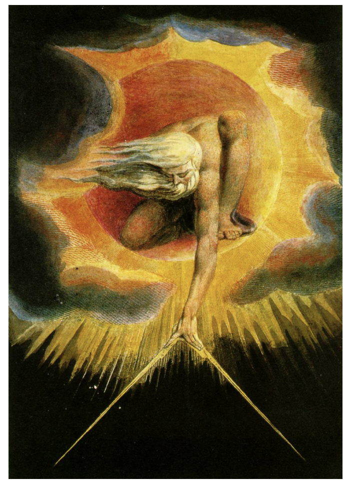
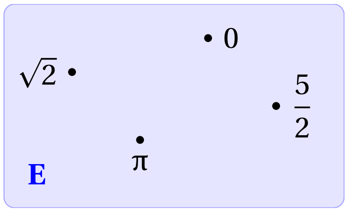
ALG 2 | Théorie des ensembles

Le cours d'algèbre se poursuit par un aperçu de la théorie des ensembles. Cette leçon, très abstraite et particulièrement difficile, a deux objectifs : familiariser le lecteur à la méthode mathématique (chaque objet nouveau est construit à partir des précédents) tout en présentant les objets fondamentaux des Mathématiques.



Le Dieu Architecte, William Blake

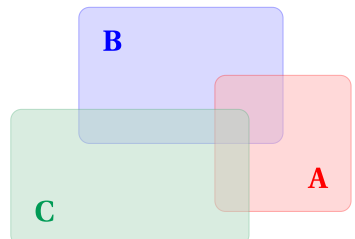
D’UN point de vue intuitif, un *ensemble* est une collection non ordonnée et sans répétition d’objets appelés ses *éléments*. Il faut bien comprendre que seule l’appartenance des objets à la collection importe : il n’y a ni hiérarchie (aucun ordre) entre les différents éléments d’un ensemble, ni répétition.



Les ensembles sont universellement délimités au moyen *d’une paire d’accolades ouvrante-fermante* $\{\}$ et leurs éléments sont énumérés entre celles-ci, séparés par des virgules. En notant E l’ensemble ci-contre, on peut donc écrire

$$\mathrm{E} = \left\{0, \pi, \sqrt{2}, \frac{5}{2}\right\}, \ \mathrm{E} = \left\{\pi, \frac{5}{2}, 0, \sqrt{2}\right\} \quad \text{et} \quad \{\pi, \pi\} = \{\pi\}$$

Afin de se forger une intuition, on peut représenter en dimension deux les ensembles comme des boîtes contenant des objets. Ces figures ne sont bien sûr qu’un support visuel permettant de donner un sens plus concret à certains résultats dont elles ne constituent nullement une démonstration. Il faut aussi de méfier des figures qui peuvent parfois induire en erreur, notamment lorsque l’on ne représente que des cas particuliers ou, au contraire, qu’on en oublie !



Ensemble, symboles $\in$ (appartenance) et $\notin$ (son contraire)

Un ensemble E est une collection non ordonnée et sans répétition d’objets.

⇛ L’énoncé $x \in \mathrm{E}$ signifie que l’objet x appartient à l’ensemble E, on dit aussi que x est un élément de E ou encore que E contient x, ou plus simplement que x est dans E.

⇛ On écrira $x \notin \mathrm{E}$ pour signifier que l’objet x n’appartient pas à l’ensemble E.

Cette approche naïve des ensembles a longtemps suffit aux savants, tant que les ensembles furent utilisés comme un langage de description des mathématiques.

Au mitan du XIXe siècle, les ensembles sont progressivement devenus un objet d’étude à part entière sous l’impulsion de Georg Cantor. Les mathématiciens et philosophes qui se sont penchés sur cette nouvelle question ont aboutit à une conclusion sans appel : l’utilisation formelle des ensembles nécessite des règles sans lesquelles surgissent des absurdités.

L’illustration la plus célèbre de cette *crise des fondements* est sans conteste le paradoxe de Russell :

Paradoxe de Russell

Supposons l’existence d’un ensemble E dont les éléments sont *tous* les ensembles. Supposons alors que l’on puisse définir le sous-ensemble A de E dont les éléments sont les ensembles X vérifiant

$$\mathrm{X} \notin \mathrm{X}$$

On aboutit à une contradiction car aucune des deux propositions $\mathrm{A} \in \mathrm{A}$ et $\mathrm{A} \notin \mathrm{A}$, pourtant contraires, n’est vérifiée.

Moralité : on ne peut donc définir sans précaution des ensembles, sous peine d’aboutir à une théorie contradictoire.

Dans la suite du cours de Mathématiques, nous verrons que le point de vue intuitif sur les ensembles est bien souvent suffisant au débutant et que seuls quelques domaines nécessitent une connaissance pointue de la théorie des ensembles.

1. Introduction à la théorie des ensembles

Cette crise des fondements aboutit au début du XX^{e} siècle à une axiomatisation de l'idée d'ensemble, connue sous le nom de théorie des ensembles.

De l'approche naïve, il reste que les notions d'ensemble et d'appartenance ne sont pas définies. On dit qu'elles sont *primitives* (ou encore *premières*). On peut faire l'analogie avec les notions de point et de droite en géométrie classique, qui ne sont pas définies mais données a priori, et dont les règles d'usage sont fixés par des axiomes.

La théorie des ensembles repose sur l'axiomatique de **Zermelo-Fraenkel** à laquelle nous ajoutons l'axiome du choix – le tout est appelé **modèle ZFC**. Ces huit axiomes dictent ce que l'on peut et ne peut pas faire avec les notions d'ensemble et d'appartenance. Ils portent traditionnellement les noms suivants : axiomes **d'extension**, **de spécification**, **de fondement**, **de la paire**, **de la réunion**, **de l'ensemble des parties**, **de l'infini** et **du choix**. Ces huit axiomes sont à comprendre comme des règles de construction d'ensembles garantissant la cohérence logique des Mathématiques (contrairement à l'approche naïve).

Avertissement au lecteur

Pour bien aborder l'intégralité de cette introduction, il est conseillé au lecteur de méditer les remarques et conseils suivants :

- Comme en géométrie, l'objectif de la théorie est de donner des définitions s'accordant avec nos intuitions. C'est la moisson ultérieure de théorèmes qui nous confortera dans l'idée que ces définitions étaient « bonnes ».
- Il faut bien jouer le jeu en s'efforçant de n'appliquer que les axiomes et les théorèmes déjà démontrés lors de nouvelles preuves. Attention à ne pas utiliser des énoncés très intuitifs mais non encore démontrés ! C'est le principal écueil des apprentis mathématiciens.
- Dans ce qui suit, TOUT est ensemble : les variables, minuscules ou majuscules, désignent des ensembles. Ce sont les seuls objets de la théorie. Ainsi, un énoncé de la forme

$$(\forall \mathrm{A}),\ (\forall \mathrm{B}),\ (\exists \mathrm{C}),\ (\forall x),\ \text{etc.}$$

  devra être lu et compris comme suit : pour tout ensemble A, tout ensemble B, il existe un ensemble C tel que, pour tout ensemble x, etc. Tous les objets mathématiques sont des ensembles : les nombres 0, -1, $\frac{2}{3}$ et π, la fonction cosinus, la suite géométrique $\left(2^{n}\right)_{n\in\mathbb{N}}$), etc. sont des ensembles.

À partir de cette théorie, on peut construire pas à pas tous les objets des mathématiques (nombres entiers, rationnels, réels, fonctions, suites, etc.). Nous verrons ainsi qu'un entier peut être défini comme un ensemble, une suite comme un autre ensemble, et ainsi de suite.

Les axiomes du modèle ZFC sont hors programme. Dans ce qui suit, ils seront introduits progressivement et, afin d'éviter toute dérive formelle, nous les énonceront dans le langage courant, sans recourir à la logique du premier ordre.

1.1. Définition en extension ou en compréhension d'un ensemble

Afin de faciliter la compréhension de ce cours très abstrait, nous nous efforcerons d'écrire en minuscule les éléments d'un ensemble écrit en majuscule. Nous écrirons par exemple $x \in \mathrm{A}$. Encore une fois, il faut bien comprendre que, dans cette relation, x et A sont des ensembles.

ZFC I – Axiome d'extension

Un ensemble est entièrement déterminé par la donnée de ses éléments. Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

De cet axiome découle une première manière de décrire un ensemble.

Notation 2.0. Définition en extension d'un ensemble

Un ensemble est défini en extension par l'énumération de ses éléments, séparés par des virgules, délimitée par une paire d'accolades.

On retrouve les notations usuelles $\{0\}$, $\{0,1\}$, etc. Dans la pratique, on ne peut pas, le plus souvent, énumérer tous les éléments d'un ensemble, par exemple parce qu'il y en a trop. La notation en extension admet une variante qui permet de surmonter cette difficulté : il est possible de donner l'expression générale des éléments au moyen de paramètres.

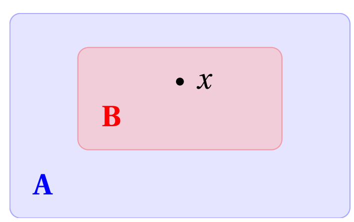
- Par exemple, on écrira $2\mathbb{N} := \left\{2k\,;\ k \in \mathbb{N}\right\}$ qui se lit « $2\mathbb{N}$ est l'ensemble des nombres de la forme $2k$ où k appartient à $\mathbb{N}$ ».

Définition 2.1. La relation d'inclusion (⚡ 2.1)

Soit A et B deux ensembles.

- On écrira $\mathrm{B} \subset \mathrm{A}$ et l'on dira que « B est un sous-ensemble de A » ou encore que « B est une partie de A » pour signifier que tous les éléments de B sont contenus dans A.
- La proposition $\mathrm{B} \subset \mathrm{A}$ est donc synonyme de $\forall x,\ (x \in \mathrm{B}) \implies (x \in \mathrm{A})$.

Ne pas confondre $\subset$ et $\in$ Le symbole d'inclusion $\subset$ est réservé à la comparaison de deux ensembles, il ne faut pas le confondre avec le symbole $\in$ qui est utilisé pour dire qu'un objet appartient à un ensemble. Ainsi, on écrira au choix $x \in \mathrm{B}$ pour traduire le fait que x est un élément de B. Ci-contre, on a les relations $x \in \mathrm{B}$ et $\mathrm{B} \subset \mathrm{A}$.



On déduit directement de cette définition et de l'axiome d'extension le principe suivant, dit de la double inclusion :

Proposition 2.2. (Principe de la double inclusion).

Pour tous ensembles A et B, $\mathrm{A} = \mathrm{B} \iff \mathrm{A} \subset \mathrm{B}$ et $\mathrm{B} \subset \mathrm{A}$.

- Réflexivité et transitivité de l'inclusion. On notera que la relation d'inclusion vérifie les propriétés suivantes, d'usage très courant :
  - $\forall A,\quad A \subset A$ (propriété de réflexivité de l'inclusion) ;
  - $\forall A,\ \forall B,\ \forall C,\ \big(A \subset B \text{ et } B \subset C\big) \implies A \subset C$ (transitivité de l'inclusion).

L'axiome de spécification exprime la possibilité de définir, pour un ensemble donné A, l'ensemble des éléments de A vérifiant une certaine propriété.

ZFC II – Axiome de spécification

Pour tout ensemble A et toute formule logique $\mathscr{P}(x)$ à une variable x, il existe un ensemble B dont les éléments sont les x vérifiant $x \in A$ et $\mathscr{P}(x)$. Cet ensemble B est noté $\big\{x \in A\,;\, \mathscr{P}(x)\big\}$.

Les formules sont construites au moyen des règles de la logique du premier ordre que nous avons évoquée dans le chapitre précédent[1].

Notation 2.3. Définition en compréhension d'un ensemble (⚡2.2)

En reprenant les notations de l'axiome de spécification, l'ensemble B est noté

$$\big\{x \in A\,;\, \mathscr{P}(x)\big\}$$

On peut également noter $\big\{x \in A : \mathscr{P}(x)\big\}$ ou $\big\{x \in A \,|\, \mathscr{P}(x)\big\}$, voire utiliser un autre séparateur.

Cette description ensembliste est appelée *définition en compréhension*, i.e. définition au moyen d'une propriété caractéristique.

- Par exemple, on peut définir ainsi l'ensemble $2\mathbb{N}$ des entiers naturels pairs :

$$2\mathbb{N} := \big\{n \in \mathbb{N}\,;\, \exists k \in \mathbb{N},\ n = 2k\big\}$$

- Déterminer l'ensemble des solutions d'une équation dont l'inconnue appartient à un ensemble E revient à écrire l'ensemble de ses solutions en extension.
  - Par exemple $F := \big\{z \in \mathbb{C}\,;\, z^2 + 1 = 0\big\}$ est une définition en compréhension.
  - Le cours sur les nombres complexes de Terminale nous permet de trouver une expression en extension de F :

$$F = \big\{-i, i\big\}$$

À des fins d'exhaustivité, il faut mentionner l'axiome de fondement mais nous ne l'énoncerons pas. Il n'est utilisé que dans certains domaines des Mathématiques et nous ne l'utiliserons jamais.

ZFC III – Axiome de fondement

Une de ses conséquences est qu'il n'existe aucun ensemble E tel que $E \in E$.

1.2. L'ensemble vide, singletons et paires

L'axiome de spécification, en admettant l'existence d'un ensemble (que garantira l'axiome de l'infini), permet de définir l'ensemble vide :

1. Nous n'en avons toutefois pas explicité les règles syntaxiques précises. Il faudra se fier à son bon sens en la matière.

L'ensemble vide

Il existe un unique ensemble n'ayant aucun élément, appelé ensemble vide et noté $\varnothing$. Il est contenu dans tous les ensembles :

$$(\forall \mathrm{E}),\ (\varnothing \subset \mathrm{E})$$

Autrement dit, $\varnothing$ est une partie (la partie vide) de tout ensemble E.

Nous en arrivons à l'axiome de la paire, autre outil fondamental pour construire de nouveaux ensembles à partir d'ensembles donnés.

ZFC IV – Axiome de la paire

- Pour tous ensembles A et B, il existe un ensemble dont les éléments sont A et B.
- Cet ensemble P est noté $\{\mathrm{A},\mathrm{B}\}$ et appelé paire formée par A et B.
- Dans le cas particulier où A et B sont égaux, la paire $\{\mathrm{A},\mathrm{B}\}$ est plus simplement notée $\{\mathrm{A}\}$ et appelée singleton.

1.3. Différence, réunion et intersection

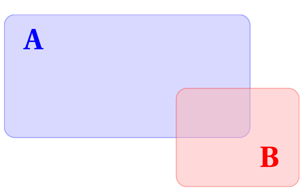
L'axiome de la réunion est un outil permettant de construire, comme nous le verrons plus loin, des ensembles de plus en plus élaborés.

Définition 2.4. Différence de deux ensemble

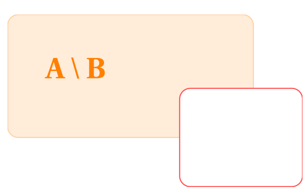
Pour tous ensembles A et B, on pose :

$$\mathrm{A} \setminus \mathrm{B} := \left\{x \in \mathrm{A}\,;\, x \notin \mathrm{B}\right\}$$

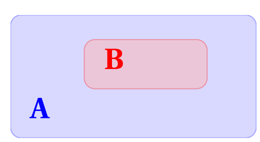
- Cet ensemble est appelé A privé de B ou encore A moins B.
- Dans le cas particulier où $\mathrm{B} \subset \mathrm{A}$, $\mathrm{A} \setminus \mathrm{B}$ est aussi appelé complémentaire de B dans A. On le note $\complement_{\mathrm{A}}\mathrm{B}$, voire B^c ou encore $\overline{\mathrm{B}}$ s'il n'y a pas d'ambiguité sur l'ensemble A par rapport auquel la différence est calculée.



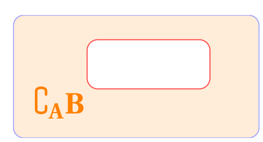
A et B



A \ B



B partie de A



Complémentaire de B dans A

La réunion est définie dans un cadre général (celui d'un nombre quelconque d'ensembles) au moyen de l'axiome suivant.

ZFC V – Axiome de la réunion

- Pour tous ensembles A et B, il existe un ensemble dont les éléments sont exactement les x tels que $x \in \mathrm{A}$ ou $x \in \mathrm{B}$.

⇛ Il est noté $A \cup B$ et appelée réunion de A et B.

⇛ Plus généralement, pour tout ensemble E, il existe un ensemble U dont les éléments sont les x qui appartiennent à au moins l'un des éléments de E :

$$U = \left\{ x\,;\, \exists S \in E,\, x \in S \right\}$$

⇛ Cet ensemble U est appelé réunion des éléments de E et noté $\bigcup\limits_{S \in E} S$.

- Par exemple, pour $E = \{A, B\}$, on a $\bigcup\limits_{S \in E} S = A \cup B$.
- Propriétés de la réunion. Commutativité et associativité :

$$\forall A,\ \forall B,\ \forall C,\ A \cup B = B \cup A \quad \text{et} \quad A \cup (B \cup C) = (A \cup B) \cup C$$

  Ces deux propriétés s'étendent facilement par récurrence sur le nombre de termes à des réunions finies quelconques.
- L'associativité de la réunion permet de généraliser la construction initiée par l'axiome de la paire. Par exemple, pour trois ensembles A, B et C, on pose

$$\left\{A, B, C\right\} := \left\{A\right\} \cup \left\{B\right\} \cup \left\{C\right\}$$

  On étend facilement cette construction par récurrence sur le nombre d'ensembles[2] A, …, J, K, etc. On remarquera que cette généralisation ne permet pas de construire un ensemble infini mais des ensembles ayant un nombre arbitraire fini d'éléments : atteindre l'infini nécessitera un autre axiome.

La définition de l'intersection dans le cadre d'un nombre quelconque d'ensembles ne nécessite aucun axiome nouveau.

Définition 2.5. Intersection

Pour tous A et B, il existe un unique ensemble dont les éléments sont les x appartenant à A et à B.

⇛ Plus généralement, pour tout ensemble E non vide, il existe un unique ensemble I dont les éléments sont les x qui appartiennent à tous les éléments de E.

⇛ Cet ensemble I est appelé intersection des éléments de E et noté $\bigcap\limits_{S \in E} S$.

Comme a réunion, l'intersection est clairement commutative et associative. Les opérations de réunion et d'intersection vérifient de nombreuses propriétés, intuitivement claires et très faciles à établir. En voici quelques unes :

- Dans le cas où $E := \{A, B\}$, on a $\bigcap\limits_{S \in E} S = A \cap B$.
- Règles de calcul usuelles. Pour tous ensembles A', B', A, B, et C :

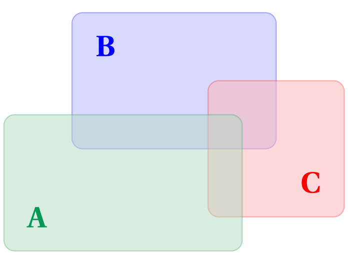
2. Cette remarque reste bien évidemment informelle à ce stade du cours où la notion d'entier naturel n'a pas encore été définie.

- $\begin{cases} A \subset A' \\ B \subset B' \end{cases} \Longrightarrow \begin{cases} A \cup B \subset A' \cup B' \, (\star) \\ A \cap B \subset A' \cap B' \, (\star\star) \end{cases}$;
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

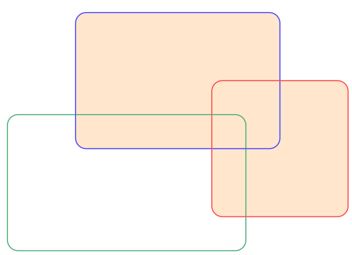
Les deux dernières propriétés sont respectivement appelées distributivité de l'intersection sur le réunion et distributivité de la réunion sur l'intersection.

- Démontrons par exemple que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. On procède par double inclusion.
  - Soit $x \in A \cap (B \cup C)$. On a $x \in A$ et $x \in B \cup C$.
    - Cas 1 : $x \in B$. On a alors $x \in A \cap B$.
    - Cas 2 : $x \in C$. On a alors $x \in A \cap C$.
    - Ainsi, dans tous les cas, $x \in (A \cap B) \cup (A \cap C)$. Ceci démontre $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$.
  - Soit $x \in (A \cap B) \cup (A \cap C)$.
    - Cas 1 : $x \in A \cap B$. On a alors $x \in B$ donc $x \in B \cup C$. Comme $x \in A$, on a aussi $x \in A \cap (B \cup C)$.
    - Cas 2 : $x \in A \cap C$. On a alors $x \in C$ donc $x \in B \cup C$. Comme $x \in A$, on a aussi $x \in A \cap (B \cup C)$.
    - Ainsi, dans tous les cas, $x \in A \cap (B \cup C)$. Ceci démontre $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.
  - L'inclusion $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$ peut se démontrer sous revenir à des éléments.
    - On a $B \subset B \cup C$ d'où $A \cap B \subset A \cap (B \cup C)$ en intersectant par A membre à membre $(\star\star)$.
    - De même $C \subset B \cup C$ d'où $A \cap C \subset A \cap (B \cup C)$.
    - On en déduit que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$ en prenant la réunion membre à membre $(\star)$.

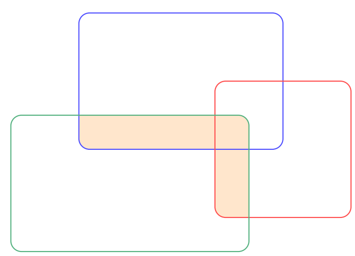
Il recommandé au lecteur de s'aider au besoin de figures pour bien comprendre certains résultats, comme par exemple la distributivité de l'intersection sur la réunion :



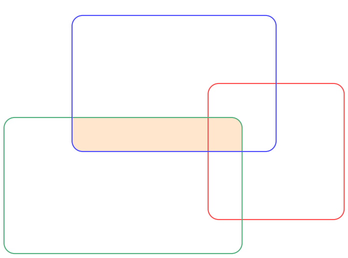
Les ensembles A, B et C



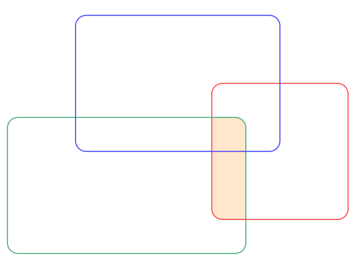
L'ensemble $B \cup C$



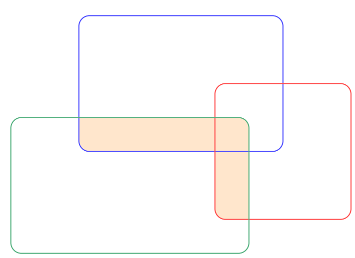
L'ensemble $A \cap (B \cup C)$



L'ensemble $A \cap B$



L'ensemble $A \cap C$



L'ensemble $(A \cap B) \cup (A \cap C)$

1

Le lecteur pourra s'entraîner grace au test (⚡ **2.3**)

1.4. Ensemble des parties

L'axiome de l'ensemble des parties postule l'existence de l'ensemble de toutes les parties d'un ensemble donné.

ZFC VI – Axiome de l'ensemble des parties

⇛ Pour tout ensemble E, il existe un ensemble P dont les éléments sont les sous-ensembles de E.

⇛ On le note $\mathscr{P}(\mathrm{E})$, ensemble des parties de E.

On déduit de cette définition que les propositions $\mathrm{F} \in \mathscr{P}(\mathrm{E})$ et $\mathrm{F} \subset \mathrm{E}$ sont donc équivalentes pour tous ensembles E et F.

✗ Déterminons $\mathscr{P}(\mathrm{E})$ pour les valeurs suivante de E : $\varnothing$, $\{\varnothing\}$ et $\big\{\varnothing, \{\varnothing\}\big\}$.

- ✔ La seule partie de $\mathrm{E}_0 := \varnothing$ étant $\varnothing$, on a $\mathrm{E}_1 := \mathscr{P}(\mathrm{E}_0) = \{\mathrm{E}_0\}$.
- ✔ Les seules parties de E_1 étant $\varnothing$ et E_1, on a $\mathrm{E}_2 := \mathscr{P}(\mathrm{E}_1) = \{\mathrm{E}_0, \mathrm{E}_1\}$.
- ✔ Les seules parties de E_2 étant $\varnothing$, $\{\mathrm{E}_0\}$, $\{\mathrm{E}_1\}$ et E_2, on a $\mathrm{E}_3 := \mathscr{P}(\mathrm{E}_2) = \big\{\mathrm{E}_0, \{\mathrm{E}_0\}, \{\mathrm{E}_1\}, \mathrm{E}_2\big\}$.

D'un point de vue intuitif, partitionner un ensemble, c'est le découper en sous-parties non vides et disjointes[3].

Définition 2.6. Partitions et recouvrements d'un ensemble (⚡ 2.4)

Soit E un ensemble.

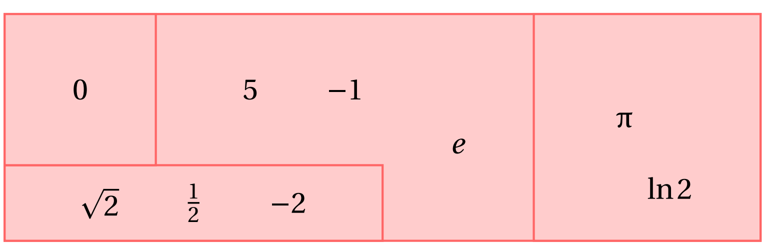
⇛ On appelle recouvrement de E tout sous-ensemble $\mathscr{R}$ de $\mathscr{P}(\mathrm{E})$ tel que $\displaystyle\bigcup_{\mathrm{S}\in\mathscr{R}} \mathrm{S} = \mathrm{E}$.

⇛ On appelle recouvrement disjoint $\mathscr{R}$ de E tout recouvrement $\mathscr{R}$ de E tel que

$$\forall (\mathrm{A}, \mathrm{B}) \in \mathscr{R}^2,\ \mathrm{A} \neq \mathrm{B} \implies \mathrm{A} \cap \mathrm{B} = \varnothing$$

⇛ On appelle partition de E tout recouvrement disjoint $\mathscr{R}$ de E tel que

$$\forall \mathrm{A} \in \mathscr{R},\ \mathrm{A} \neq \varnothing$$



Ci-contre la partition

$$\Big\{\big\{\pi, \ln 2\big\}, \big\{0\big\}, \Big\{\sqrt{2}, \frac{1}{2}, -2\Big\}, \big\{5, -1, e\big\}\Big\}$$

de $\{\pi, \ln 2, 0, \sqrt{2}, \frac{1}{2}, -2, 5, -1, e\}$.

Les règles de négation des disjonctions, des conjonctions et des quantificateurs permettent de décrire *mécaniquement* le complémentaire d'une union ou d'une intersection.

Proposition 2.7. Relations de De Morgan

Soit A et B des parties d'un ensemble E et $\mathscr{R} \in \mathscr{P}\big(\mathscr{P}(\mathrm{E})\big)$.

3. Penser par exemple aux partitions d'un disque dur en informatique.

a. $\overline{A\cap B}=\overline{A}\cup\overline{B}$ et $\overline{A\cup B}=\overline{A}\cap\overline{B}$; **b.** $\overline{\bigcup_{S\in\mathscr{R}} S}=\bigcap_{S\in\mathscr{R}}\overline{S}$, $\overline{\bigcap_{S\in\mathscr{M}} S}=\bigcup_{S\in\mathscr{M}}\overline{S}$.

Dans ce qui précède, $\mathscr{R}$ est un ensemble dont les éléments sont des parties de E.

1.5. Couples ordonnés et produits cartésiens

Nous continuons par la notion de couple ordonné, essentielle en mathématique, et sa généralisation : les n-listes. Les ensembles n'étant pas ordonnés, la paire $\{a,b\}$ ne peut modéliser le couple ordonné formé par a (en premier) et b (en second). Il faut un peu d'astuce pour *détourner* la notion de paire à cet effet.

Définition 2.8. Couple ordonné

Pour deux ensembles a et b, on appelle couple ordonné de a (en premier) et b (en second) la paire

$$\Big\{\{a\},\{a,b\}\Big\}$$

que l'on note plus simplement (a,b).

✗ Cette définition réalise bien ce que l'on attend d'un couple ordonné. À savoir $(\forall a)$, $(\forall b)$, $(\forall c)$, $(\forall d)$, $\Big((a,b)=(c,d) \iff \big((a=c)\wedge(b=d)\big)\Big)$.

Définition 2.9. Produit cartésien de deux ensembles

Pour deux ensembles quelconques A et B, il existe un ensemble contenant tous les couples (a,b) tels que $a\in A$ et $b\in B$. On le note $A\times B$, produit cartésien de A par B.

On généralise facilement cette définition aux triplets : $(a,b,c):=\big((a,b),c\big)$ et ainsi de suite par récurrence à un nombre fini quelconque de composantes. On définit alors les produits cartésiens $A\times B\times C$ et leurs généralisations. Dans le cas particulier où $A=B$ et $B=C$, on note plus simplement A^2 et A^3 au lieu de $A\times B$ et $A\times B\times C$; on généralise à A^n où n est un entier naturel non nul.

1.6. Axiomes de l'infini et du choix (HP)

L'idée sur laquelle repose l'axiome de l'infini est celle de successeur : pour tout ensemble x, on pose $x^+:=x\cup\{x\}$ (expression qui est bien définie par l'axiome de la paire et de la réunion). Cet ensemble est appelé successeur de x. À partir de cette définition, on peut envisager une construction naturelle de l'ensemble $\mathbb{N}$: $0:=\varnothing$, $1:=0^+$, $2:=1^+$, $3:=2^+$ etc. C'est-à-dire :

$$0:=\varnothing,\ 1:=\big\{0\big\},\ 2:=\big\{0,1\big\},\ 3:=\big\{0,1,2\big\}$$

ZFC VII – Axiome de l'infini

Il existe un ensemble A tel que $0\in A$ et $\forall x,\ x\in A \implies x^+\in A$.

En utilisant cet axiome, on peut formaliser la construction esquissée ci-dessus de l'ensemble $\mathbb{N}$ au moyen des axiomes du modèle ZFC.

Le dernier axiome de la théorie formalise l'idée qu'il est possible de faire le choix simultané d'un élément dans chacun des éléments d'un ensemble E.

ZFC VIII – Axiome du choix

Si E est un ensemble dont les éléments sont non vides, alors il existe un ensemble F contenant exactement un élément de chacun des éléments de E.

Continuons par un exemple plus imagé. Considérons une infinité de paires de chaussures. Pour effectuer le choix d'une chaussure pour chacune des paires, on n'a pas besoin de l'axiome du choix (on peut choisir la chaussure gauche à chaque fois). Dans le cas d'une infinité de paires de chaussettes, on aurait cette fois-ci besoin de l'axiome du choix. Cet axiome subtil peut être ignoré en première lecture d'un cours de Mathématiques.

2. Relations binaires et relations (HP)

La notion de relation binaire est essentielle en Mathématiques. Le lecteur connaît déjà de nombreux symboles de relation tels que $\leqslant$ sur $\mathbb{R}$ ou encore $\equiv$ en arithmétique. La définition suivante généralise cet usage.

Définition 2.10. Relation binaire, relation

Soit E et F deux ensembles.

- On dit que $\mathscr{R}$ est une relation binaire sur $\mathrm{E}\times\mathrm{F}$ si $\mathscr{R}$ est une partie de $\mathrm{E}\times\mathrm{F}$.
- Au lieu d'écrire $(x,y)\in\mathscr{R}$, il est d'usage de noter $x\,\mathscr{R}\,y$, ce qui se lit « x est en relation avec y ».
- On emploie aussi la terminologie de graphe relationnel à propos de $\mathscr{R}$.
- Le domaine et l'image d'une relation binaire $\mathscr{R}$ sur $\mathrm{E}\times\mathrm{F}$ sont définis par :

$$\mathrm{Dom}\,\mathscr{R} := \left\{x\in\mathrm{E}\,;\,\exists y\in\mathrm{F},\,(x,y)\in\mathscr{R}\right\} \quad\text{et}\quad \mathrm{Im}\,\mathscr{R} := \left\{y\in\mathrm{F}\,;\,\exists x\in\mathrm{E},\,(x,y)\in\mathscr{R}\right\}$$

- Lorsque $\mathrm{E}=\mathrm{F}$, on parle simplement relation sur E.

Le plus souvent une relation binaire $\mathscr{R}$ sera définie sans expliciter la partie $\mathscr{R}$ mais plutôt au moyen d'une propriété caractéristique et en définissant à l'occasion un nouveau symbole relationnel.

- Rappelons au lecteur la définition de la relation de congruence modulo 4 sur $\mathbb{Z}$.
  - On dit que deux entiers relatifs x et y sont congrus modulo 4 s'il existe k dans $\mathbb{Z}$ tel que $y=x+4k$, et l'on note $x\equiv y\,[4]$ cette propriété.
  - Ce mode de définition est plus naturel qu'une explicitation du graphe relationnel $\mathscr{R}$ sous-jacent :

$$\mathscr{R} = \left\{(x,y)\in\mathbb{N}^2\,;\,\exists k\in\mathbb{Z},\ y=x+4k\right\}$$

Les quatre propriétés suivantes apparaissent très couramment en Mathématiques.

Définition 2.11. Propriétés des relations binaires

Soit E un ensemble. Une relation $\mathscr{R}$ sur E est dite :

- réflexive si
$$\forall x \in \mathrm{E},\ x\mathscr{R}x$$
- symétrique si
$$\forall (x,y) \in \mathrm{E}^2,\ x\mathscr{R}y \Longrightarrow y\mathscr{R}x$$
- antisymétrique si
$$\forall (x,y) \in \mathrm{E}^2,\ \left(x\mathscr{R}y \wedge y\mathscr{R}x\right) \Longrightarrow x = y$$
- *transitive* si
$$\forall (x,y,z) \in \mathrm{E}^3,\ \left(x\mathscr{R}y \wedge y\mathscr{R}z\right) \Longrightarrow x\mathscr{R}z$$

Nous verrons un peu plus loin que les relations binaires sont aussi au fondement de la notion de fonction.

2.1. Relations d'équivalence

Une relation d'équivalence permet d'identifier des éléments vérifiant une propriété commune. Cela impose la définition suivante :

Définition 2.12. Relations d'équivalence

Soit E un ensemble. On appelle relation d'équivalence sur E toute relation sur E réflexive, symétrique et transitive.

- Par exemple, la relation d'égalité sur un ensemble E quelconque est une relation d'équivalence.
- La relation de congruence modulo 4 sur $\mathbb{Z}$ (ou modulo un entier m quelconque) est une relation d'équivalence.
  - Fixons x, y et z dans $\mathbb{Z}$.
  - On a $x = x + 0$ donc $x \equiv x\,[4]$. D'où la réflexivité de la relation.
  - De plus, $y - x$ est un multiple de 4 *si et seulement si* $x - y$ est un multiple de 4 donc $x = y\,[4] \iff y = x\,[4]$. Ainsi la relation est symétrique.
  - Supposons que $x = y\,[4]$ et $y = z\,[4]$. Soit alors des entiers k et ℓ tels que $y = x + 4k$ et $z = y + 4\ell$. On a $z = x + 4(k+\ell)$ et puisque $k + \ell \in \mathbb{Z}$, on en déduit que $x = z\,[4]$. On en déduit la transitivité de la relation.
- Un petit pas vers les entiers relatifs et les nombres rationnels. Vérifions que la relation définie ci-dessous est une relation d'équivalence sur $\mathbb{N}^2$:

$$\text{Sur } \mathbb{N}^2, \text{ on note } (p,q)\,\mathscr{R}\,(n,m) \text{ si } p+m = q+n$$

  - Soit (p,q), (k,ℓ) et (n,m) dans $\mathbb{N}^2$.
  - Comme $p + q = q + p$, $p,q)\,\mathscr{R}\,(p,q)$. La relation est bien réflexive.
  - Supposons $(p,q)\,\mathscr{R}\,(n,m)$. On a alors $p + m = q + n$ donc $n + q = m + p$ et donc$(n,m)\,\mathscr{R}\,(p,q)$. La relation est bien symétrique.

- ✔ Supposons $(p,q)\,\mathscr{R}\,(n,m)$ et $(n,m)\,\mathscr{R}\,(k,\ell)$. On a alors $p+m=q+n$ et $n+\ell=m+k$. Ainsi
$$p+n+\ell+m=q+n+m+k$$
d'où $p+\ell=q+k$ puis $(p,q)\,\mathscr{R}\,(k,\ell)$. La relation est donc transitive.

Dans ce cadre, on regroupe dans des *classes d'équivalences* les éléments qui sont en relation.

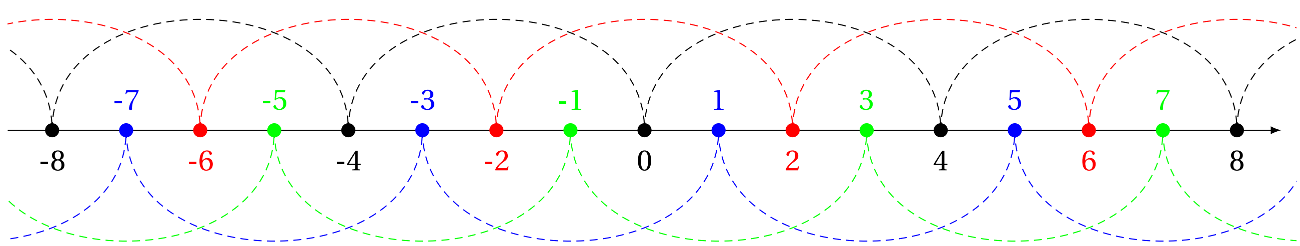
Proposition 2.13. (Classes d'équivalence).

Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Pour tout $x\in \mathrm{E}$, on appelle classe d'équivalence de x le sous-ensemble
$$\overline{x}:=\left\{y\in \mathrm{E}\,;\,x\mathscr{R}y\right\}$$
Les classes d'équivalence forment une partition de E.

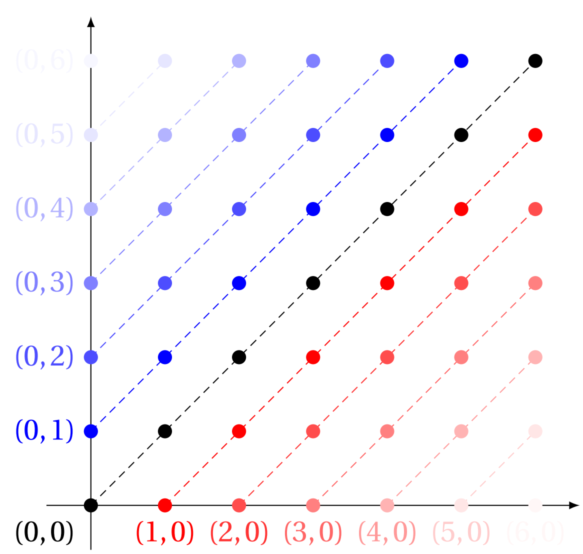
L'ensemble des classes d'équivalence peut être vu comme résultant de *l'identification* (ou encore du recollement) des éléments d'une même classe d'équivalence.

✗ On observera les partitions de $\mathbb{Z}$ et de $\mathbb{N}^2$ correspondant aux relations étudiées ci-dessus dans les figures suivantes.

- ✔ Ci-dessous, une représentation des quatre classes d'équivalences de la relation de congruence modulo 4 dans $\mathbb{Z}$:
$$\overline{0}\,,\ \overline{1}\,,\ \overline{2}\,,\ \overline{3}$$
On a, par exemple, $\overline{1}=\left\{4k+1\,;\,k\in\mathbb{Z}\right\}$.



- ✔ La relation d'équivalence $\mathscr{R}$ sur $\mathbb{N}^2$ (cf. le 2.1), admet une infinité de classes d'équivalences, ce sont les sous-ensembles de $\mathbb{N}^2$ de la forme
$$\overline{(n,0)}\ \text{ ou }\ \overline{(0,n)}\ \text{ avec } n\in\mathbb{N}$$
  - ✦ En effet, deux éléments (p,q) et (x,y) sont en relation *si et seulement si* $q-p=y-x$.
  - ✦ On trouve donc que la classe d'équivalence de (p,q) est l'ensemble des couples d'entiers (x,y) tels que le point de coordonnées (x,y) appartienne à la droite d'équation $y-x=q-p$ (le plan est supposé muni d'un repère orthonormé).



Chaque élément d'une classe d'équivalence est appelé représentant de celle-ci. Afin de bien comprendre une relation d'équivalence, il est souvent intéressant de trouver un représentant remarquable de chacune de ses classes. Comme par exemple $(n, 0)$ et $(0, n)$ pour $n \in \mathbb{N}$ dans le cas de la relation $\mathscr{R}$ ci-dessus.

Définition 2.14. Ensemble quotient d'une relation d'équivalence

Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. L'ensemble des classes d'équivalence de $\mathscr{R}$ est appelé ensemble quotient de E par $\mathscr{R}$ est noté $\mathrm{E}/\mathscr{R}$.

2.2. Relations d'ordre

On cherche ici à généraliser les propriétés de la relation $\leqslant$ sur $\mathbb{R}$.

Définition 2.15. Relations d'ordre

Soit E un ensemble.

- On appelle relation d'ordre sur E toute relation réflexive, antisymétrique et transitive. On note traditionnellement $\preccurlyeq$ une relation d'ordre et on dira que $(\mathrm{E}, \preccurlyeq)$ est un ensemble ordonné pour signifier que E est muni de la relation d'ordre $\preccurlyeq$.
- Une relation d'ordre $\preccurlyeq$ sur E est dite totale lorsque $\forall (x, y) \in \mathrm{E}^2$, $x \preccurlyeq y$ ou $y \preccurlyeq x$. On dit alors que l'ensemble $(\mathrm{E}, \preccurlyeq)$ est totalement ordonné.

Par exemple, pour un ensemble E, la relation d'inclusion $\subset$ est une relation d'ordre sur $\mathscr{P}(\mathrm{E})$. Le lecteur est également familier de la relation d'ordre qui permet de classer les mots de la langue française dans un dictionnaire : l'ordre lexicographique. Les relations d'ordre permettent de généraliser le vocabulaire de la majoration et de la minoration à de nombreux contextes.

Définition 2.16. Majorants et minorants, etc.

Soit $(\mathrm{E}, \preccurlyeq)$ un ensemble ordonné, F une partie non vide de E et $x \in \mathrm{E}$. On dit que

- x est un majorant de F ou encore que x majore F lorsque $\forall f \in \mathrm{F},\ f \preccurlyeq x$,
- x est un minorant de F ou encore que x minore F lorsque $\forall f \in \mathrm{F},\ x \preccurlyeq f$,

Nous continuons par deux définitions essentielles en Analyse.

Définition 2.17. Maximum ou plus grand élément, borne supérieure

Soit $(\mathrm{E}, \preccurlyeq)$ un ensemble ordonné et F une partie non vide de E. On dit que :

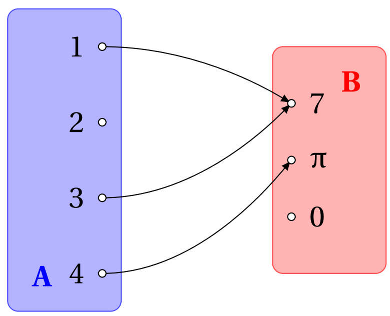
- F admet un plus grand élément (ou encore un maximum) s'il existe un majorant M de F tel que $\mathrm{M} \in \mathrm{F}$. Celui-ci est alors unique : on l'appelle plus grand élément de F (ou encore maximum de F) et on le note $\max \mathrm{F}$.
- F admet une borne supérieure lorsque l'ensemble $\mathscr{M}_{\mathrm{F}}$ des majorants de F est non vide et admet un plus petit élément. Ce dernier est alors unique : on l'appelle borne supérieure de F et on le note $\sup \mathrm{F}$.

On définit de même, sous réserve d'existence, les notions de plus petit élément (ou encore minimum) et borne inférieure de F comme respectivement un minorant de F appartenant à F et le plus grand élément de l'ensemble μ_F des minorants de F. Ils sont uniques et notés $\min F$ et $\inf F$.

- Par exemple, dans le cas de $(\mathbb{R}, \leqslant)$, $[0,1[$ admet un minimum mais pas de maximum, et ce même ensemble admet une borne supérieure.

3. Fonctions et applications

Rappelons l'idée intuitive de fonction f d'un ensemble A dans un ensemble B : à certains éléments x de A (pas tous, seulement ceux du domaine de définition de f) on associe un seul élément de B noté $f(x)$ et appelé son image par f.



On peut se représenter une fonction f de A dans B au moyen d'un diagramme sagittal (cf. la figure ci-contre) : on relie x à $f(x)$ par un arc coiffé d'une flèche pour tout x appartenant au domaine de définition de f. Par exemple, la fonction f du diagramme ci-contre est définie sur l'ensemble $\{1,3,4\}$ par

$$f(1) = f(3) = 7, \ f(4) = \pi$$

Une façon plus abstraite de définir cette fonction f est de donner les associations $x - f(x)$ sous la forme d'un ensemble de couples ordonnés $\big(x, f(x)\big)$:

$$\Big\{(1,7), (3,7), (4,\pi)\Big\}$$

Cette approche a l'avantage de bien se généraliser : on peut appréhender une fonction f de A dans B comme une relation binaire sur $A \times B$ via l'ensemble

$$G := \Big\{\big(x, f(x)\big) \, ; \, x \in A\Big\}$$

qui est bien une partie de $A \times B$, appelée graphe de f. Cette relation binaire G vérifie la propriété suivante :

$$\forall x \in A, \ \forall (y,z) \in B^2, \ \big((x,y) \in G\big) \wedge \big((x,z) \in G\big) \implies y = z$$

C'est ce point de vue qu'adopte la théorie des ensembles pour définir les fonctions comme des relations binaires vérifiant une condition dite de fonctionnalité.

3.1. Définitions et notations usuelles

Définition 2.18. Fonction

Soit A et B deux ensembles.

- Une relation binaire G sur $A \times B$ est dite fonctionnelle si

$$\forall x \in A, \ \forall (y,z) \in B^2, \ \big((x,y) \in G\big) \wedge \big((x,z) \in G\big) \implies y = z$$

- Une fonction f est la donnée d'un triplet $f := (A, B, G)$ où A, B sont des ensembles et G est une relation fonctionnelle sur $A \times B$. L'ensemble G est appelé graphe de la fonction f, le domaine de G est appelé domaine de définition de f ou encore ensemble de définition de f, on le note $\operatorname{Dom} f$.

- Pour $x \in \operatorname{Dom} f$, il existe y dans B tel que $(x, y) \in G$ (par définition du domaine) et cet élément y est unique (car la relation G est fonctionnelle), on le note $f(x)$.
- On a $\operatorname{Im} f = \{y \in B; \exists x \in A,\ (x, y) \in G\} = \{f(x); x \in A\}$.

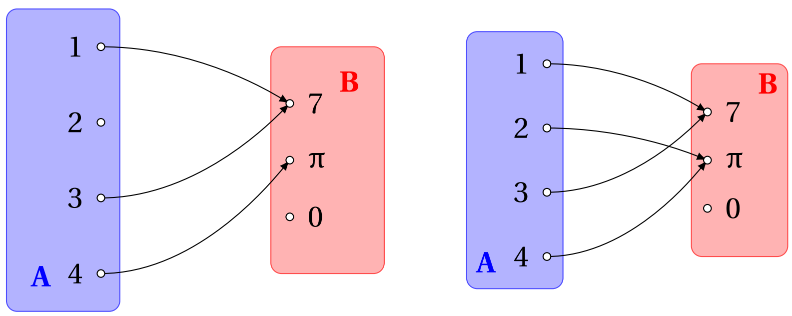
On retrouve ainsi les notations et le vocabulaire usuels sur les fonctions.

Définition 2.18. Applications

Soit A et B deux ensembles.

- On appelle application de A dans B toute fonction f de A dans B telle que $\operatorname{Dom} f = A$.
- Une application de A dans B sera notée $f : A \to B$.

- Par exemple, les diagrammes représentés ci-contre, lus de gauche à droite, représentent respectivement une fonction de A dans B qui n'est pas une application et une application de A dans B.



Fonction Versus Application

En CPGE (et donc au concours), fonction et application sont considérées comme synonymes. On pourra écrire, par exemple, soit $f : A \to B$ une fonction.

Dans la plupart des cas, une fonction (ou une application) est définie de la façon suivante :

$$\begin{aligned} f : A &\longrightarrow B \\ a &\longmapsto \text{expression de } f(a) \text{ au moyen de } a \end{aligned}$$

Dans le cas particulier où la fonction f est à variable et valeurs réelles, une autre représentation s'impose pour mieux la comprendre.

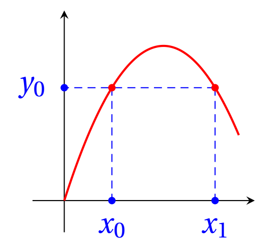
Définition 2.19. Graphe et courbe représentative

Soit $f : A \to B$ avec $A \subset \mathbb{R}$ et $B \subset \mathbb{R}$, et $(O, \mathbf{u}, \mathbf{v})$ un repère du plan. On appelle courbe représentative de f dans ce repère l'ensemble des points de coordonnées $(x, f(x))$ pour $x \in A$.

C'est une représentation géométrique du graphe de f et on emploiera parfois le mot *graphe* au lieu de *courbe représentative*.

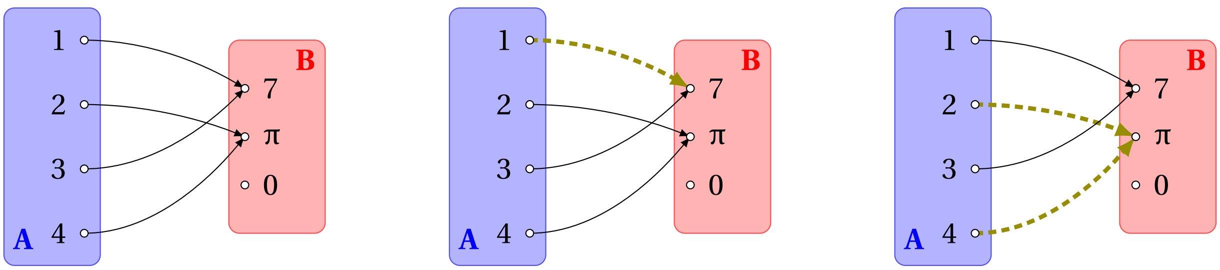
Définition 2.20. Image et antécédent

Soit $f : \mathrm{A} \to \mathrm{B}$ et $(x, y) \in \mathrm{A} \times \mathrm{B}$. Si $f(x) = y$, alors on dit que y est *l'image* de x par f et que x est *un antécédent* de y par f.



Dans la figure ci-contre, $y_0 = f(x_0) = f(x_1)$ donc y_0 est l'image par f de x_0 et x_1, x_0 et x_1 sont des antécédents de y_0 par f.

On reprend l'exemple donné un plus haut.



✘ Dans l'ordre des figures de gauche à droite :

- ✔ La définition de la fonction f, 0 n'a aucun antécédent par f ;
- ✔ comme $f(1) = 7$, 7 est l'image de 1 par f et 1 est un antécédent de 7 par f ;
- ✔ puisque $f(2) = f(4) = \pi$, 2 et 4 sont deux antécédents de π par f ;

Il arrive très couramment de modifier les ensembles de départ et d'arrivée d'une fonction.

Définition 2.21. Restriction et prolongement

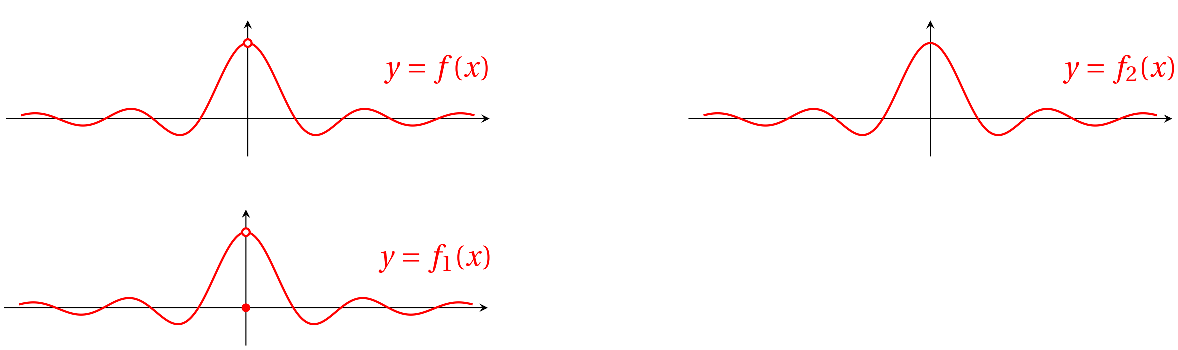
Soit $f : \mathrm{A} \to \mathrm{B}$ une application, et des ensembles B_0, A_0 et A_1 tels que $\mathrm{B} \subset \mathrm{B}_1$ et $\mathrm{A}_0 \subset \mathrm{A} \subset \mathrm{A}_1$.

⇛ Restriction : on appelle restriction de f à A_0 et l'on note $f|_{\mathrm{A}_0}$ l'unique application $g : \mathrm{A}_0 \to \mathrm{B}$ définie par $g(x) := f(x)$ pour tout $x \in \mathrm{A}_0$.

⇛ Co-restriction : dans le cas où $\mathrm{Im}(f) \subset \mathrm{B}_0$, on appelle co-restriction de f à B_0 et l'on note $f|^{\mathrm{B}_0}$ l'unique application $g : \mathrm{A} \to \mathrm{B}_0$ définie par $g(x) = f(x)$ pour tout x dans A.

⇛ Prolongement : on appelle prolongement de f à A_1 toute application $g : \mathrm{A}_1 \to \mathrm{B}_1$ telle que $g|_{\mathrm{A}}^{\mathrm{B}} = f$.

✘ Illustration par le sinus cardinal. Ci-dessus, les graphes du sinus cardinal puis de deux de ses prolongements à $\mathbb{R}$.



✔ Le *sinus cardinal* est la fonction définie par

$$f : \mathbb{R}^* \longrightarrow \mathbb{R}$$
$$x \longmapsto \frac{\sin(x)}{x}$$

✔ Parmi tous les prolongements de f à $\mathbb{R}$, on distingue *le prolongement par continuité*, noté ici f_2, défini par

$$f_2(0) := \lim_{x\to 0} \frac{\sin(x)}{x} = 1$$

Bien qu'un prolongement d'une application f soit une *nouvelle application*, on continue le plus souvent à la noter f.

3.2. Images directes et réciproques

Les images directes et réciproques permettent de décrire des ensembles d'images et d'antécédents.

Définition 2.22. Images directes et réciproques (↯ 2.5)

Soit $f : \mathrm{A} \to \mathrm{B}$ une application.

⇛ *Image directe* : pour $\mathrm{U} \subset \mathrm{A}$, on note $f\langle \mathrm{U} \rangle := \{ f(x) \,;\, x \in \mathrm{U} \}$ (image directe de U par f).

⇛ *Image réciproque* ou encore *pré-image* : pour $\mathrm{V} \subset \mathrm{B}$, on note $f^{-1}\langle \mathrm{V} \rangle := \{ x \in \mathrm{A} \,;\, f(x) \in \mathrm{V} \}$ (image réciproque de V par f ou encore pré-image de V par f).

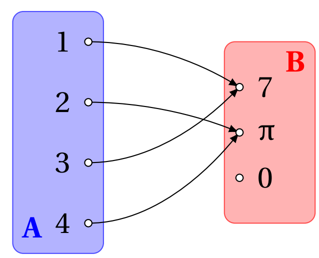
De façon plus imagée, $f\langle \mathrm{U} \rangle$ est l'ensemble des valeurs prises par f sur U.

✘ Pour une application quelconque $f : \mathrm{A} \to \mathrm{B}$, on a donc $\mathrm{Im}\, f = f\langle \mathrm{A} \rangle$.

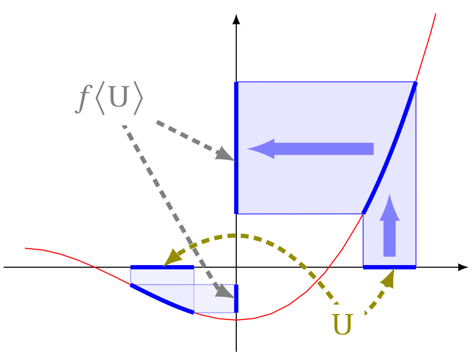
✘ Pour l'application f définie ci-contre :

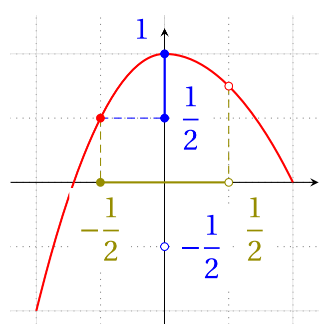
$$f\langle \mathrm{A} \rangle = \mathrm{Im}(f) = \{7, \pi\}\,,\ f\langle \{1,4\} \rangle = \{7,\pi\}\,,\ f^{-1}\langle \{0\} \rangle = \varnothing\,,$$

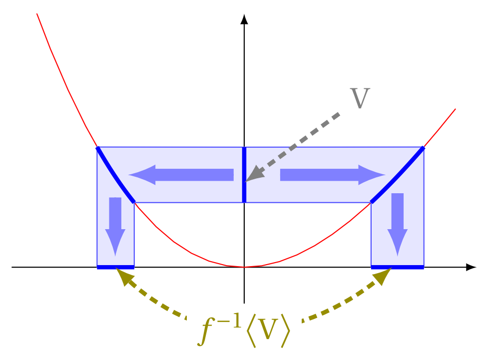
$$f^{-1}\langle \mathrm{B} \rangle = \mathrm{Dom}(f) = \mathrm{A}\,,\ f^{-1}\langle \{\pi\} \rangle = \{2,4\}\,,\ f\langle \{2,4\} \rangle = \{\pi\}$$



✘ Pour tout $y_0 \in \mathrm{B}$, $f^{-1}\langle \{ y_0 \} \rangle$ est l'ensemble des antécédents de y_0 par f.







Nous concluons ce paragraphe par la notion de partie stable, fondamentale en Analyse et en Algèbre.

Définition 2.23. Partie stable par une application

Soit $f : \mathrm{A} \to \mathrm{B}$ une application et S une partie de A. On dit que S est stable par f si $f\langle \mathrm{S} \rangle \subset \mathrm{S}$.

3.3. Ensembles d'applications et composition

Notation 2.24. Ensembles d'applications

Soit A et B deux ensembles. L'ensemble des applications de A dans B est noté B^{A} ou encore $\mathscr{F}(\mathrm{A},\mathrm{B})$.

C'est encore une fois le recours aux axiomes ZFC qui permet de justifier l'existence d'un tel ensemble.

Définition 2.24. Composée

Soit $f : \mathrm{A} \to \mathrm{B}$ et $g : \mathrm{B} \to \mathrm{C}$. L'application définie de A dans C par $x \mapsto g\big(f(x)\big)$ est notée $g \circ f$ et appelée composée de g et f.

✘ La composition n'est pas commutative. En effet, les fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ définies par

$$\forall x \in \mathbb{R},\ f(x) := x+1 \quad \text{et} \quad g(x) := 2x$$

vérifient $f \circ g : x \mapsto 2x+1$ et $g \circ f : x \mapsto 2x+2$.

Proposition 2.25. (Associativité de la composition).

Pour $f : \mathrm{A} \to \mathrm{B}$, $g : \mathrm{B} \to \mathrm{C}$ et $h : \mathrm{C} \to \mathrm{D}$, on a $(h \circ g) \circ f = h \circ (g \circ f)$.

Nous terminons ce paragraphe par l'idée d'itération pour la composition.

Notation 2.26. Itérées d'une fonction (⚡ 2.6)

Pour $f : \mathrm{A} \to \mathrm{B}$ où A est stable par f, on définit par récurrence les itérées f^n par $f^0 = \mathrm{id}_{\mathrm{A}}$ et, pour tout $n \in \mathbb{N}^*$ $f^n = f^{n-1} \circ f$.

Dans le cas où les itérées de f sont bien définies, on déduit de l'associativité de la composition les relations suivantes :

$$\forall (n,m) \in \mathbb{N}^2,\ f^{n+m} = f^n \circ f^m \quad \text{et} \quad \left(f^n\right)^m = f^{nm}$$

Attention, si A n'est pas stable par f, alors il existe $a \in \mathrm{A}$ tel que $f(a) \notin \mathrm{A}$ et $f^2(a)$ n'est donc pas défini !

3.4. Injectivité, surjectivité et bijectivité

La généralisation de la notion de bijectivité à des applications quelconques est très importante.

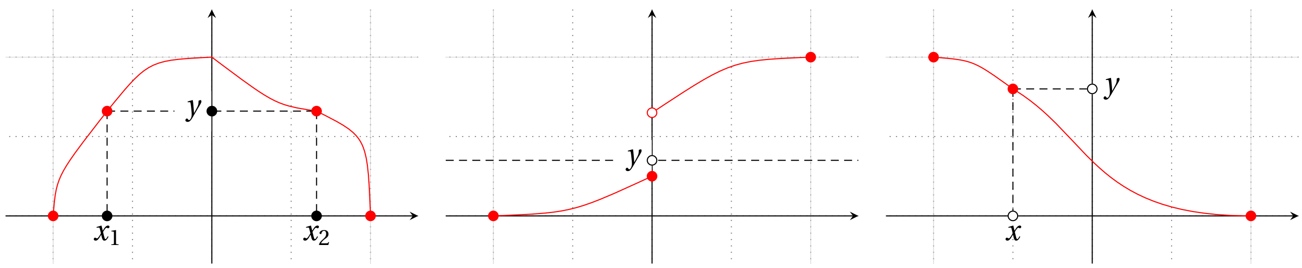
Définition 2.27. Injectivité, surjectivité et bijectivité

Une application $f : \mathrm{A} \to \mathrm{B}$ est dite :

- ⇛ injective si $\forall (x,y) \in \mathrm{A}^2,\ f(x) = f(y) \implies x = y$, i.e. tout élément de B admet au plus un antécédent par f ;
- ⇛ surjective si $\forall y \in \mathrm{B},\ \exists x \in \mathrm{A},\ y = f(x)$, i.e. tout élément de B admet au moins un antécédent par f ;

⇛ bijective si elle est injective et surjective, i.e. tout élément de B admet un unique antécédent par f.

✗ Les figures suivantes illustrent les notions d'injectivité, de surjectivité et de bijectivité pour une application $f:[-1,1]\to[0,1]$.



- ✔ f est non injective (il existe deux éléments distincts x_1 et x_2 de $[-1,1]$ ayant la même image y) et surjective (tout élément de $[0,1]$ admet au moins un antécédent).
- ✔ f est non surjective (il existe un élément y de $[0,1]$ n'ayant pas d'antécédent) et injective (tout élément de $[0,1]$ admet au plus un antécédent).
- ✔ f est bijective (tout élément y de $[0,1]$ admet un unique antécédent x).

Définition 2.28. Réciproque d'une bijection

Soit $f:\mathrm{A}\to\mathrm{B}$ une bijection. On appelle bijection réciproque de f et on note $f^{-1}:\mathrm{B}\to\mathrm{A}$ l'application telle que, pour tout $y\in\mathrm{B}$, $f^{-1}(y)$ est l'unique antécédent de y par f.

Avec les notations de la définition précédente, pour $(x,y)\in\mathrm{A}\times\mathrm{B}$, $\left(f\circ f^{-1}\right)(y)=y$ puisque $f^{-1}(y)$ est un antécédent de y par f et $\left(f^{-1}\circ f\right)(x)=x$ car x est un antécédent de $f(x)$ par f. On a donc $f\circ f^{-1}=\mathrm{id}_\mathrm{F}$ et $f^{-1}\circ f=\mathrm{id}_\mathrm{E}$.

Il est parfois possible de prouver la bijectivité d'une application « *en sortant du chapeau sa bijection réciproque* ». La proposition suivante formalise cette méthode.

Proposition 2.29. Bijectivité et inversibilité pour la composition

Soit $f:\mathrm{A}\to\mathrm{B}$ une application. Les propriétés suivantes sont équivalentes :

a. f est bijective ;

b. il existe $g:\mathrm{B}\to\mathrm{A}$ telle que $f\circ g=\mathrm{id}_\mathrm{B}$ et $g\circ f=\mathrm{id}_\mathrm{A}$.

Si ces conditions sont vérifiées, alors $g=f^{-1}$.

Attention, la condition $g\circ f=\mathrm{id}_\mathrm{E}$ seule ne garantit pas la bijectivité de f.

✗ Considérons par exemple $f:\mathbb{N}\to\mathbb{N}$ définie par $f(n):=n+1$ pour tout entier naturel n.

- ✔ Comme f ne prend par la valeur 0, f n'est pas bijective.

- ✔ Cependant, la fonction $g : \mathbb{N} \to \mathbb{N}$ définie par
$$g(0) := 0 \quad \text{et} \quad \forall n \in \mathbb{N}^*,\ g(n) := n-1$$
vérifie bien $g \circ f = \mathrm{id}_{\mathbb{N}}$.
- ✔ On remarque de plus que g n'est pas bijective car non injective : aucune des deux conditions du b de la proposition précédente ne suffit à conclure *en général* à la bijectivité de f.

Pistes pour établir la bijectivité d'une application

Soit $f : \mathrm{E} \to \mathrm{F}$. Voici plusieurs pistes pour démontrer la bijectivité de f :

- ⇛ Montrer que f est injective et bijective en revenant aux définitions ;
- ⇛ Montrer que, pour tout $y \in \mathrm{F}$, l'équation $f(x) = y$ d'inconnue x a une unique solution dans E (si on sait calculer x en fonction de y, on obtient *en plus* de la bijectivité de f l'expression de sa bijection réciproque f^{-1}) ;
- ⇛ Trouver $g : \mathrm{F} \to \mathrm{E}$ telle que $f \circ g = \mathrm{id}_{\mathrm{F}}$ et $g \circ f = \mathrm{id}_{\mathrm{E}}$, on sait alors que $g = f^{-1}$;
- ⇛ Dans le cas particulier des fonctions définies sur une réunion finie d'intervalles de $\mathbb{R}$ et à valeurs réelles, on dispose de conditions suffisantes de bijectivité, cf. le cours d'analyse (calculus, continuité et bijectivité).
- ⇛ **To be continued...** La liste ne s'arrête pas ici, nous la complèterons dans le cours d'Algèbre linéaire.

En résumé, une preuve de bijectivité va beaucoup dépendre du contexte mathématique.

✘ La fonction $f : x \mapsto \dfrac{x}{1-x}$ réalise une bijection de $[0,1[$ sur $[0,+\infty[$.

- ✔ Soit $y \in \mathbb{R}_+$ et $x \in \mathbb{R} \setminus \{1\}$. On a
$$\begin{aligned} y = \frac{x}{1-x} &\iff (1-x)y = x \\ &\iff (y+1)x = y \\ &\iff x = \frac{y}{y+1} \quad \text{car } y+1 \neq 0 \end{aligned}$$
- ✔ Comme y est positif, la solution $\frac{y}{y+1}$ est bien dans $[0,1[$.
- ✔ Pour tout $y \in \mathbb{R}_+$, 'équation $y = f(x)$ a donc bien une seule solution dans $[0,1[$. La fonction f réalise une bijection de $\mathbb{R}_+$ sur $[0,1[$.
- ✔ On a même, grâce à cette démonstration l'expression de la réciproque $f^{-1} : x \mapsto \frac{y}{y+1}$.

✘ La fonction $f : x \mapsto xe^x$ réalise une bijection de $[-1,+\infty[$ sur $\left[-\frac{1}{e},+\infty\right[$.

- ✔ Après quelques tentatives au brouillon, nous abandonnons la résolution de l'équation $y = f(x)$. Le cours de Terminale nous fournit une autre piste : le théorème de la bijection. La fonction f est continue sur $\mathbb{R}$. Elle est aussi dérivable et
$$\forall x \in [-1,+\infty[,\ f'(x) = (x+1)e^x \geqslant 0$$
et f' ne s'annule qu'en -1. Ainsi f est strictement croissante sur $[-1,+\infty[$. Comme $f(x) \xrightarrow[x\to+\infty]{} +\infty$, on en déduit le tableau de variation suivants :

- ✔ Par le théorème de la bijection, f réalise une bijection de $[-1,+\infty[$ sur $\left[-\frac{1}{e},+\infty\right[$.

✘ La fonction $\phi : f \mapsto \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(1-x) \end{array}$ réalise une bijection de $\mathbb{R}^{[0,1]}$ sur $\mathbb{R}^{[0,1]}$.

- ✔ On va vérifier que $\phi\circ\phi = \mathrm{id}_{\mathrm{E}}$ où $\mathrm{E} := \mathbb{R}^{[0,1]}$.
- ✔ Soit $f \in \mathrm{E}$. Posons $g := \phi(f)$ et $h := \phi(g)$. Pour $x \in [0,1]$, on a

$$h(x) = g(1-x) = f\big(1-(1-x)\big) = f(x)$$

Ains $\phi^2 = \mathrm{id}_{\mathrm{E}}$. L'application ϕ est donc bijective, inverse d'elle-même.

✘ Montrons la bijectivité de $f : \mathbb{N} \to \mathbb{Z}$ par

$$f(n) = \begin{cases} -\dfrac{n}{2} & \text{si } n \text{ est pair} \\[2ex] \dfrac{n+1}{2} & \text{si } n \text{ est impair} \end{cases}$$

- ✔ Démontrons l'injectivité de f. Soit $(n_1,n_2) \in \mathbb{N}^2$ tel que $f(n_1) = f(n_2)$. Comme f est négative sur l'ensemble des entiers pairs et strictement positive sur l'ensemble des entiers impairs, on en déduit que nécessairement n_1 et n_2 sont de même parité.
  - ✦ Cas 1 : n_1 et n_2 sont pairs. On a alors $-\frac{n_1}{2} = -\frac{n_2}{2}$ d'où $n_1 = n_2$.
  - ✦ Cas 1 : n_1 et n_2 sont impairs. On a alors $2n_1+1 = 2n_2+1$ d'où $n_1 = n_2$.
- ✔ Prouvons la surjectivité de f. Soit $n \in \mathbb{Z}$.
  - ✦ Cas 1 : n est négatif. On a $-2n \in \mathbb{N}$ et $f(-2n) = n$.
  - ✦ Cas 2 : n est strictement positif. On a $2n-1 \in \mathbb{N}$ et $f(2n-1) = n$.

  Dans tous les cas, n admet un antécédant par f.
- ✔ Ici aussi, nous pouvons déduire de la démonstration l'expression de la réciproque f^{-1} :

$$f^{-1} : n \mapsto \begin{cases} -2n & \text{si } n \leqslant 0 \\ 2n+1 & \text{si } n > 0 \end{cases}$$

On finit le paragraphe par une propriété importante de stabilité par composition.

Proposition 2.30. Composées d'injections, de surjections, de bijections

Soit $f : \mathrm{A} \to \mathrm{B}$ et $g : \mathrm{B} \to \mathrm{C}$ des applications.

a. Si f et g sont injectives, alors $g\circ f$ est injective ;

b. Si f et g sont surjectives, alors $g\circ f$ est surjective ;

c. Si f et g sont bijectives, alors $g\circ f$ est une bijection et $(g\circ f)^{-1} = f^{-1}\circ g^{-1}$.

d. Si $g\circ f$ est injective, alors f est injective.

e. Si $g\circ f$ est surjective, alors g est surjective.

Nous recommandons au lecteur de clore ce paragraphe par le test (↯ **2.7**)

4. Les ensembles de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$

Une construction exhaustive des ensembles de nombres usuels est hors programme et, à vrai dire, n'est pas essentielle à l'apprenti mathématicien. Il nous semble plus profitable d'insister sur les grandes étapes de la construction et les problématiques sous-jacentes plutôt que détailler les démonstrations pour cette première approche. Les lignes qui suivent ont pour objet principal de sensibiliser le jeune mathématicien à la notion de construction.

Les paragraphes hors programmes sont signalé par les lettres HP dans leur titre. Ils peuvent être omis en première lecture.

4.1. L'ensemble $\mathbb{N}$ des entiers naturels

Au sein de la théorie ZFC, l'existence de l'ensemble $\mathbb{N}$ est une conséquence très directe de l'axiome de l'infini. Nous supposerons l'ensemble des entiers naturels construit et muni de sa relation d'ordre $\leqslant$ bien connue du lecteur ainsi que des opérations + et × usuelles.

L'absence de construction nécessite d'admettre la proposition suivante dite de bon ordre.

Proposition 2.31. (Propriété de bon ordre)

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Cette propriété admet un énoncé dual sur les parties majorées et permet de démontrer le théorème de la récurrence (la proposition b ci-dessous) :

Theoreme 2.32. (Propriétés fondamentales de $\mathbb{N}$).

a. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

b. Soit, pour tout entier naturel n, une assertion $\mathscr{P}(n)$.

$$\text{Si } \mathscr{P}(0) \text{ est vraie, et, } \forall n \in \mathbb{N},\ \mathscr{P}(n) \implies \mathscr{P}(n+1), \text{ alors } \forall n \in \mathbb{N},\ \mathscr{P}(n) \text{ est vraie}$$

Revenons quelques instants à l'existence dans le théorème de la division euclidienne sur $\mathbb{N}$, déjà démontré dans le chapitre précédent par récurrence :

Theoreme 2.33. (de la division euclidienne).

Soit $(a,b) \in \mathbb{N}^2$ avec $b \neq 0$. Il existe un unique couple $(q,r) \in \mathbb{N}^2$ tel que $a = qb + r$ et $0 \leqslant r < b$.

- La propriété de bon ordre permet d'en donner une autre démonstration.
  - Plaçons-nous sous les hypothèses du théorème ci-dessus. Posons

    $$\mathrm{E} := \left\{ x \in \mathbb{N} \,;\, \exists n \in \mathbb{N}\,,\ x = nb \,\text{et}\, x \leqslant a \right\}$$

  - L'ensemble E est une partie non vide de $\mathbb{N}$ puisque $0 \in \mathrm{E}$. De plus, pour $n \in \mathbb{N}$ tel que $n > a$, on a $nb \geqslant n > a$. On en déduit que E est majoré par ab. Ainsi E admet un plus grand élément.
  - Celui est de la forme qb où $q \in \mathbb{N}$. Comme $(q+1)b > qb = \max \mathrm{E}$, on a $(q+1)b \notin \mathrm{E}$ et donc, par définition de E, $(q+1)b > a$. On a donc $qb \leqslant a < (q+1)b$, d'où $0 \leqslant a - qb < b$.
  - Le couple (q,r) où $r := a - qb$ vérifie donc $a = bq + r$ avec $(q,r) \in \mathbb{N}^2$ et $0 \leqslant r < b$.

4.2. Introduction à l'idée de structure algébrique (HP)

Il ne faudrait pas penser qu'il n'existe qu'une seule façon de construire l'ensemble $\mathbb{N}$, l'histoire des sciences en recense plus d'une dizaine. Comment alors assurer la cohérence des Mathématiques si plusieurs définitions de $\mathbb{N}$ coexistent ?

C'est ici qu'intervient l'idée de structure : l'ensemble $\mathbb{N}$ n'est pas tant un ensemble qu'une structure algébrique, i.e. la donnée d'un ensemble muni de deux opérations $+$ et $\times$ vérifiant un ensemble de règles qui ont déjà été rappelées ci-dessus. Par exemple, un ensemble $\mathbb{N}'$ d'éléments $0'$, $1'$, $2'$, etc. muni de deux opérations $\oplus$ et $\otimes$ ayant des tables *analogues* à celles de l'addition et la multiplication de $\mathbb{N}$, est en quelque sorte un copier-coller de $\mathbb{N}$:

$+$	0	1	2	3	$\dots$
0	0	1	2	3	$\dots$
1	1	2	3	4	$\dots$
2	2	3	4	5	$\dots$
3	3	4	5	6	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\times$	0	1	2	3	$\dots$
0	0	0	0	0	$\dots$
1	0	1	2	3	$\dots$
2	0	2	4	6	$\dots$
3	0	3	6	9	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\oplus$	$0'$	$1'$	$2'$	$3'$	$\dots$
$0'$	$0'$	$1'$	$2'$	$3'$	$\dots$
$1'$	$1'$	$2'$	$3'$	$4'$	$\dots$
$2'$	$2'$	$3'$	$4'$	$5'$	$\dots$
$3'$	$3'$	$4'$	$5'$	$6'$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\otimes$	$0'$	$1'$	$2'$	$3'$	$\dots$
$0'$	$0'$	$0'$	$0'$	$0'$	$\dots$
$1'$	$0'$	$1'$	$2'$	$3'$	$\dots$
$2'$	$0'$	$2'$	$4'$	$6'$	$\dots$
$3'$	$0'$	$3'$	$6'$	$9'$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

L'analogie des tables d'addition et de multiplication a pour conséquence que les règles de calcul sont les mêmes dans les triplets $(\mathbb{N},+,\times)$ et $(\mathbb{N}',\oplus,\otimes)$. En particulier, tout théorème ne concernant que les opérations vrai dans l'un des triplets sera automatiquement vrai dans l'autre. On peut donc développer des arithmétiques analogues dans chacun de ces triplets.

Pour formaliser l'idée précédente *d'analogie des tables d'addition et de multiplication*, on utilise en Algèbre la notion d'isomorphisme : tout ensemble muni de deux opérations $(\mathrm{E},\oplus,\otimes)$ est isomorphe à $(\mathbb{N},+,\times)$ s'il existe une bijection $\phi : \mathbb{N} \to \mathrm{E}$ telle que :

$$\forall (n,m) \in \mathbb{N}^2,\ \phi(n+m) = \phi(n) \oplus \phi(m) \quad \text{et} \quad \phi(n \times m) = \phi(n) \otimes \phi(m)$$

Un tel triplet $(\mathrm{E},\oplus,\otimes)$ est aussi un modèle acceptable de l'ensemble des entiers naturels tel qu'on l'imagine. Quand dans un théorème, on fait référence à l'ensemble $(\mathbb{N},+,\times)$ des entiers naturels, ce triplet désigne en fait tout triplet $(\mathrm{E},\oplus,\otimes)$ isomorphe à celui dont nous avons esquissé la construction dans le paragraphe précédent : le choix de la construction de $\mathbb{N}$ perd alors de son importance.

Cette notion d'isomorphisme peut bien-sûr s'étendre aux ensembles usuels $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ en l'adaptant à chaque fois en conséquence, et peut-être généraliser à d'autre type d'ensemble.

4.3. Constructions de $\mathbb{Z}$ et $\mathbb{Q}$ à partir de $\mathbb{N}$ (HP)

Comment définir les entiers relatifs à partir des entiers naturels ? Une idée consiste à utiliser la relation d'équivalence $\mathscr{R}$ sur $\mathbb{N}^2$ introduite à l'exemple 2.1 de la page 12. Le relatif k est représenté par tous les couples d'entiers naturels (x,y) tels que $y-x=k$.

Ensemble $\mathbb{Z}$ des entiers relatifs

On note $\mathbb{Z} := \mathbb{N}^2 / \mathscr{R}$ où $\mathscr{R}$ est la relation d'équivalence définie sur $\mathbb{N}^2$ par

$$(a_1,b_1)\,\mathscr{R}\,(a_2,b_2) \ \text{ si } \ b_1+a_2 = b_2+a_1$$

On pose alors
$$\overline{(p_1,q_1)}+\overline{(p_2,q_2)} := \overline{(p_1+p_2,q_1+q_2)}$$
Cette définition nécessite cependant une justification : pour définir la somme de deux classes, on utilise des représentants *particuliers* de celles-ci – les couples (p_1,q_1) et (p_2,q_2)–, il faut donc vérifier que la classe de (p_1+p_2,q_1+q_2) ne dépend par du choix de ces deux représentants. Supposons $\overline{(p_1,q_1)}=\overline{(p'_1,q'_1)}$ et $\overline{(p_2,q_2)}=\overline{(p'_2,q'_2)}$. On a alors $q'_1-p'_1=q_1-p_1$ et $q'_2-p'_2=q_2-p_2$ d'où $q'_1+q'_2-p'_1-p'_2=q_1+q_2-p_1-p_2$, ce qui justifie bien l'égalité
$$\overline{(p_1+p_2,q_1+q_2)}=\overline{(p'_1+p'_2,q'_1+q'_2)}$$
On définit de même (avec une justification analogue que nous ne détaillerons pas) le produit :
$$\overline{(p_1,q_1)}\times\overline{(p_2,q_2)} := \overline{(p_1\times p_2,q_1\times q_2)}$$
Effectuons une petite pause dans cette construction. Pour tout entier naturel n, notons
$$\phi(n) := \overline{(n,0)}\ \ ,\ \ -\overline{(n,0)} := \overline{(0,n)}\ \text{ et }\ -\overline{(0,n)} := \overline{(n,0)}$$
Posons enfin $\mathbb{N}' := \phi(\mathbb{N})$. On démontre facilement que ϕ réalise une bijection de $\mathbb{N}$ sur $\mathbb{N}'$ vérifiant
$$\forall (n,m)\in\mathbb{N}^2,\ \phi(n+m)=\phi(n)+\phi(m)\ \text{ et }\ \phi(n\times m)=\phi(n)\times\phi(m)$$
Le sous-ensemble $\mathbb{N}'$ de $\mathbb{Z}$ ainsi défini est donc une copie de $\mathbb{N}$ dans $\mathbb{Z}$. En identifiant n et $\phi(n)$, on peut donc considérer que $\mathbb{N}\subset\mathbb{Z}$. On obtient alors que
$$\mathbb{Z}=\mathbb{N}\cup\left\{-n\,;\,n\in\mathbb{N}\right\}$$
On démontre facilement que les opérations + et × sur $\mathbb{Z}$ sont associatives, commutatives, admettent pour éléments neutres respectifs 0 et 1, et que la multiplication est distributive sur l'addition. On notera $p-q$ l'expression $p+(-q)$. Enfin, on défini la relation $\leqslant$ sur $\mathbb{Z}$ par :
$$\text{Pour } (n,m)\in\mathbb{Z}^2,\text{ on dit que } n\leqslant m \text{ si } m-n\in\mathbb{N}$$
On démontre facilement qu'il s'agit d'une relation d'ordre pour laquelle toute partie non vide de $\mathbb{Z}$ minorée (resp. majorée) admet un plus petit élément (resp. un plus grand élément).

Theoreme 2.34. (de la division euclidienne).

Soit $(a,b)\in\mathbb{Z}^2$ avec $b\neq 0$. Il existe un unique couple $(q,r)\in\mathbb{Z}^2$ tel que $a=qb+r$ et $0\leqslant r<|b|$.

Avec ces notations, les entiers naturels q et r sont appelés *quotient* et *reste* dans la division euclidienne de a par b, et $b\,|\,a \iff$ le reste dans la division euclidienne de a par b est nul[4].

Passons à présent à la construction de $\mathbb{Q}$. Comment définir des fractions d'entiers à partir d'entiers ? Une première idée est de définir un rationnel par le couple numérateur-dénominateur, en imposant un numérateur dans $\mathbb{Z}$ et un dénominateur dans $\mathbb{N}^*$. Le problème est que les couples $(1,2)$ et $(2,4)$ bien que distincts correspondent au même rationnel. L'idée est d'identifier tous les couples représentant le même rationnel au moyen de la notion de la relation d'équivalence et d'ensemble quotient. On remarque que les couples (a_1,b_1) et (a_2,b_2) représentent le même rationnel *si et seulement si* $a_1b_2=a_2b_1$.

4. On rappelle que a divise b (ou que a est un diviseur de b ou encore que b est un multiple de a) s'il existe $c\in\mathbb{Z}$ tel que $b=ac$. On note cette propriété $a\,|\,b$ (le contraire est noté $a\nmid b$).

Ensemble $\mathbb{Q}$ des nombres rationnels

On pose $\mathbb{Q} := \mathbb{Z}\times\mathbb{N}^* / \mathscr{R}$ où $\mathscr{R}$ est la relation d'équivalence définie sur $\mathbb{Z}\times\mathbb{N}^*$ par

$$(a_1, b_1)\,\mathscr{R}\,(a_2, b_2) \ \text{ si } \ a_1 b_2 = a_2 b_1$$

La classe d'équivalence de (a, b), élément de $\mathbb{Z}\times\mathbb{N}^*$, est notée $\dfrac{a}{b}$, de sorte que $\mathbb{Q} = \left\{\dfrac{a}{b}\,;\,(a,b)\in\mathbb{Z}\times\mathbb{N}^*\right\}$. On retrouve alors les relations bien connues :

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$$

qui traduisent le fait que les couples $(1,2)$, $(2,4)$, $(3,6)$, etc. sont des représentants de la même classe d'équivalence. On définit ensuite les opérations usuelles sur $\mathbb{Q}$ par :

$$\forall (a_1, b_1)\in\mathbb{Z}\times\mathbb{N}^*,\ \forall (a_2, b_2)\in\mathbb{Z}\times\mathbb{N}^*,\ \frac{a_1}{b_1} + \frac{a_2}{b_2} := \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \quad \text{et} \quad \frac{a_1}{b_1}\times\frac{a_2}{b_2} := \frac{a_1 a_2}{b_1 b_2}$$

Comme dans le cas de $\mathbb{Z}$, ces définitions doivent être justifiées en vérifiant à chaque fois que l'expression figurant à droite du symbole = est indépendant des représentants choisis des deux classes d'équivalence. Nous passerons ce point plus fastidieux que difficile. La définition de la relation $\leqslant$ se fait en deux temps[5] : pour $\frac{a}{b}\in\mathbb{Q}$, on note $-\frac{a}{b} := \frac{-a}{b}$ puis, pour tout $(r_1, r_2)\in\mathbb{Q}^2$, on pose $r_2 - r_1 := r_2 + (-r_1)$; on définit ensuite la positivité :

$$\text{Pour } \tfrac{a}{b}\in\mathbb{Q}, \text{ on dit que } \tfrac{a}{b}\geqslant 0 \text{ si } a\geqslant 0$$

Pour $(r_1, r_2)\in\mathbb{Q}^2$, on dit que $r_1\leqslant r_2$ si $r_2 - r_1\geqslant 0$. Il s'agit d'une relation d'ordre sur $\mathbb{Q}$. Un isomorphisme permet de « trouver » un exemplaire de $\mathbb{Z}$ dans $\mathbb{Q}$. Notons

$$\mathbb{Z}' := \left\{\frac{n}{1}\,;\,n\in\mathbb{Z}\right\} \ \text{ et } \ \phi : \mathbb{Z}\to\mathbb{Z}' \ \text{ défini par } \forall n\in\mathbb{Z},\ \phi(n) := \frac{n}{1}$$

On démontre facilement que l'application ϕ est un isomorphisme de $(\mathbb{Z}, +, \times)$ dans $(\mathbb{Z}', +, \times)$.

Rappelons que tout rationnel admet une unique forme irréductible, ce qui permet de simplifier les calculs dans $\mathbb{Q}$ et fournit un représentant naturel à chaque classe d'équivalence :

Forme irréductible d'un rationnel

Tout nombre rationnel r s'écrit de manière unique sous la forme

$$r = \frac{a}{b}, \text{ où } (a,b)\in\mathbb{Z}\times\mathbb{N}^* \text{ vérifie que } a \text{ et } b \text{ n'ont pas de diviseurs communs dans } \mathbb{Z} \text{ autres que } \pm 1$$

Cette écriture est appelée forme irréductible de r. On rappelle que pour calculer la somme de deux nombres rationnels, on commence par les écrire sous forme irréductible puis on les *met au même dénominateur* (qui est le plus petit multiple commun de leurs dénominateurs) :

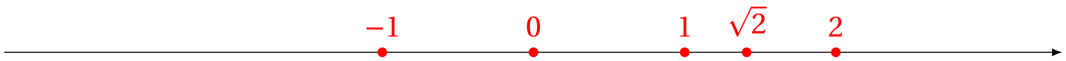
$$\frac{17}{35} + \frac{13}{21} = \frac{17}{5\times 7} + \frac{13}{3\times 7} = \frac{3\times 17}{3\times 5\times 7} + \frac{5\times 13}{3\times 5\times 7} = \frac{116}{3\times 5\times 7}$$

5. Encore une fois, ces définitions nécessiteraient une vérification puisqu'elles font intervenir le choix d'un représentant de la classe d'équivalence définissant un rationnel.

4.4. Un mot à propos de $\mathbb{R}$ et $\mathbb{C}$

La construction de $\mathbb{R}$ à partir de $\mathbb{Q}$ peut s'effectuer en utilisant la même technique de passage au quotient[6]. Mais elle s'avère plus délicate à mettre en place et peu naturelle pour un débutant en Mathématiques. Il est raisonnable d'atteindre le niveau d'un bon L3, et notamment d'être rompu à la topologie élémentaire et l'analyse réelle, avant d'aborder cette construction de $\mathbb{R}$.

Il est intéressant de se représenter mentalement l'ensemble des nombres réels comme une droite graduée :



Le chapitre AN 1 sera en entier consacré à l'ensemble des nombres réels, nous nous contenterons pour l'instant du résultat bien connu suivant[7] :

Proposition 2.35. (Irrationnalité de racine de deux).

Le nombre $\sqrt{2}$ est irrationnel.

La construction de $\mathbb{C}$ à partir de $\mathbb{R}$ ne pose aucune difficulté particulière, elle est même plus facile que celles de $\mathbb{Z}$ et $\mathbb{Q}$, essentiellement parce qu'elle s'appuie sur l'interprétation géométrique des nombres complexes. Le nombre complexe $x+iy$ (où x et y sont réels) peut être vu comme le couple de réels (x,y) et il suffit se souvenir des opérations sur les nombres complexes pour aboutir à une construction de $(\mathbb{C},+,\times)$. On pose $\mathbb{C}:=\mathbb{R}^2$ et l'on définit :

$$\forall (x,y)\in\mathbb{C},\ \forall (a,b)\in\mathbb{C},\ (x,y)+(a,b) := (x+a,y+b) \ \text{ et } \ (x,y)\times(a,b) := (xa-yb,xb+ya)$$

L'application $x\mapsto(x,0)$ est un isomorphisme de $\mathbb{R}$ sur $\mathbb{R}\times\{0\}$ qui permet d'identifier un réel x au couple $(x,0)$. Pour $(x,y)\in\mathbb{C}$, on a donc

$$(x,y) = (x,0)+(0,1)\times(y,0) = x+iy$$

en posant $i:=(0,1)$. De plus $i^2=(0,1)\times(0,1)=(-1,0)=-1$. On vérifie ensuite toutes les propriétés usuelles de l'ensemble $(\mathbb{C},+,\times)$, nous les étudierons en détail dans le chapitre ALG 3 qui leur sera en grande partie dédié.

5. Familles et suites

Les suites sont des applications définies sur $\mathbb{N}$.

Définition 2.36. Suites à valeurs dans A

Soit A un ensemble.

- ⇛ On appelle suite à valeurs dans A toute fonction $u:\mathbb{N}\to\mathrm{A}$.
- ⇛ Notation séquentielle : plutôt que $u(n)$, on note u_n pour une suite u à valeurs dans A et $n\in\mathbb{N}$; on écrit aussi $u=(u_n)_{n\in\mathbb{N}}$.

6. Il existe de nombreuses constructions, parmi lesquelles celle des coupures de Dedekind.
7. En l'absence de construction, nous admettrons pour l'instant la définition de $\sqrt{2}$: il s'agit de l'unique réel positif α tel que $\alpha^2=2$.

⇛ L'ensemble des suites à valeurs dans A est donc $A^{\mathbb{N}}$.

En mathématiques, on a parfois besoin de manipuler des indices qui ne sont pas entiers. Par exemple, si E est un ensemble fini de réels, la somme des éléments de E peut s'écrire de deux manières

$$\sum_{x\in E} x \quad \text{et} \quad \sum_{i=1}^{n} x_i$$

où $E := \{x_1, \ldots, x_n\}$. La première écriture est plus économique que la seconde dans le sens où elle ne nécessite pas de numéroter les éléments de E.

La notion de famille indexée généralise celle de suite à des indices non nécessairement entiers.

Définition 2.37. Familles d'éléments de A indexées par I

Soit A et I des ensembles.

⇛ On appelle famille à valeurs dans A indexée par I toute fonction $a : I \to A$.

⇛ Plutôt que $a(i)$, on note a_i pour une famille a à valeurs dans A indexée par I et $i \in I$; on écrit aussi $a = (a_i)_{i\in I}$.

⇛ L'ensemble des familles à valeurs dans A indexées par I est donc A^I.

On peut généraliser les opérations d'intersection et de réunion aux éléments d'une famille d'ensembles.

Définition 2.38. Réunion et intersection sur une famille d'ensembles

Soit $(A_i)_{i\in I}$ une famille d'ensembles indexée par un ensemble I non vide. On pose

$$\bigcup_{i\in I} A_i := \left\{x \,;\, \exists i \in I,\, x \in A_i\right\} \quad \text{et} \quad \bigcap_{i\in I} A_i := \left\{x \,;\, \forall i \in I,\, x \in A_i\right\}$$

Dans le cas où les les A_i sont deux à deux disjoints[8], on note $\bigsqcup_{i\in I} A_i$ la réunion des A_i.

Dans le cas où $I = \varnothing$, on peut définir la réunion des A_i par le vide car la propriété $\exists i \in I,\ x \in A_i$ est fausse. En revanche, on ne peut définir dans l'absolu l'intersection[9].

8. C'est-à-dire $\forall (i,j) \in I^2,\ i \neq j \implies A_i \cap A_j = \varnothing$.
9. Mais si tous les A_i sont des parties d'un même ensemble E, on peut poser $\bigcap_{i\in I} A_i = E$ car la propriété $\forall i \in I,\ x \in A_i$ est vraie pour tout $x \in E$. Mais ceci est très anecdotique.

6. Tests

2.1.

Vrai ou faux ?

a. $\{0\} \in \{0,1\}$; **b.** $\{0\} \subset \{0,1\}$; **c.** $\{0,1\} \subset \{0,1\}$.

2.2.

Écrire en extension et en compréhension l'ensemble E des entiers relatifs x vérifiant les deux inégalités $|x| < 5$ et $|2x-1| \leqslant 3$.

2.3.

Vrai ou faux ?

a. $\Big\{1, \{0\}\Big\} \cap \{0\} \neq \varnothing$; **b.** $\Big\{1, \{0\}\Big\} \cap \Big\{\{0\}\Big\} = \Big\{\{0\}\Big\}$; **c.** $\Big\{1, \{0\}\Big\} \cap \Big\{\{1\}\Big\} = \Big\{1\Big\}$.

2.4.

L'ensemble $\mathscr{M} := \Big\{\{0,1\}, \Big\{\{0\}\Big\}\Big\}$ est une partition de $\mathrm{E} := \Big\{0, 1, \{0\}\Big\}$: Vrai ou faux ?

2.5.

Soit $f : \mathrm{A} \to \mathrm{B}$. Que vaut $f^{-1}\langle \mathrm{B} \rangle$?

2.6.

Soit $f : \mathbb{R} \to \mathbb{R}$, $a \in \mathbb{R}$ et $(u_n)_{n\in\mathbb{N}}$ la suite définie par

$$u_0 := a \quad \text{et} \quad \forall n \in \mathbb{N} \quad , \quad u_{n+1} = f(u_n)$$

Exprimer, pour $n \in \mathbb{N}$, u_n en fonction de f^n.

2.7.

On peut simplifier, à gauche par une injection, à droite par une surjection.

a. Soit $g : \mathrm{F} \to \mathrm{G}$ injective, $f_1 : \mathrm{E} \to \mathrm{F}$ et $f_2 : \mathrm{E} \to \mathrm{F}$ tels que $g \circ f_1 = g \circ f_2$. Montrer que $f_1 = f_2$.

b. Soit $f : \mathrm{E} \to \mathrm{F}$ surjective, $g_1 : \mathrm{F} \to \mathrm{G}$ et $g_2 : \mathrm{F} \to \mathrm{G}$ tels que $g_1 \circ f = g_2 \circ f$. Montrer que $g_1 = g_2$.

7. Solutions

2.1.

a. Faux : l'ensemble $\{0\}$ n'est pas *un élément* de $\{0,1\}$ (les éléments de cet ensembles sont 0 et 1).

b. Vrai : $\{0\}$ est un sous-ensemble de $\{0,1\}$ puisque $0 \in \{0,1\}$.

c. Vrai : tout ensemble est inclus dans lui-même.

2.2.

La définition en compréhension est

$$E := \left\{x \in \mathbb{Z} ; |x| < 5 \text{ et } |2x-1| \leqslant 3\right\}$$

On trouve facilement que $E = \left\{-1,0,1,2\right\}$.

2.3.

a. Faux : $\left\{1,\{0\}\right\} \cap \{0\} = \varnothing$ car $0 \notin \left\{1,\{0\}\right\}$.

b. Vrai car $\{0\} \in \left\{1,\{0\}\right\}$.

c. Faux car $\{1\} \not\subset \left\{1,\{0\}\right\}$.

2.4.

Vrai car les deux éléments de $\mathscr{M}$ sont non vides, disjoints et leur réunion vaut E :

$$\{0,1\} \cup \left\{\{0\}\right\} = \left\{0,1,\{0\}\right\}$$

2.5.

On a $f^{-1}\langle B \rangle = A$ car, pour $a \in A$, $f(a) \in B$.

2.6.

On a $u_0 = a = f^0(a)$, $u_1 = f(a)$ puis

$$u_2 = f(u_1) = f^2(a)$$

et, par une récurrence facile, $u_n = f^n(a)$ pour tout $n \in \mathbb{N}$.

2.7.

a. Supposons $g \circ f_1 = g \circ f_2$.

⇛ On remarque que f_1 et f_2 ont même ensemble de départ et d'arrivée.

⇛ Soit $x \in E$. Comme $g\big(f_1(x)\big) = g\big(f_2(x)\big)$, on a $f_1(x) = f_2(x)$ par injectivité de g. Ainsi $f_1 = f_2$.

b. Supposons $g_1 \circ f = g_2 \circ f$.

⇛ On remarque que g_1 et g_2 ont même ensemble de départ et d'arrivée.

⇛ Soit $y \in F$. Par surjectivité de f, il existe $x \in E$ tel que $y = f(x)$. Comme

$$g_1\big(f(x)\big) = g_2\big(f(x)\big)$$

on a $g_1(y) = g_2(y)$. Ainsi $g_1 = g_2$.