontre que dans tout système formel contenant l'arithmétique des entiers, il existe des propriétés telles que l'on ne peut prouver ni qu'elles sont vraies, ni qu'elles sont fausses : on dit qu'elles sont indécidables. La démonstration de Gödel est trop difficile pour être exposée ici, mais elle ressemble dans ses grandes lignes à celle de la proposition 15. Il considère un système consistant pour l'arithmétique des entiers. Il construit alors une assertion sur les nombres entiers qui exprime par elle-même qu'elle n'est pas dénombrable : si elle est vraie, alors elle est fausse, et si elle est fausse, alors elle est vraie. Il en déduit que le système ne peut pas être complet.

Parmi les exemples d'assertions indécidables, l'*axiome du choix* est le plus célèbre. Il s'agit de l'assertion affirmant que si un ensemble E est muni d'une relation d'équivalence, alors on peut choisir dans chacune des classes d'équivalence un élément particulier. C'est évident si les classes d'équivalence sont finies ou dénombrables, mais cela ne l'est pas en général. On peut le supposer vrai, ou bien faux, sans jamais aboutir à une contradiction.

Loin de sonner le glas de la recherche sur les systèmes formels, le résultat négatif de Gödel a donné une impulsion décisive à la logique, conduisant en particulier avec Alan Turing (1912–1954), aux fondements de l'informatique théorique.

3.5 Les cardinaux infinis

Combien y a-t-il d'entiers naturels, de rationnels, de réels ? Une infinité bien sûr. Mais l'infinité des réels est plus grande que l'infinité des rationnels. Pour donner un sens à cette affirmation, il faut d'abord définir ce qu'est un ensemble dénombrable.

Définition 13. *Un ensemble infini est dit dénombrable s'il existe une application injective de cet ensemble vers* $\mathbb{N}$.

Il peut paraître paradoxal que $\mathbb{Q}$ soit dénombrable. C'est pourtant le cas, car il existe une application injective de $\mathbb{Q}$ vers $\mathbb{Z} \times \mathbb{N}$ (à un rationnel p/q on associe le couple (p, q)), et une application bijective de $\mathbb{Z} \times \mathbb{N}$ dans $\mathbb{N}$: on compte les éléments de $\mathbb{Z} \times \mathbb{N}$, en commençant par $(0, 0)$, puis $(1, 0), (0, 1), (-1, 0)$, puis $(2, 0), (1, 1), (0, 2)$, $(-1, 1), (-2, 0)$, ... Plus généralement, on démontre que le produit et la réunion de deux ensembles dénombrables sont eux-mêmes dénombrables.

Théorème 4. *L'ensemble des réels n'est pas dénombrable.*

Démonstration : Nous allons démontrer par l'absurde que l'intervalle $[0, 1]$ n'est pas dénombrable. Supposons que l'on puisse compter les éléments de $[0, 1]$, donc les mettre en bijection avec $\mathbb{N}$. Nous aurions $[0, 1] = \{x_n\,,\ n \in \mathbb{N}\}$. À l'élément x_n, nous associons un développement décimal :

$$x_n = 0.a_{n,1}a_{n,2}a_{n,3}\ldots\ ,$$

où les $a_{n,k}$ sont des entiers compris entre 0 et 9. Pour tout n, fixons $b_n \in \{1, \ldots, 8\}$, tel que $b_n \neq a_{n,n}$. Considérons le réel x dont le développement décimal est

$$x = 0.b_1 b_2 b_3 \ldots$$

Ce réel est différent de x_n pour tout n, par construction. Il n'a donc pas pu être compté. (Ce principe de démonstration s'appelle le *procédé diagonal de Cantor*). □

Il y a plus de réels que de rationnels, et donc plus d'irrationnels que rationnels. Parmi les irrationnels, on distingue ceux qui sont solutions d'une équation polynomiale à coefficients entiers, comme $\sqrt{2}$: on les appelle les nombres algébriques. Ils semblent former une grosse masse. Pourtant il n'y a pas plus de polynômes à coefficients entiers que d'entiers : l'ensemble des nombres algébriques est lui aussi dénombrable. Les nombres qui ne sont pas algébriques (on les appelle « transcendants ») forment l'essentiel des réels. Pourtant il est extrêmement difficile de démontrer qu'un réel particulier est transcendant. C'est une des victoires du 19e siècle que de l'avoir fait pour π et e.

Existe-t-il des ensembles « intermédiaires » entre $\mathbb{N}$ et $\mathbb{R}$, qui seraient non dénombrables, sans pourtant être en bijection avec $\mathbb{R}$? C'est le premier des 23 problèmes posés par Hilbert en 1900. On a longtemps essayé d'en construire, ou de démontrer qu'il n'en existe pas, avant de s'apercevoir finalement que c'est une assertion indécidable : on peut la supposer vraie, ou bien fausse, sans jamais aboutir à une contradiction. Elle s'appelle « l'hypothèse du continu ».

3.6 Ensembles quotients

Bertrand Russel (1872–1970) a dit « It must have required many ages to discover that a brace of pheasants and a couple of days were both instances of the number two ». Nous avons vu cela sous une forme moins imagée : le cardinal d'un ensemble peut être défini comme une classe d'équivalence d'ensembles en bijection avec lui.

À la base des mathématiques, comme de toute activité intellectuelle se trouvent les concepts. Concept en mathématiques se dit classe d'équivalence : cela désigne une boîte fictive dans laquelle nous pouvons ranger toutes sortes d'objets, pourvu qu'ils aient une propriété commune. Une fois la boîte remplie, et dûment pourvue d'une étiquette nommant la propriété qu'elle représente, on peut oublier son contenu et ne plus garder que l'étiquette qui pourra d'ailleurs devenir un nouvel objet. Cette faculté d'abstraire des propriétés communes est essentiellement humaine. C'est l'arme qui nous a permis de prendre une telle avance dans la lutte darwinienne pour la survie de l'espèce. Parce que l'homme préhistorique voyait un rapport entre un bras qui frappe et une branche qui tombe, il a été capable d'inventer la massue. C'est aussi la base du langage. Tout mot est une classe d'équivalence : « bleu » ou « table » ne sont que des boîtes pouvant contenir des objets différents. Le miracle est que ces classes d'équivalence soient transmissibles : que deux humains différents puissent être globalement d'accord sur les contenus de leurs boîtes.

En mathématiques, les relations d'équivalence servent à fabriquer toutes sortes d'ensembles. Nous n'en donnerons qu'un exemple, la construction de l'ensemble $\mathbb{Q}$ des rationnels à partir de l'ensemble des entiers.

Un rationnel est le rapport de deux nombres entiers, l'un entier relatif, l'autre entier naturel non nul.

$$\mathbb{Q} = \left\{ \frac{p}{q}\,,\ (p,q) \in \mathbb{Z} \times \mathbb{N}^* \right\}$$

Deux couples d'entiers peuvent représenter le même rationnel.

$$\forall p \in \mathbb{Z}\,,\ \forall q \in \mathbb{N}^* \quad \frac{p}{q} = \frac{p'}{q'} \iff pq' = qp'$$

Oublions maintenant les rationnels et supposons que nous ne connaissions que l'ensemble $E = \mathbb{Z} \times \mathbb{N}^*$. Considérons la relation $\mathcal{R}$ définie sur E de la façon suivante.

$$(p,q)\mathcal{R}(p',q') \iff pq' = qp'\ .$$

Il est facile de vérifier qu'elle est réflexive, symétrique et transitive : c'est une relation d'équivalence. L'ensemble quotient $E/\mathcal{R}$ est précisément l'ensemble des rationnels. Mais pour que cette définition soit utilisable, il faut la compléter par les opérations dont nous avons besoin : addition, multiplication, ordre total.

1. *addition :* considérons l'application de $E \times E$ vers E qui à deux couples (p,q) et (r,s) associe le couple $(ps+rq, qs)$. C'est bien ce que nous attendons de l'addition des rationnels : $p/q + r/s = (ps + rq)/qs$. Le miracle est que l'application que nous avons définie « passe au quotient » : si $(p',q')\mathcal{R}(p,q)$ et $(r',s')\mathcal{R}(r,s)$, alors $(p's' + r'q', q's')\mathcal{R}(ps + rq, qs)$ (vérifiez... !). Si on la transporte sur l'ensemble quotient, cette application définit l'addition des rationnels.
2. *multiplication :* considérons l'application de $E \times E$ vers E qui à deux couples (p,q) et (r,s) associe le couple (pr, qs). C'est ce que nous attendons de la multiplication des rationnels : $(p/q)(r/s) = (pr)/(qs)$. Comme ci-dessus, si on la transporte sur l'ensemble quotient, l'application définit la multiplication des rationnels.
3. *ordre :* considérons la relation $\mathcal{O}$ sur E définie par :

   $$(p,q)\mathcal{O}(r,s) \iff (ps \leqslant rq)$$

   Même technique : une fois transportée sur l'ensemble quotient, la relation $\mathcal{O}$ devient la relation d'ordre total que nous attendons sur $\mathbb{Q}$.

Ce que nous venons de décrire pour l'ensemble des rationnels est un cas particulier d'une procédure très générale, qui consiste à rajouter ce qui manque à un ensemble en définissant une relation d'équivalence sur un ensemble plus gros. Ainsi on peut définir $\mathbb{Z}$ à partir de $\mathbb{N}$, puis $\mathbb{Q}$ à partir de $\mathbb{N}$ et $\mathbb{Z}$, puis $\mathbb{R}$ à partir de $\mathbb{Q}$ puis $\mathbb{C}$ à partir de $\mathbb{R}$. Cela sert aussi pour des espaces de fonctions, et encore bien d'autres objets que vous rencontrerez plus tard.

3.7 Ramener l'infini au fini

Le principe du raisonnement par récurrence a probablement été formulé clairement pour la première fois par Blaise Pascal (1623-1662), dans son *Traité du triangle arithmétique*. Voici son texte.

> Quoique cette proposition ait une infinité de cas, j'en donnerai une démonstration bien courte, en supposant deux lemmes.
>
> Le premier, qui est évident de soi-même, que cette proportion se rencontre dans la seconde base [...]
>
> Le second, que si cette proportion se trouve dans une base quelconque, elle se trouvera nécessairement dans la base suivante.
>
> D'où il se voit qu'elle est nécessairement dans toutes les bases : car elle est dans la seconde base par le premier lemme ; donc par le second elle est dans la troisième base, donc dans la quatrième, et à l'infini.