Université Claude Bernard Lyon 1
L1 de Mathématiques : Algèbre
Année 2013–2014

Ensembles, applications

En guise d'introduction

Le jeu mathématique est addictif, et ce depuis très longtemps. Même au sens moderne, on y joue avec sensiblement les mêmes règles depuis au moins deux mille cinq cents ans – depuis la Grèce classique, Euclide, Thalès ou Pythagore. Mais les règles ont toujours été laissées un peu dans le flou : pour s'en convaincre, on peut constater que les « définitions » du Livre I des *Éléments d'Euclide* ne définissent pas grand-chose.
En fait, on sait au moins depuis les travaux de David Hilbert [1] au tournant du XX^e siècle qu'il manque un certain nombre d'axiomes pour pouvoir faire des déductions irréprochables. Les mathématiciens de cette époque, dont Hilbert est une figure de proue, essaient d'asseoir les mathématiques sur des bases logiques irréprochables, qui pourraient en particulier démontrer la cohérence des mathématiques (de sorte à être sûr de pouvoir continuer à jouer). Mais la tâche est difficile et conduit à la crise des fondements. Produisant une variante du paradoxe du menteur [2], Bertrand Russell met en évidence vers 1901 qu'une théorie naïve des ensembles conduit à des paradoxes insurmontables. Ernst Zermelo et publie en 1908 une liste d'axiomes complétée par Abraham Frankel pour donner le paradigme dans lequel sont énoncées (presque) toutes les mathématiques contemporaines.
Plus tard, en 1929, Kurt Gödel publie le théorème de complétude qui parachève en quelque sorte la mise au point des règles du jeu : il donne un sens à *vrai* et explique en quoi les notions de *vrai* et de *démontrable* se correspondent. C'est un grand succès. Malheureusement, en 1931, le même Gödel prouve le théorème d'incomplétude, plus célèbre que le précédent mais sans doute moins utile, qui exprime qu'à l'intérieur d'une théorie non triviale, il n'est pas possible de prouver la cohérence de la théorie – c'est une autre variation du paradoxe du menteur.
Cette histoire est fascinante mais hors de nos objectifs. Dans ce chapitre, nous allons simplement voir les notations nécessaires pour manipuler les ensembles et les applications (fonctions) et quelques résultats abstraits au passage.

I Ensembles

1° Notions de base

a) Pas de définition. Non, il n'est pas question de donner une définition de ce qu'est un ensemble. Les manipulations qui suivent correspondent à l'idée intuitive d'une collection d'objets [3]. Tout repose sur la relation d'appartenance.
Si l'on a un objet x et un ensemble E, on forme une assertion notée « $x \in E$ », que l'on lit « x appartient à E », « x est un élément de E » ou « E contient x » ; elle est vraie ou fausse.
En termes vagues, un ensemble contient des éléments [4]. Mieux : un ensemble est caractérisé par les éléments qu'il contient. Autrement dit, deux ensembles sont égaux si et seulement s'ils ont les mêmes éléments. En symboles : si E et F sont deux ensembles, on a l'équivalence :

$$E = F \iff \big(\forall x,\ x \in E \Leftrightarrow\ x \in F\big).$$

1. David Hilbert, 1862-1943, mathématicien allemand que l'on retrouvera en deuxième année avec les espaces hilbertiens.
2. Attribuer une valeur de vérité à la phrase « Cette phrase est fausse. » conduit à une contradiction. Russel a constaté que s'il existe un ensemble de tous les ensembles, on peut alors définir l'ensemble F des ensembles qui ne se contiennent pas ; il est impossible de répondre à la question : est-ce que F se contient ?
3. D'un autre côté, comme toutes les mathématiques s'expriment, *in fine*, en termes de théorie des ensembles, on peut considérer que tout objet mathématique est un ensemble, de sorte que le mot *ensemble* devient à peu près synonyme de *symbole*, ce qui le vide de son sens.
4. Le déterminant *des* est indéfini : un ensemble peut contenir un seul élément, voire aucun.

b) Deux façons de décrire un ensemble :

— *en extension*, c'est-à-dire par la liste exhaustive de ses éléments, que l'on écrit entre accolades ; voici des exemples :
  — l'ensemble $\{1, 4, 5\}$ est l'ensemble dont les éléments sont exactement 1, 4 et 5 et aucun autre :
$$\forall x, \quad x \in \{1, 4, 5\} \;\Leftrightarrow\; (x = 1 \text{ ou } x = 4 \text{ ou } x = 5);$$
  — on peut définir $B = \big\{\{1\}, \{0, 2\}, \{1, 3\}\big\}$; c'est un ensemble qui contient trois éléments, lesquels sont eux-mêmes des ensembles ;

  il importe de noter que dans la notation, l'ordre des éléments n'importe pas et la répétition est autorisée ; ainsi, on a : $\{1, 2\} = \{2, 1\} = \{1, 2, 1\}$ et $\{1, 1\} = \{1\}$;

— *en compréhension* : on caractérise les éléments d'un ensemble par une propriété ; plus précisément, on se donne un ensemble E et une assertion $P(x)$ dans laquelle x est une variable parlante et qui a un sens lorsque l'on remplace cette variable par un élément quelconque de E ; les éléments x de E pour lesquels $P(x)$ est vraie forment un ensemble que l'on note[5] :
$$\big\{x \in E,\ P(x)\big\};$$
  voici quelques exemples :
  — l'ensemble $\{x \in \mathbb{R},\ 1 \leq x \leq 2\}$ est l'intervalle $[1, 2]$;
  — on a : $\mathbb{N} = \{x \in \mathbb{Z},\ n \geq 0\}$;
  — anticipant sur la suite pour la notation $\mathbb{R}^2$ et les couples, $\big\{(x, y) \in \mathbb{R}^2,\ x^2 + y^2 = 1\big\}$ désigne un cercle dans $\mathbb{R}^2$.

c) L'ensemble vide

Il existe un ensemble appelé *ensemble vide* et noté $\emptyset$ ou $\{\}$ qui ne contient aucun élément : pour tout objet x, l'assertion « $x \in \emptyset$ » est fausse.

Notons qu'il n'existe qu'un seul ensemble vide : si E est un ensemble vide, alors pour tout x, l'assertion « $x \in E$ » est fausse donc on a l'équivalence $x \in E \Leftrightarrow x \in \emptyset$, de sorte que $E = \emptyset$.

d) Cardinal

On ne va pas donner de définition précise de la notion de cardinal (mais il en existe). On se contentera d'utiliser le mot et la notation $\mathrm{card}(E)$ pour désigner le « nombre d'éléments » d'un ensemble E. En première approximation, c'est un entier naturel ou l'infini. Par exemple : $\mathrm{card}(\emptyset) = 0$; $\mathrm{card}\big(\{1, 4, 5\}\big) = 3$; $\mathrm{card}(\mathbb{N}) = \infty$.

2° Inclusion et parties

a) Inclusion

Définition. Soient E et F deux ensembles. On dit que F *est inclus dans* E ou que E *contient* F et on écrit $F \subset E$ si tout élément de F appartient à E, c'est-à-dire :
$$\forall x,\ x \in F \;\Rightarrow\; x \in E.$$

On dit encore que F est une *partie* de E.

On voit que la relation d'inclusion $\subset$ est un phénomène d'implication.

b) Ensemble des parties

Un axiome assure que pour tout ensemble E, les ensembles inclus dans E forment un ensemble appelé *ensemble des parties* de E et noté généralement $\mathscr{P}(E)$ (ou parfois 2^E).

Exemple. On a : $\mathscr{P}(\emptyset) = \{\emptyset\}$; $\mathscr{P}\big(\{1\}\big) = \big\{\emptyset, \{1\}\big\}$; $\mathscr{P}\big(\{1, 2\}\big) = \big\{\emptyset, \{1\}, \{2\}, \{1, 2\}\big\}$.

Exercice (infaisable pour l'instant...). Pour n entier naturel, on a : $\mathrm{card}\,\mathscr{P}\big(\{1, \ldots, n\}\big) = 2^n$.

5. On trouve aussi les notations $\big\{x \in E :\ P(x)\big\}$ et $\big\{x \in E \mid P(x)\big\}$; le séparateur n'importe pas.

3° Opérations sur les ensembles

a) Produit cartésien

Étant donnés deux objets x et y, on forme le *couple* (x, y). Informellement, c'est une liste ordonnée dont le premier élément est x et le deuxième y. Ainsi, on a : $(x, y) \neq (y, x)$ si $x \neq y$ et $(x, x) \neq (x)$ (et $(x, x) \neq x$). (C'est donc très différent des paires : comparer avec les égalités : $\{x, y\} = \{y, x\}$ quels que soient x et y et $\{x, x\} = \{x\}$.)
Plus formellement (ne pas retenir ce paragraphe), on peut définir le couple (x, y) comme l'ensemble $\big\{\{x\}, \{x, y\}\big\}$. Cela constitue un codage des couples en termes que l'on a déjà rencontrés. On peut vérifier que la donnée de $\big\{\{x\}, \{x, y\}\big\}$ permet de retrouver, en les distinguant, x et y.
Étant donnés deux ensembles E et F, les couples (x, y) formés par un élément x de E et un élément y de F forment un ensemble appelé *produit cartésien* de E par F et noté : $E \times F$.

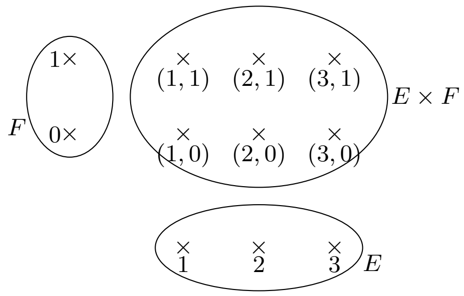


FIGURE 1 – Un exemple de produit cartésien : $E = \{1, 2, 3\}$, $F = \{0, 1\}$

Exercice (infaisable pour l'instant). Soient E et F deux ensembles finis. Justifier l'égalité[6] : $\operatorname{card}(E \times F) = \operatorname{card}(E) \times \operatorname{card}(F)$.

b) Réunion et intersection

Définition. Soient E et F deux ensembles. On appelle *réunion* de E et F et on note $E \cup F$ (lire : « E union F ») l'ensemble dont les éléments sont ceux qui appartiennent à E ou à F :

$$\forall x, \quad x \in E \cup F \;\Leftrightarrow\; (x \in E \text{ ou } x \in F).$$

On appelle *intersection* de E et F et on note $E \cap F$ (lire : « E inter F ») l'ensemble dont les éléments sont ceux qui appartiennent à E et à F :

$$\forall x, \quad x \in E \cap F \;\Leftrightarrow\; (x \in E \text{ et } x \in F).$$

Proposition. *Soient E, F et G trois ensembles. On a :*

(i) $E \cup F = F \cup E$;
(ii) $E \cap F = F \cap E$;
(iii) $(E \cup F) \cup G = E \cup (F \cup G)$;
(iv) $(E \cap F) \cap G = E \cap (F \cap G)$;
(v) $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$;
(vi) $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

Démonstration. Exercice facile qui utilise des propriétés analogues des connecteurs « et » et « ou ». □

6. Le signe $\times$ du membre de gauche est le produit cartésien des deux ensembles ; celui du membre de droite est le produit des entiers.

c) Différence et complémentaire

Définition. Soient E et F deux ensembles. On appelle *différence* de E et F et on note $E \setminus F$ (lire : « E privé de F ») l'ensemble dont les éléments sont les éléments de E qui n'appartiennent pas à F :

$$\forall x, \quad x \in E \setminus F \;\Leftrightarrow\; (x \in E \text{ et } x \notin F).$$

Proposition. *Soient E, F et G trois ensembles. On a :*
(i) $E \setminus (F \cup G) = (E \setminus F) \cap (E \setminus G)$ *;*
(ii) $E \setminus (F \cap G) = (E \setminus F) \cup (E \setminus G)$ *;*

Démonstration. Exercice qui utilise des propriétés des connecteurs « et », « ou » et « non ».□

Définition. Soit E un ensemble et soit A une partie de E. On appelle *complémentaire de A dans E* l'ensemble $E \setminus A$. On le note parfois ${}^cA$ ou $\complement_E A$.

Mise en garde. *La notion de complémentaire n'a pas de sens sans un ensemble de référence E. Par exemple, soit $A = \{1,2,3\}$. Si l'on considère A comme une partie de $\{0,1,2,3,4\}$, le complémentaire de A est $\{0,4\}$. Mais si l'on considère A comme une partie de $\mathbb{N}$, son complémentaire est $\{0,4,5,6,\dots\}$.*

On peut reformuler la proposition précédente dans le cas de deux parties d'un même ensemble.

Proposition. *Soient E un ensemble et soient A et B deux parties de E. On a :*
(i) ${}^c(A \cup B) = {}^cA \cap {}^cB$ *;*
(ii) ${}^c(A \cap B) = {}^cA \cup {}^cB$.

Remarque. Tous les connecteurs du chapitre sur la logique ont une traduction pour les ensembles. Voici la correspondance (on fixe un ensemble E, deux parties A et B de E et enfin x dans E) :

logique		ensembles	
implication	$x \in A \Rightarrow x \in B$	inclusion	$A \subset B$
disjonction	$x \in A$ ou $x \in B$	réunion	$x \in A \cup B$
conjonction	$x \in A$ et $x \in B$	intersection	$x \in A \cap B$
négation	non$(x \in A)$	complémentaire	$x \in E \setminus A$

4° Quelques cardinaux

a) Cardinal de la réunion

Vu que nous n'avons pas de définition raisonnable du cardinal, nous prendrons pour acquis le fait suivant.

Fait. *Soient E et F deux ensembles finis disjoints,* i.e. *tels que $E \cap F = \emptyset$. Alors :*

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F).$$

Proposition. *Soient E et F deux ensembles finis quelconques. Alors :*

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F).$$

Démonstration. Soit $E' = E \setminus (E \cap F)$. On vérifie que l'on a : $E \cup F = E' \cup F$ et $E' \cap F = \emptyset$. En appliquant le fait ci-dessus à E' et F, on trouve donc :

$$\text{card}(E \cup F) = \text{card}(E' \cup F) = \text{card}(E') + \text{card}(F).$$

De plus, on vérifie les égalités : $E = E' \cup (E \cap F)$ et $E' \cap (E \cap F) = \emptyset$. En appliquant le fait ci-dessus à E' et $E \cap F$, on trouve alors :

$$\text{card}(E) = \text{card}\big(E' \cup (E \cap F)\big) = \text{card}(E') + \text{card}(E \cap F).$$

La proposition résulte de ces deux égalités.□

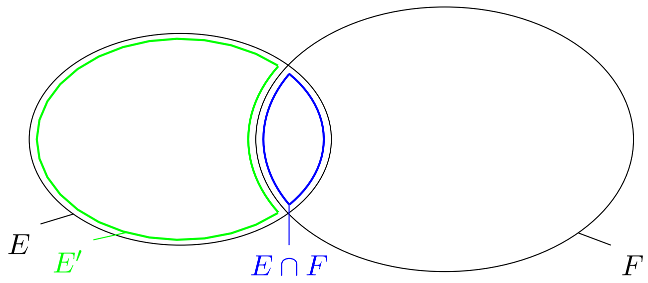


FIGURE 2 – Décomposition d'une réunion en parties disjointes

b) Cardinal du produit

Proposition. *Soient E et F deux ensembles finis. Alors :*

$$\mathrm{card}(E \times F) = \mathrm{card}(E) \times \mathrm{card}(F).$$

Démonstration. On procède par récurrence sur $\mathrm{card}(E)$. Pour n entier naturel, soit H_n l'assertion : pour tout ensemble E de cardinal n et tout ensemble fini F, on a : $\mathrm{card}(E \times F) = n \times \mathrm{card}(F)$.
Prouvons H_0. Soit E un ensemble de cardinal 0, c'est-à-dire que E est vide. Pour tout ensemble F, le produit $\emptyset \times F$ est vide car il n'existe aucun couple de la forme (x, y) avec $x \in \emptyset$ et $y \in F$. Ainsi, on a bien : $0 = \mathrm{card}(\emptyset \times F) = 0 \times \mathrm{card}(F)$.
Pour l'hérédité, on va avoir besoin d'utiliser H_1 donc il faut la prouver à part. Soit E un ensemble de cardinal 1, notons x_0 l'unique élément de E. Soit F un ensemble (fini). Il y a autant [7] de couples de la forme (x_0, y) avec $y \in F$ que d'éléments y dans F. On a donc : $\mathrm{card}(E \times F) = \mathrm{card}(F) = 1 \times \mathrm{card}(F)$, ce qui prouve H_1.
Soit n un entier naturel, supposons que H_n soit vraie. Soit E un ensemble de cardinal $n+1$ et soit x_0 un élément de E. On note $E' = E \setminus \{x_0\}$, de sorte que E est la réunion disjointe de $\{x_0\}$ et de E'. Soit alors F un ensemble fini. On vérifie que $E \times F$ est la réunion disjointe de $\{x_0\} \times F$ et de $E' \times F$: en effet, un couple (x, y) avec $x \in E$ et $y \in F$ appartient à $\{x_0\} \times F$ si $x = x_0$, à $E' \times F$ si $x \neq x_0$, mais pas aux deux simultanément. D'après la proposition précédente, on a : $n + 1 = \mathrm{card}(E) = \mathrm{card}\big(\{x_0\}\big) + \mathrm{card}(E') = 1 + \mathrm{card}(E')$, si bien que $\mathrm{card}(E') = n$, et :

$$\begin{aligned}
\mathrm{card}(E \times F) &= \mathrm{card}\Big(\big(\{x_0\} \times F\big) \cup \big(E' \times F\big)\Big) \\
&= \mathrm{card}\big(\{x_0\} \times F\big) + \mathrm{card}(E' \times F) \\
&= \mathrm{card}(F) + n \times \mathrm{card}(F),
\end{aligned}$$

où la dernière égalité résulte de H_1 et de H_n. D'où l'hérédité, et l'on conclut par récurrence. □

II Applications

Dans ce cours, les mots *fonction* et *application* seront utilisés de façon interchangeable. La nuance que l'on peut faire est expliquée dans une remarque plus bas.

1° Définition

a) Plusieurs idées de ce qu'est une fonction

7. Plus formellement, on dira plus tard que l'application $F \to \{x_0\} \times F$, $y \mapsto (x_0, y)$ est une bijection.

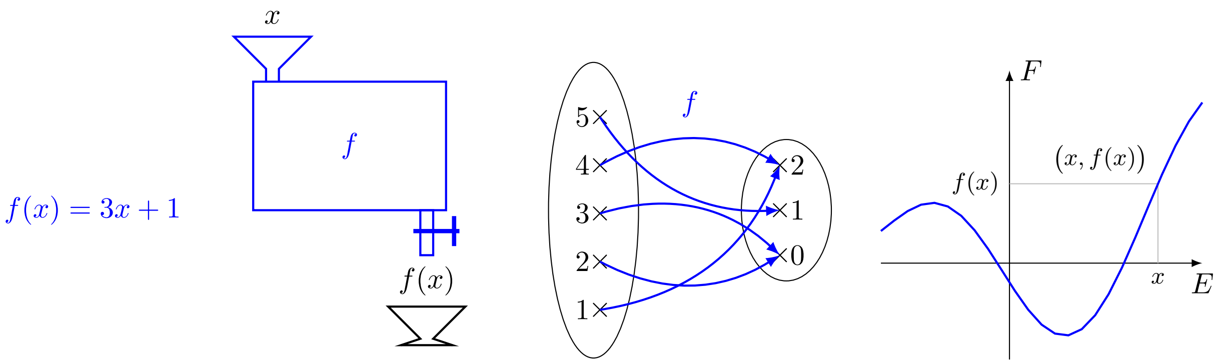


FIGURE 3 – Quatre images d'une fonction : (a) comme formule (insuffisant) ; (b) comme « machine » (très informel) ; (c) par un diagramme sagittal ; (d) par son graphe

(a) L'idée naïve de fonction est liée à celle de *formule* : par exemple, $y = 3x + 1$; on prend une « grandeur » x, on exprime une autre « grandeur » y par une formule qui dépend de x. Cette idée est insuffisante : une formule ne précise pas où vivent les variables qui la composent ni où vit le résultat obtenu ; de plus, des fonctions bien connues comme le sinus ou la racine carrée ne semblent pas être définies par une « formule », du moins pas comparable à $3x+1$.

(b) La deuxième idée est liée à celle de transformation : une fonction f est comme une machine [8] qui prend comme ingrédient [9] x et qui renvoie un résultat [10] $f(x)$ (figure 3 (b)). « Le » doit être un élément d'un ensemble bien défini, disons E « le » $f(x)$ doit être un élément d'un autre ensemble bien défini, disons F. Intéressant mais pas du tout formalisé...

(c) La troisième idée est liée à celle de correspondance : la machine, le processus précédent permet d'associer à un élément x de E un élément $f(x)$ de F. On peut représenter la situation par un *diagramme saggital* [11]. On peut considérer qu'une fonction est la donnée de toutes les flèches, lesquelles sont essentiellement des couples de la forme $\big(x, f(x)\big)$.

(d) Cela conduit naturellement à la quatrième idée : le *graphe* d'une fonction est justement l'ensemble des couples $\big(x, f(x)\big)$. Si la variable x et son image $f(x)$ sont réels et si l'on identifie un plan muni d'un repère à l'ensemble $\mathbb{R}^2$ des couples de réels, c'est bien la représentation d'une fonction habituelle depuis le lycée. C'est cette dernière idée qui se formalise convenablement et se visualise le mieux.

b) Formalisation

Définition. Une *fonction* ou *application* f est définie par :
- un *ensemble de départ* E ;
- un *ensemble d'arrivée* F ;
- la donnée, pour tout élément x de E, d'un élément appelé *image de x par f* et noté $f(x)$.

Le *graphe* de la application f est la partie du produit cartésien $E \times F$ formée des couples $\big(x, f(x)\big)$; autrement dit, un couple (x, y) de $E \times F$ appartient au graphe de f si et seulement si l'on a : $y = f(x)$; encore autrement dit, x étant fixé dans E, parmi les couples (x, y) de $E \times F$ qui ont pour abscisse x, un seul appartient au graphe de f : c'est $\big(x, f(x)\big)$.

Remarque formaliste. [12] Les ultras qui trouvent le troisième point de la définition précédente

8. Image très naïve : un presse-agrume.
9. Filons la métaphore : un agrume.
10. Refilons la métaphore (mais à qui ?) : le jus !
11. De même que le Sagittaire qui a reçu l'arc d'Artémis, un diagramme sagittal est plein de flèches.
12. Ce type de remarques peut être sauté en première lecture. Voire en deuxième lecture.

un peu vague pourront préférer cette version. Une application est un triplet $f = (E, F, \Gamma)$ où E et F sont deux ensembles et où Γ est une partie du produit $E \times F$ telle que pour tout élément x de E, il existe un unique élément y de F tel que (x, y) appartient à Γ (en symboles : $\forall x \in E,\ \exists! y \in F,\ (x, y) \in \Gamma$) ; cet unique élément y est l'image de x par f, c'est lui que l'on note $f(x)$.

NOTATION. La locution « Soit $f : E \to F$. » abrège : « Soit f une application ayant pour ensemble de départ E et pour ensemble d'arrivée F. » On dit aussi : « Soit f une fonction de E dans F. » Lorsque l'on décrit l'image d'un élément quelconque x de E, on écrit [13] :

$$f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \qquad \text{ou} \qquad f : E \longrightarrow F, \quad x \longmapsto f(x).$$

Exemples.

1. La situation la plus fréquentée depuis le lycée est celle où l'ensemble de départ est (une partie de) $\mathbb{R}$ et l'ensemble d'arrivée est $\mathbb{R}$. Cela donne lieu, par exemple, aux applications $f_1 : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto \sqrt{x}$ ou $f_2 : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin(x)$ ou encore $f_3 : \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x + 1$.
2. Nuance : il faut distinguer les applications
$$f_1 : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{x} \end{array} \qquad \text{et} \qquad f_2 : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & \sqrt{x} \end{array}$$
car elles n'ont pas le même ensemble d'arrivée ; NB : selon la notion développée plus bas, f_1 n'est pas bijective, alors que f_2 l'est.
3. Une *suite réelle* n'est autre qu'une application de $\mathbb{N}$ dans $\mathbb{R}$. Dans la notation usuelle $u = (u_n)_{n \in \mathbb{N}}$, l'image d'un entier n est le n-ième terme u_n.
4. Soit E un ensemble quelconque : l'*identité*, notée Id_E ou Id, est l'application de E dans E qui, à tout élément x de E, associe x.

Mise en garde. *Il importe de comprendre au plus vite, pour une application f de E dans F :*
- *que tout élément x de l'ensemble de départ a* exactement une *image $f(x)$;*
- *à faire la différence entre*
  - *le symbole f, qui désigne une application – la « machine », le « processus » qui associe à un élément x de E un élément $f(x)$ de F, un objet complexe –*
  - *et le symbole $f(x)$, qui n'a pas de sens si l'on ne sait pas qui est x et qui désigne un élément de F si x est précisé par le contexte ;*
- *à faire la différence entre la flèche $\to$, qui s'utilise entre l'ensemble de départ et l'ensemble d'arrivée, et la flèche avec empennage $\mapsto$, qui s'utilise entre un élément de l'ensemble de départ et son image.*

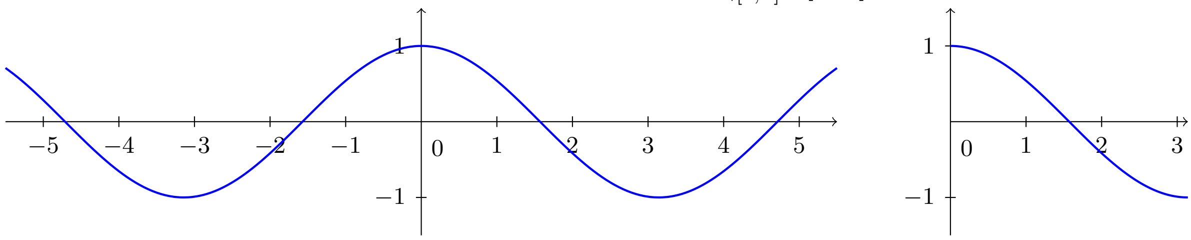
Remarque formaliste. Ici, on utilisera les mots *application* et *fonction* comme s'ils étaient synonymes. On aurait pu ajouter la nuance suivante. Pour une application, un élément de l'ensemble de départ E possède *exactement une* image par f. Pour une fonction, un élément de l'ensemble de départ E possède *au plus une* image par f ; en termes du graphe Γ : pour x dans E, il peut arriver qu'il n'y ait aucun élément y de F tel que $(x, y) \in \Gamma$; mais si y et y' sont deux éléments de F tels que $(x, y) \in \Gamma$ et $(x, y') \in \Gamma$, alors $y = y'$.

13. À la place de « $f(x)$ », on écrit généralement une formule qui définit l'image de x par f. Voir les exemples.

c) Restriction

Définition. Soit $f : E \to F$ une application et soit E' une partie de E. On peut alors définir la *restriction* de f à E' comme l'application $f|_{E'} : E' \to F$, $x \mapsto f(x)$.
Sens : l'ensemble de départ est E' ; l'image par $f|_{E'}$ d'un élément x de E' est $f(x)$. Informellement, on oublie les éléments de $E \setminus E'$. Le graphe de $f|_{E'}$ est $\big\{(x, y) \in E' \times F,\ y = f(x)\big\}$.

Exemple. Graphes de $\cos : \mathbb{R} \to \mathbb{R}$ et de sa restriction $\cos|_{[0,\pi]} : [0, \pi] \to \mathbb{R}$.



Remarque formaliste. Soit $f : E \to F$ et soit $F' \subset F$. On suppose que l'image de tout élément de E appartient à F'. On pourrait définir la *corestriction* de f à F' comme l'application $f : E \to F'$, $x \mapsto f(x)$. Mais on peut survivre sans ce mot.

d) Composition

Définition. Soient $f : E \to F'$ et $g : F \to G$ deux applications. On suppose que F, l'ensemble d'arrivée de f, est contenu dans F l'ensemble de départ de g. Pour tout élément x de E, on peut donc calculer l'image de $f(x)$ par g, notée : $g\big(f(x)\big)$. La *composée* de f et g est l'application notée $g \circ f$ définie par :

$$\begin{array}{rccc} g \circ f : & E & \longrightarrow & G \\ & x & \longmapsto & g\big(f(x)\big). \end{array}$$

Voici un diagramme :

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] & F \arrow[r, "g"] & G \end{tikzcd}$$

$$\begin{array}{l} x \longmapsto f(x) \\ \qquad\quad y \longmapsto g(y) \\ x \longmapsto g \circ f(x) \end{array}$$

Mise en garde. *La notation est déplaisante : pour x donné dans E, on applique d'abord f, puis g, alors que l'on écrit d'abord g, puis f dans « $g \circ f$ ». Cela serait évité si l'on écrivait de droite à gauche ou*[14]*, $(x)f$ à la place de $f(x)$. Mais il faut faire avec.*
Pourtant, il faut vraiment faire la différence entre $g \circ f$ et $f \circ g$. Dans la situation de la définition, $g \circ f$ est bien définie mais, a priori*, $f \circ g$ ne l'est pas. Et même si elle l'est, elle n'est* a priori *pas égale à $g \circ f$.*

Exemples. Voici deux exemples pour illustrer la mise en garde.

1. Soient $f : \mathbb{R}^+ \to \mathbb{R}$ l'application définie par $f(x) = \sqrt{x}$ pour tout x de $\mathbb{R}^+$ et $g : \mathbb{R} \to \mathbb{R}$ l'application définie par $g(y) = 3y + 1$ pour tout y de $\mathbb{R}$. Alors, pour tout réel x, on a :

$$g \circ f(x) = g\big(f(x)\big) = 3f(x) + 1 = 3\sqrt{x} + 1.$$

14. Un peu comme dans les langages de programmation orientés objets. En Python par exemple, si `x` est un objet pour lequel une fonction `f` est définie, l'instruction `x.f()` renvoie l'image de `x` par `f`. On écrit des choses comme `x.f().g()` au lieu de $g\big(f(x)\big)$.

En revanche, $f \circ g$ n'est pas une application. En effet, pour tout réel x strictement inférieur à $-1/3$, on a : $g(x) < 0$, de sorte que $g(x)$ n'appartient pas à l'ensemble de départ de f et que $f\big(g(x)\big)$ n'est pas défini.

2. Soient $h : \mathbb{R} \to \mathbb{R}$, $x \mapsto 2x + 5$ et $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x + 1$. Comme l'ensemble de départ de h (resp. g) est l'ensemble d'arrivée de g (resp. h), la composée $g \circ h$ (resp. $h \circ g$) est bien définie. Cependant, on a, pour x réel :

$$g \circ h(x) = 3h(x)+1 = 3(2x+5)+1 = 6x+16 \text{ et } h \circ g(x) = 2g(x)+5 = 2(3x+1)+5 = 6x+7.$$

Ainsi, dans cet exemple, $g \circ h(x)$ est différent de $h \circ g(x)$ pour tout x.

Remarque formaliste. En notant Γ_f et Γ_g les graphes de f et g, le graphe de $g \circ f$ est :

$$\Gamma_{g \circ f} = \big\{(x, z) \in E \times G \;\big|\; \exists y \in F,\ (x, y) \in \Gamma_f \text{ et } (y, z) \in \Gamma_g\big\}.$$

Lemme. *La composition des fonctions est associative : soient $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois fonctions, alors les deux applications $(h \circ g) \circ f : E \to H$ et $h \circ (g \circ f) : E \to H$ sont égales.*

Remarque formaliste. Pour un énoncé un peu plus général, on aurait pu prendre des applications $f : E \to F'$, $g : F \to G'$ et $h : G \to H$ avec $F' \subset F$ et $G' \subset G$.

Démonstration. Soit $x \in E$. Comme F, l'ensemble d'arrivée de f, est l'ensemble de départ de g, la composée $g \circ f$ est bien définie et, pour x dans E, on a : $(g \circ f)(x) = g\big(f(x)\big)$. Comme G, l'ensemble d'arrivée de $g \circ f$, est l'ensemble de départ de h, la composée $h \circ (g \circ f)$ est bien définie et, pour x dans E, on a :

$$\big(h \circ (g \circ f)\big)(x) = h\big(g \circ f(x)\big) = h\Big(g\big(f(x)\big)\Big).$$

De même que $h \circ g : F \to G$ est bien définie et, pour y dans F, on a : $h \circ g(y) = h\big(g(y)\big)$. Mais pour x dans E, l'image $f(x)$ appartient à F, l'ensemble de départ de $h \circ g$, et on a de plus :

$$\big((h \circ g) \circ f\big)(x) = (h \circ g)\big(f(x)\big) = h\Big(g\big(f(x)\big)\Big).$$

Les deux applications $(h \circ g) \circ f : E \to H$ et $h \circ (g \circ f) : E \to H$ ont mêmes ensembles de départ et d'arrivée et tout élément x de E a la même image par chacune, donc elles sont égales. $\square$

2° Injections et surjections

a) Notion d'antécédent

Définition. Soit $f : E \to F$ une application. Soit y un élément de l'ensemble d'arrivée F. On appelle *antécédent* de y par f tout élément x de l'ensemble de départ E dont l'image est y – en symboles : un antécédent de y est n'importe quel $x \in E$ tel que $y = f(x)$.

Pour $x \in E$ et $y \in F$, les phrases suivantes sont donc synonymes :
- y est l'image de x par f ;
- x est un antécédent de y par f ;
- $y = f(x)$.

Mise en garde. *Étant donnée une application $f : E \to F$,*
— *on parle de l'image d'un élément de E et c'est un élément de F ;*
— *on parle d'un antécédent d'un élément de F et c'est un élément de E.*

Dans les phrases précédentes, bien noter la différence entre l'article défini dans « l'image » et l'article indéfini dans « un antécédent ». En effet, tout élément de E possède un image unique mais un élément de F peut avoir zéro, un ou plusieurs antécédents (voire une infinité).

Exemple. Soit $f : \mathbb{R} \to \mathbb{R}$ l'application dont le graphe est représenté dans la figure 4. Alors :
- le réel $7/2$ possède exactement un antécédent, x_4 ;
- le réel $1/2$ possède exactement trois antécédents, x_1, x_2, x_3 ;
- le réel 3 n'a pas d'antécédent.

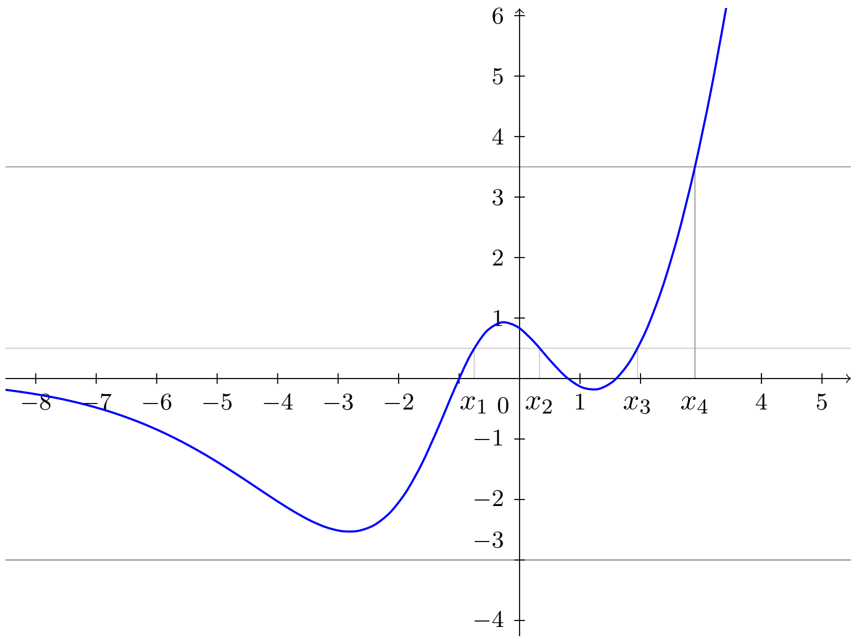


FIGURE 4 – Un exemple de fonction (non injective, non surjective)

b) Injections

Définition. Soit $f : E \to F$ une application. On dit que f est *injective* ou que c'est une *injection* si tout élément de l'ensemble d'arrivée F possède au plus un antécédent. Autrement dit, si deux éléments ont la même image, ils sont égaux :

$$\forall x \in E,\ \forall x' \in E,\ f(x) = f(x') \ \Rightarrow\ x = x'.$$

Exercice. Vérifier que la négation de l'injectivité s'écrit :

$$\exists x \in E,\ \exists x' \in E,\ f(x) = f(x') \text{ et } x \neq x'.$$

Autrement dit, pour prouver qu'un application n'est pas injective, il s'agit de trouver deux éléments distincts de l'ensemble de départ qui ont la même image.

Graphiquement, l'injectivité se teste ainsi : toute droite horizontale coupe le graphe de la fonction en un point au plus SSI la fonction est injective.

Exemples.
- L'application de la figure 4 n'est pas injective car $1/2$ a plusieurs antécédents.
- L'application $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ n'est pas injective puisque $f(-3) = f(3)$.
- L'application $g : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto x^2$ est injective puisque si $0 \leq x < x'$, on a : $x^2 < x'^2$ (ah bon ? et alors ? justifier !).

Remarque. On a d'ores et déjà deux types de méthodes pour montrer qu'une application $f : E \to F$ est injective :

- on fixe x et x' dans E tels que $f(x) = f(x')$, on travaille et on prouve que $x = x'$;
- on fixe y dans F et on suppose que x est un antécédent de y ; on exprime x en fonction de y : cela entraîne l'injectivité de f (pourquoi ?).

Voici deux exemples pour illustrer la deuxième méthode.

Exemple. Soit $\mathrm{sh} : \mathbb{R} \to \mathbb{R}$, $x \mapsto (e^x - e^{-x})/2$. Pour montrer que sh est injective, on fixe y dans $\mathbb{R}$ et on suppose que x est un antécédent de y. On a alors :

$$y = \mathrm{sh}(x) \;\Leftrightarrow\; \frac{e^x - e^{-x}}{2} = y \;\Leftrightarrow\; e^{2x} - 2y\,e^x - 1 = 0 \;\Leftrightarrow e^x = y \pm \sqrt{y^2+1}.$$

Mais on sait que e^x est strictement positif et on vérifie que $y - \sqrt{y^2+1} < 0$. Par suite, on a nécessairement : $x = \ln\bigl(y + \sqrt{y^2+1}\bigr)$, ce qui entraîne l'injectivité. Mais c'est un peu triché car cela définit la fonction réciproque de sh (voir plus loin).

Exemple. Soit $f : \mathbb{R}^2 \to \mathbb{R}^3$, $(x_1, x_2) \mapsto (-3x_1 + x_2, -3x_1 - x_2, x_1 + x_2)$. Montrons que f est injective. Soit $y = (y_1, y_2, y_3) \in \mathbb{R}^3$ et soit $x = (x_1, x_2)$ un antécédent de y. On a :

$$\begin{aligned} y = f(x) &\iff (-3x_1 + x_2, -3x_1 - x_2, x_1 + x_2) = (y_1, y_2, y_3) \\ &\iff \begin{cases} -3x_1 + x_2 = y_1 \\ -3x_1 - x_2 = y_2 \\ x_1 + x_2 = y_3 \end{cases} \\ &\iff \begin{cases} -6x_1 = y_1 + y_2 \\ -3x_1 - x_2 = y_2 \\ x_1 + x_2 = y_3. \end{cases} \end{aligned}$$

On a donc nécessairement : $x_1 = -(y_1 + y_2)/6$ et $x_2 = y_3 - x_1$, ce qui prouve l'unicité de x. (Attention, certains éléments y de $\mathbb{R}^3$ n'ont pas d'antécédent. Lesquels en ont, au fait ?)

c) Surjections

Définition. Soit $f : E \to F$ une application. On dit que f est *surjective* ou que c'est une *surjection* si tout élément de l'ensemble d'arrivée F possède au moins un antécédent – en symboles :

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

Pour prouver qu'un application n'est pas surjective, il s'agit de trouver un élément de l'ensemble d'arrivée qui n'a pas d'antécédent. En symboles, la négation de la surjectivité s'écrit :

$$\exists y \in E,\ \forall x \in E,\ y \neq f(x).$$

Graphiquement, la surjectivité se teste ainsi : toute droite horizontale coupe le graphe de la fonction en un point au moins SSI la fonction est surjective.

Exemples.
- L'application de la figure 4 n'est pas surjective puisque -3 n'a pas d'antécédent.
- L'application $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ n'est pas surjective puisque -1 n'a pas d'antécédent.
- L'application $g : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto x^2$ est surjective puisque tout réel positif possède une racine carrée ; ainsi, tout réel positif y a deux antécédents, $\sqrt{y}$ et $-\sqrt{y}$ (égaux si $y = 0$).

Exercice. Tracer le graphe de quatre fonctions de $\mathbb{R}$ dans $\mathbb{R}$, de sorte que l'une d'entre elles soit injective et surjective, l'une soit non injective et surjective, l'une soit injective et non surjective et l'une soit non injective et non surjective.

d) Propriétés formelles

On peut passer ces propriétés (faciles) en première lecture mais elle sont un entraînement à la manipulation de ces notions abstraites et elles seront utiles dans la suite.

Lemme. *Soient $f : E \to F$ et $g : F \to G$ deux applications. Alors :*

(i) *si f et g sont injectives, alors $g \circ f$ est injective ;*

(ii) *si f et g sont surjectives, alors $g \circ f$ est surjective.*

Démonstration. (i) Soient x et x' deux éléments de E qui ont la même image par $g \circ f$, c'est-à-dire : $g\big(f(x)\big) = g\big(f(x')\big)$. Comme g est injective et que $f(x)$ et $f(x')$ ont la même image par g, on a : $f(x) = f(x')$. Comme f est injective, on en déduit : $x = x'$. Ainsi, $g \circ f$ est injective.
(ii) Soit z un élément de G. Comme g est surjective, il existe y dans F tel que $z = g(y)$. Comme f est surjective, il existe x dans E tel que $y = f(x)$. Mais alors, on a : $z = g\big(f(x)\big)$, c'est-à-dire que x est un antécédent de z par $g \circ f$. Ainsi, $g \circ f$ est surjective.$\square$

Les réciproques ne sont que partiellement vraies.

Lemme. *Soient $f : E \to F$ et $g : F \to G$ deux applications. Alors :*

(i) *si $g \circ f$ est injective, alors f est injective ;*

(ii) *si $g \circ f$ est surjective, alors g est surjective.*

Démonstration. (i) Soient x et x' deux éléments de E tels que $f(x) = f(x')$. On a alors : $g\big(f(x)\big) = g\big(f(x')\big)$. Comme $g \circ f$ est injective, cela entraîne que $x = x'$. L'injectivité de f en résulte.
(ii) Soit z un élément de G. Comme $g \circ f$ est surjective, il existe $x \in E$ tel que $z = g \circ f(x) = g\big(f(x)\big)$. Ainsi, z est l'image de $f(x)$. La surjectvité de g en résulte.$\square$

Exemples. Voici des contre-exemples aux réciproques qui ne marchent pas.

(i) Pour $f : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto -\sqrt{x}$ et $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, la composée $g \circ f : \mathbb{R}^+ \to \mathbb{R}$, $x \mapsto x$ est injective mais g ne l'est pas.

(ii) Pour $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ et $g : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto \sqrt{|x|}$, la composée $g \circ f : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto |x|$ est surjective mais f ne l'est pas.

Exercice. Soit $f : E \to F$ avec E et F *finis*. Montrer que f est injective SSI f est surjective.

3° Bijections

a) Définition

Définition. Soit $f : E \to F$ une application. On dit que f est *bijective* ou que c'est une *bijection* si elle est injective et surjective ; autrement dit, tout élément de l'ensemble d'arrivée possède un unique antécédent :

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

(En effet, il en a au plus un par injectivité et au moins un par surjectivité.)

Remarque. En anglais, pour exprimer que f est bijective, on peut dire que "f is one-to-one" : il y a exactement un élément de E pour un élément de F.
Attention ! Les notions d'image et d'antécédent ne jouent pas du tout le même rôle :

- pour toute application $f : E \to F$, tout élément de E possède une unique image ;
- en revanche, le fait que tout élément de F possède un unique antécédent est rare parmi les applications de E dans F et il caractérise les bijections.

b) Bijection réciproque

Définition. Soient $f : E \to F$ et $g : F \to E$ deux applications. On dit que g est une *application réciproque* de f si l'on a :

$$g \circ f = \mathrm{Id}_E \quad \text{et} \quad f \circ g = \mathrm{Id}_F.$$

A priori, il pourrait exister plusieurs applications réciproques ; en fait, il en existe au plus une.

Lemme. *Soit $f : E \to F$ une application. Si f admet une application réciproque, celle-ci est nécessairement unique.*

Démonstration. Soient g_1 et g_2 sont deux applications réciproques de f, montrons qu'elles sont égales. Comme g_1 et g_2 ont les mêmes ensembles de départ et d'arrivée, il s'agit de montrer que l'on a, pour tout y dans F : $g_1(y) = g_2(y)$. Fixons donc y. On a, par définition : $g_1 \circ f = \mathrm{Id}_E$ et $\mathrm{Id}_F = f \circ g_2$. On déduit de la deuxième relation : $y = f\big(g_2(y)\big)$. En appliquant g_1, il vient :

$$\begin{aligned}
g_1(y) &= g_1\Big(f\big(g_2(y)\big)\Big) & \\
&= (g_1 \circ f)\big(g_2(y)\big) & \text{par définition de } \circ \\
&= \mathrm{Id}_E\big(g_2(y)\big) & \text{car } g_1 \circ f = \mathrm{Id}_E \\
&= g_2(y) & \text{par définition de } \mathrm{Id}_E.
\end{aligned}$$

Comme y était quelconque, le lemme en résulte.□

Notation. Soit $f : E \to F$. *Si elle existe*, l'application réciproque (unique) de f est notée f^{-1}.

Proposition. *Soit $f : E \to F$ une application. Alors, f admet une application réciproque si et seulement si f est bijective. On a alors :*

$$\forall x \in E,\ \forall y \in F, \quad y = f(x) \iff x = g(y)$$

(autrement dit, l'image de y par f^{-1} est l'unique antécédent de y par f).

Démonstration. On veut prouver une équivalence, on procède par double implication. Supposons que f admet une application réciproque g, c'est-à-dire que l'on a : $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. Montrons que f est bijective. Soit y un élément de F. On a : $y = f\big(g(y)\big)$, donc $g(y)$ est un antécédent de y par f, ce qui prouve que f est surjective. Soit x un antécédent de y par f. On a : $x = g\big(f(x)\big) = g(y)$, ce qui prouve que $g(y)$ est l'unique antécédent de y par f. Ainsi, f est bijective. [On aurait pu invoquer le deuxième lemme de 2°d) : $g \circ f = \mathrm{Id}_E$ est injective donc f l'est ; $f \circ g = \mathrm{Id}_F$ est surjective donc f l'est.]
Réciproquement, supposons que f soit bijective. Cela signifie que tout y de F possède un unique antécédent : notons-le $g(y)$. On construit ainsi une application $g : F \to E$. Montrons que g est une application réciproque de f (et donc la seule, d'après le lemme). Il faut montrer que l'on a : $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$. Pour la première relation, fixons $x \in E$ et posons $y = f(x)$; par définition de g, $g(y)$ est l'antécédent de y par f, c'est-à-dire x ; autrement dit, on a : $g\big(f(x)\big) = g(y) = x$. Pour la deuxième relation, fixons $y \in F$ et posons $x = g(y)$; par définition de g, x est l'antécédent de y par f, donc $f\big(g(y)\big) = f(x) = y$.
Enfin, pour (x, y) fixé dans $E \times F$, l'équivalence entre les assertions $y = f(x)$ et $x = g(y)$ n'est autre que la définition de g :

— si $y = f(x)$, alors $g(y)$ est l'unique antécédent de y par f, qui est x, d'où $x = g(y)$;

— si $x = g(y)$, alors x est l'unique antécédent de y par f, d'où $f(x) = y$.□

Mise en garde. *Soient $f : E \to F$ et $g : F \to E$ deux applications. En général, la relation $g \circ f = \mathrm{Id}_E$ ne suffit pas à prouver que f est bijective et que g est son application réciproque.*

Exemple. Pour un contre-exemple, prendre $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$ et définir $g : \mathbb{N} \to \mathbb{N}$ par : $g(p) = p-1$ si $p \geq 1$ et $g(0) = 17$. On a bien : $g\big(f(n)\big) = n$ pour tout n mais f n'est pas surjective car 0 n'a pas d'antécédent.

Exercice. Soit f une bijection. Vérifier que l'application réciproque de f^{-1} est f.

Proposition. *La composée de deux bijections est une bijection : si $f : E \to F$ et $g : F \to G$ sont deux bijections, alors $g \circ f : E \to G$ est une bijection. De plus, on a :*

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

Démonstration. On a par associativité :

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \mathrm{Id}_F \circ g^{-1} = g \circ g^{-1} = \mathrm{Id}_G$$
$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \mathrm{Id}_F \circ f = f^{-1} \circ f = \mathrm{Id}_E.$$

4° Retour sur la notion de cardinal [pas traité en amphi]

a) Bijections et injections entre ensembles finis et leurs cardinaux

Au sens le plus enfantin possible (penser aux *comptines*), compter des objets, c'est associer à chacun un nombre en commençant par 1, puis 2, etc., et regarder à quel entier on s'arrête. Dire qu'un ensemble fini non vide[15] E contient n éléments pour un entier naturel n, c'est dire que l'on peut numéroter ses éléments par les entiers de 1 à n, chaque élément étant associé à un unique entier, c'est-à-dire que l'on peut établir une correspondance *one-to-one* de $\{1, 2, \ldots, n\}$ sur E.

Il semble naturel que l'entier n sur lequel on tombe ne dépende pas de l'ordre dans lequel on énumère les éléments de E, *i.e.* de la bijection. Formellement, si on a deux bijections $f : \{1, \ldots, n\} \to E$ et $g : \{1, \ldots, p\} \to E$, alors $f^{-1} \circ g$ est une bijection de $\{1, \ldots, p\}$ sur $\{1, \ldots, n\}$. Cela entraîne que $n = p$.

C'est une conséquence du *principe des tiroirs*. Informellement, si l'on range $n+1$ objets dans n tiroirs, il y a au moins un tiroir qui contient au moins deux objets. En termes plus formels, quel que soit l'entier n, il n'existe pas d'injection d'un ensemble à $n+1$ éléments vers un ensemble à n éléments. Autrement dit, si h est une application de $\{1, \ldots, n+1\}$ vers $\{1, \ldots, n\}$, alors h n'est pas injective. (Exercice : essayer de le démontrer, par exemple par récurrence sur n.) *A fortiori*, si h est une application de $\{1, \ldots, p\}$ vers $\{1, \ldots, n\}$ avec $p > n$, alors h n'est pas injective (pourquoi ?). Par contraposée, on obtient que si $h : \{1, \ldots, p\} \to \{1, \ldots, n\}$ est injective, alors $p \leq n$. Pour revenir au paragraphe précédent, en appliquant le principe des tiroirs à $f^{-1} \circ g$ puis à $g^{-1} \circ f$ on obtient que $p \leq n$ et que $n \leq p$, donc que $n = p$.

Tout cela pour dire qu'il y a un lien fort entre l'existence d'une bijection et l'égalité des cardinaux, entre l'existence d'une injection et une inégalité des cardinaux. On étend ces deux idées aux ensembles infinis.

b) Équipotence

D'après le paragraphe précédent (et avec ses notations), avec une notion naïve de cardinal, on a l'équivalence : $\mathrm{card}(E) = n$ SSI il existe une bijection de $\{1, \ldots, n\}$ sur E. Pour étendre la notion de cardinal aux ensembles infinis, on introduit la définition suivante.

Définition. Soient E et F deux ensembles. On dit que E et F sont *équipotents* et on écrit $E \simeq F$ ou $\mathrm{card}(E) = \mathrm{card}(F)$ s'il existe une bijection de E sur F.

Le lemme suivant justifie l'usage d'un symbole proche de l'égalité pour la relation d'équipotence.

Lemme. *Soient E, F et G trois ensembles :*

(i) *on a : $E \simeq E$;*

(ii) *si $E \simeq F$ alors $F \simeq G$;*

(iii) *si $E \simeq F$ et $F \simeq G$ alors $E \simeq G$.*

Démonstration. (i) L'identité $\mathrm{Id}_E : E \to E$, $x \mapsto x$ est une bijection de E sur E.
(ii) Si $f : E \to F$ est une bijection, alors sa réciproque $f^{-1} : F \to E$ est une bijection de F sur E.
(iii) Si $f : E \to F$ et $g : F \to G$ sont des bijections, alors la composée $g \circ f : E \to H$ est une bijection.

---

15. Si E est vide, on a bien une bijection de $\emptyset$ sur $\{1, \ldots, 0\} = \emptyset$ – l'identité, dont le graphe est vide. Eh...

c) ≪ Relation d'ordre ≫ sur les cardinaux

Affaiblissons un peu et passons des bijections aux injections et surjections. Soient E et F deux ensembles finis ayant respectivement n et p éléments. Si $n \leq p$, il existe une injection de E dans F : en effet, on peut numéroter les ensembles $E = \{x_1, \ldots, x_n\}$ et $F = \{y_1, \ldots, y_p\}$ et définir une injection $f : E \to F$ par $f(x_i) = y_i$ pour $1 \leq i \leq n$. Inversement, si $n > p$, le principe des tiroirs montre qu'il n'existe pas d'injection de E dans F. Pour étendre ces considérations aux ensembles infinis, on pose la définition suivante.

Définition. Soient E et F deux ensembles. On dit que le cardinal de E est inférieur ou égal au cardinal de F et on note $\mathrm{card}(E) \leq \mathrm{card}(F)$ s'il existe une injection de E dans F.

Bien sûr, on a : $\mathrm{card}(E) \leq \mathrm{card}(E)$ pour tout ensemble E – l'identité est une injection de E dans E. Pour trois ensembles E, F et G, les inégalités $\mathrm{card}(E) \leq \mathrm{card}(F)$ et $\mathrm{card}(F) \leq \mathrm{card}(G)$ entraînent $\mathrm{card}(E) \leq \mathrm{card}(G)$. En effet, la composée de deux injections est une injection.
Le théorème suivant est un peu délicat, on l'admet.

Théorème (Cantor-Bernstein). *Soient E et F deux ensembles. S'il existe une injection $f : E \to F$ et une injection $g : F \to E$, alors il existe une bijection $h : E \to F$.*
Autrement dit : si $\mathrm{card}(E) \leq \mathrm{card}(F)$ et $\mathrm{card}(F) \leq \mathrm{card}(E)$, alors $\mathrm{card}(E) = \mathrm{card}(F)$.

Voici une autre façon de caractériser la relation $\leq$. La propriété est plus subtile qu'il n'y paraît. Elle repose sur une fausse évidence, l'axiome du choix que l'on va passer sous silence ici.

Proposition. *Soient E et F deux ensembles non vides. Alors, il existe une injection $f : E \to F$ si et seulement s'il existe une surjection $g : F \to E$.*

Démonstration. Supposons qu'il existe une injection $f : E \to F$ et construisons une surjection g. Choisissons un élément x_0 dans E. Soit $y \in F$. Si y possède un antécédent x par f, il est unique par injectivité ; on pose alors $g(y) = x$. Si y n'a pas d'antécédent, on pose $g(y) = x_0$. L'application g ainsi construite est surjective. En effet, soit $x \in E$: alors, par construction de g, on a : $x = g\big(f(x)\big)$.
Supposons qu'il existe une surjection $g : F \to E$. Tout élément x de E possède au moins un antécédent par g ; parmi tous ces antécédents, on en choisit un que l'on note [16] $f(x)$. On fabrique ainsi une injection. En effet, si x et x' ont la même image par f, alors $y = f(x) = f(x')$ est à la fois un antécédent de x par g, de sorte que $g(y) = x$ et de x', de sorte que $g(y) = x'$; ainsi, $x = x'$.□

d) Des infinis de cardinaux différents !

Proposition. $\mathrm{card}(\mathbb{N}) = \mathrm{card}(\mathbb{N}^*) = \mathrm{card}(\mathbb{Z}) = \mathrm{card}(\mathbb{N}^2) = \mathrm{card}(\mathbb{Q})$ *mais* $\mathrm{card}(\mathbb{N}) < \mathrm{card}(\mathbb{R})$.

Esquisse de preuve. Exhiber une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$ n'est pas difficile [17] : à tout entier n, on associe son successeur $n+1$. Voici des bijections réciproques entre $\mathbb{N}$ et $\mathbb{Z}$:

$$f : \begin{array}{ccl} \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \begin{cases} n/2 & \text{si } n \text{ est pair,} \\ -(n-1)/2 & \text{sinon ;} \end{cases} \end{array} \qquad f^{-1} : \begin{array}{ccl} \mathbb{Z} & \longrightarrow & \mathbb{N} \\ p & \longmapsto & \begin{cases} 2p & \text{si } p \geq 0, \\ -2p-1 & \text{si } p < 0. \end{cases} \end{array}$$

Il est plus étonnant encore que $\mathbb{N}$ et $\mathbb{N}^2$ soient équipotents. Pourtant, il n'est pas très difficile de montrer (=exercice !) que pour tout entier $n \geq 1$, il existe un unique couple $(p, q) \in \mathbb{N}^2$ tel que $n = 2^p(2q+1)$. Poser $f(n) = (p, q)$ définit donc une bijection de $\mathbb{N}^*$ sur $\mathbb{N}^2$. En composant avec la bijection de $\mathbb{N}$ sur $\mathbb{N}^*$, on trouve une bijection de $\mathbb{N}$ sur $\mathbb{N}^2$.
On en déduit facilement [18] que $\mathrm{card}(\mathbb{Q}) = \mathrm{card}(\mathbb{N})$. D'une part, comme l'application $\mathbb{N} \to \mathbb{Q}$, $n \mapsto n$ est injective, on a : $\mathrm{card}(\mathbb{N}) \leq \mathrm{card}(\mathbb{Q})$. D'autre part, l'application $h : \mathbb{Z} \times \mathbb{N}^* \to \mathbb{Q}$, $(p, q) \mapsto p/q$ est surjective (vérifier) et l'on a : $\mathrm{card}(\mathbb{N}) = \mathrm{card}(\mathbb{N}^2) = \mathrm{card}(\mathbb{Z} \times \mathbb{N}^*) \geq \mathrm{card}(\mathbb{Q})$ (vérifier ! la dernière inégalité provient de la surjection h). Par le théorème de Cantor-Bernstein, on a donc : $\mathrm{card}(\mathbb{N}) = \mathrm{card}(\mathbb{Q})$.

16. C'est précisément ici qu'intervient l'axiome du choix.
17. Lire toutefois la version ≪ hôtel de Hilbert ≫.
18. Il est plus difficile d'exhiber une bijection explicite ; on peut en fabriquer grâce aux suites de Farey.

Soit $u : \mathbb{N}^* \to [0,1[$ une application, c'est-à-dire une suite $(u_n)_{n\geq 1}$. On décompose chaque terme en base 10 : pour tout $n \in \mathbb{N}$, il existe une unique suite $(a_n^p)_{p\geq 1}$ d'entiers compris entre 0 et 9 qui ne stationne pas à 9 telle que

$$u_n = \sum_{p\geq 1} \frac{a_n^p}{10^p}.$$

Dans une variation du paradoxe du menteur, appelée *argument diagonal de Cantor*, posons, pour $n \geq 1$:

$$b_n = \begin{cases} 3 & \text{si } a_n^n \neq 3, \\ 4 & \text{si } a_n^n = 4, \end{cases} \qquad \text{et} \quad y = \sum_{n\geq 1} \frac{b_n}{10^n}.$$

Alors, y est un réel de $[0,1[$ qui est différent de tous les u_n. En effet, pour chaque entier n, les n-ièmes décimales de y et de u_n diffèrent par construction de y : $b_n \neq a_n^n$. Autrement dit, l'application u n'est pas surjective, ce qui prouve que $\mathrm{card}(\mathbb{N}) < \mathrm{card}\big([0,1[\big) \leq \mathrm{card}(\mathbb{R})$.

Remarque. Vu l'injection de $\mathbb{N}$ dans $\mathbb{N}^*$, le principe des tiroirs ne fonctionne pas avec des ensembles infinis.

5° Image directe ou réciproque d'une partie

Dans tout ce paragraphe, on fixe une application $f : E \to F$.

a) Image directe d'une partie

Définition. Soit A une partie de E. On appelle *image directe* (ou *image*) de A par f la partie de F notée $f(A)$ définie par :

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

(On pourrait écrire : $f(A) = \{f(x) \mid x \in A\}$.) Noter l'équivalence : f est surjective SSI $f(E) = F$.

b) Image réciproque d'une partie

Définition. Soit B une partie de F. On appelle *image réciproque* de B par f la partie de E notée $f^{-1}(B)$ définie par :

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

(On pourrait écrire : $f^{-1}(B) = \{x \in E \mid \exists y \in B,\ y = f(x)\}$. Ce serait compliqué pour rien.)

Exemple. Pour y fixé dans F, on note en général $f^{-1}(y) = f^{-1}\big(\{y\}\big)$: c'est l'ensemble des antécédents de y (pourquoi ?).

Mise en garde. *Bien que l'on écrive $f^{-1}(B)$, cela ne signifie pas en général qu'il existe une application réciproque f^{-1} pour f. En effet, la notation $f^{-1}(B)$ est définie pour toute application f, qu'elle soit bijective ou pas ; en revanche, seules les bijections ont une application réciproque. Pour y fixé, il y a un conflit de notations sur $f^{-1}(y)$:*

— *pour une application f quelconque, $f^{-1}(y)$ désigne l'ensemble des antécédents de y ; c'est une partie de F ;*

— *si f est une bijection, $f^{-1}(y)$ désigne le plus souvent l'image de y par l'application réciproque f^{-1} : c'est un élément de F.*

6° Familles

Une *famille* est un autre mot pour *application* associée à une autre notation pour les images. Dire que $(A_i)_{i\in I}$ est une famille d'éléments de $\mathscr{F}$ indexée par I, c'est parler de l'application $I \to \mathscr{F}$, $i \mapsto A_i$ (l'image de $i \in I$ est notée A_i). Lorsque A_i est un ensemble pour tout i, on définit la *réunion* $\bigcup_{i\in A} A_i$ et l'*intersection* $\bigcap_{i\in A} A_i$ des A_i par :

$$\forall x, \quad x \in \bigcup_{i\in A} A_i \iff \exists i \in I,\ x \in A_i;$$

$$\forall x, \quad x \in \bigcap_{i\in A} A_i \iff \forall i \in I,\ x \in A_i.$$