INJECTIONS, SURJECTIONS, BIJECTIONS

Ce chapitre généralise un certain nombre de concepts importants du chapitre « Rappels et compléments sur les fonctions ». Nous avons manipulé ensemble déjà pas mal de fonctions, mais presque toujours définies sur une partie de $\mathbb{R}$ et à valeurs dans $\mathbb{C}$. Nous aurons désormais souvent l'occasion de travailler avec des fonctions **définies sur des ensembles quelconques** et **à valeurs dans des ensembles quelconques** — des ensembles de ce que vous voulez, pas forcément des ensembles de nombres.

Dans tout ce chapitre, $E, F, G\ldots$ sont des ensembles **quelconques**.

1 Vocabulaire usuel des applications

Qu'est-ce qu'une fonction ? On se contente généralement de dire ce qu'une fonction **fait** pour éviter d'avoir à dire ce qu'elle **est** : « Une fonction associe à tout élément d'un ensemble un unique élément d'un autre ensemble. » Ceci hélas n'est pas une définition, quel est donc ce quelque chose qui « associe » une chose à une autre ?

Intuitivement, une fonction c'est une figure, une courbe, un graphe. La fonction $x \longmapsto x^2$ par exemple peut être vue comme l'ensemble des points du plan de coordonnées $\left(x, x^2\right)$, x décrivant $\mathbb{R}$. On vous a sans doute expliqué qu'il ne faut pas confondre une fonction et sa courbe représentative. Avec la définition qui suit, au contraire, très anglo-saxonne et bien peu française, toute fonction **est** son graphe.

Définition **(Application/fonction, ensemble de définition/d'arrivée, image et antécédents d'un point)**

- **Application/fonction :** On appelle *application* (ou *fonction*) *de E dans F* toute partie f de $E \times F$ pour laquelle :
$$\forall x \in E, \quad \exists ! \, y \in F, \quad (x, y) \in f.$$
La présence du pseudo-quantificateur $\exists !$ permet de noter $f(x)$ l'unique $y \in F$ de la proposition ci-dessus. La proposition $(x, y) \in f$ n'est donc en fait jamais notée ainsi mais plutôt $y = f(x)$.
- **Ensemble de définition/arrivée :** L'ensemble E est appelé l'*ensemble de définition* (ou *de départ*) *de f*. L'ensemble F est quant à lui appelé un *ensemble d'arrivée de f*.
- **Image/antécédents :** Pour tous $x \in E$ et $y \in F$, si $y = f(x)$, on dit que y est **l'***image de x par f* et que x est **un** *antécédent de y par f*.

Conformément au programme, les mots « fonction » et « application » seront pour nous parfaitement synonymes, mais vous trouverez peut-être dans certains ouvrages non scolaires deux définitions distinctes attachées à ces deux noms. N'y prêtez pas attention, c'est sans importance.

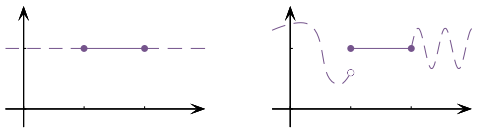
On représente classiquement les applications de deux façons — soit au moyen de « patates » (figure de gauche), soit au moyen d'un graphe (figure de droite).

Définition **(Restriction et prolongements)** Soit A une partie de E.

- **Restriction :** Soient $f : E \longrightarrow F$ une application. On appelle *restriction de f à A*, notée $f_{|A}$, l'application définie sur A **seulement** par : $f_{|A}(x) = f(x)$ pour tout $x \in A$.
- **Prolongements :** Soit $f : A \longrightarrow F$ une application. On appelle *prolongement de f à E* toute application g de E dans F pour laquelle pour tout $x \in A$: $f(x) = g(x)$.

Restreindre/prolonger une application, c'est diminuer/augmenter la taille de son ensemble de définition.

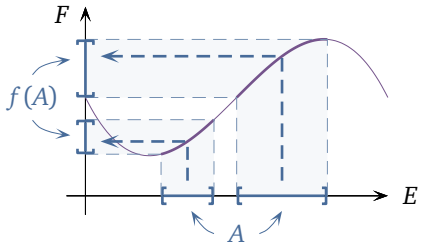
✖ **Attention !** Toute application possède **beaucoup** de prolongements, on parle toujours d'**un** prolongement et non « du » prolongement. Les figures ci-contre représentent deux prolongements de la fonction $x \longmapsto 1$ définie sur $[1, 2]$.



Définition **(Image d'une partie par une application, image d'une application, expression « à valeurs dans… »)** Soit $f : E \longrightarrow F$ une application.

- **Image :** Pour toute partie A de E, on appelle *image (directe) de A par f* l'ensemble des images par f des éléments de A :
$$f(A) = \big\{y \in F \mid \quad \exists a \in A, \quad y = f(a)\big\} = \big\{f(a) \mid \quad a \in A\big\}.$$
L'image de E tout entier est simplement appelée l'*image de f*.
- **Expression « à valeurs dans… » :** Soit B une partie de F. On dit que f est *à valeurs dans B* si toute valeur de f est élément de B, i.e. si : $\forall x \in E, \quad f(x) \in B$, ou encore si l'image de f est incluse dans B : $f(E) \subset B$.

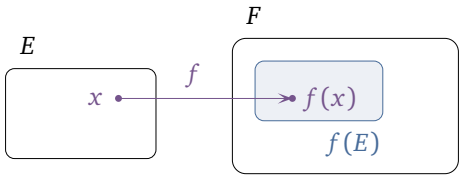
Pour représenter $f(A)$, on projette sur l'axe des ordonnées la portion du graphe de f qui se situe au-dessus de A.



Exemple La fonction $z \longmapsto \mathrm{Re}(z)^2$ définie sur $\mathbb{C}$ est à valeurs dans $\mathbb{C}$, mais son image est (seulement) $\mathbb{R}_+$.
La fonction $x \longmapsto \mathrm{i}x$ définie sur $\mathbb{R}$ est à valeurs dans $\mathbb{C}$, mais son image est (seulement) l'ensemble $\mathrm{i}\mathbb{R}$ des imaginaires purs.
La fonction $\theta \longmapsto \mathrm{e}^{\mathrm{i}\theta}$ définie sur $\mathbb{R}$ est à valeurs dans $\mathbb{C}$, mais son image est (seulement) $\mathbb{U}$.

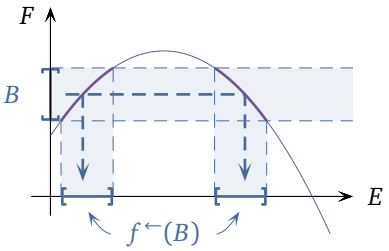
Exemple Soit A une partie de E. L'application $X \longmapsto X \cup A$ définie sur $\mathscr{P}(E)$ est à valeurs dans $\mathscr{P}(E)$, mais son image est (seulement) l'ensemble des parties de E qui contiennent A.

Attention ! En général, l'image de E est plus petite que F !



Définition **(Image réciproque d'une partie par une application)** Soit $f : E \longrightarrow F$ une application. Pour toute partie B de F, on appelle *image réciproque de B par f* l'ensemble des éléments de E dont l'image par f appartient à B :
$$\big\{x \in E \mid \quad f(x) \in B\big\}, \qquad \text{noté PROVISOIREMENT } f^{\leftarrow}(B).$$

Pour représenter $f^{\leftarrow}(B)$, on projette sur l'axe des abscisses la portion du graphe de f située dans le tube horizontal défini par B.



Pour tout $x \in E$: $\quad x \in f^{\leftarrow}(B) \iff f(x) \in B.$ Équivalence vitale !

Pour une fonction f de $\mathbb{R}$ dans $\mathbb{R}$, chercher l'image réciproque d'un singleton $\{y\}$ par f revient à résoudre l'équation $y = f(x)$ d'inconnue x, alors que pour un intervalle $[a, b]$, cela revient à résoudre l'inéquation $a \leqslant f(x) \leqslant b$.

Exemple

- L'image réciproque de $\mathbb{R}_+$ par la fonction exponentielle est $\mathbb{R}$ tout entier. L'image réciproque de $[1, 2[$ est $[0, \ln 2[$, liée à l'inéquation $1 \leqslant \mathrm{e}^x < 2$ d'inconnue $x \in \mathbb{R}$.
- L'image réciproque de $\{1\}$ par la fonction sinus est $\dfrac{\pi}{2} + 2\pi\mathbb{Z}$, liée à l'équation $\sin x = 1$ d'inconnue $x \in \mathbb{R}$. L'image réciproque de $[2, 3]$ est vide, liée à l'inéquation $2 \leqslant \sin x \leqslant 3$ d'inconnue $x \in \mathbb{R}$.
- L'image réciproque de $[4, +\infty[$ par la fonction carré est $]-\infty, -2] \cup [2, +\infty[$, liée à l'inéquation $x^2 \geqslant 4$ d'inconnue $x \in \mathbb{R}$.

Définition **(Ensembles d'applications)** L'ensemble des applications de E dans F est noté F^E ou $\mathscr{F}(E, F)$.

Attention ! Ne confondez pas F^E et E^F !

Définition **(Famille)** Soit I un ensemble. On appelle *famille (d'éléments) de E indexée par I* toute application de I dans E. Les familles, au lieu d'être notée comme des applications, sont presque toujours notées sous la forme $(x_i)_{i \in I}$.

L'ensemble des familles de E indexée par I est naturellement noté E^I.

Une famille $(x_1,\dots,x_n)$ d'éléments de E n'est rien de plus que l'application f de $[\![1,n]\!]$ dans E définie par les relations : $f(1)=x_1,\quad\dots,\quad f(n)=x_n,$ qui associe à chaque position l'élément qui lui correspond.

Exemple $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des suites réelles, $\mathbb{C}^{\mathbb{N}}$ celui des suites complexes.

Exemple Une famille d'éléments de E indexée par l'ensemble vide est une application de $\varnothing$ dans E et ça existe ! D'après la définition d'une application, l'ensemble vide une application de $\varnothing$ dans E et c'est la seule, appelée la *famille vide de E*.

Définition-théorème (Identité, composition)

- **Identité :** On appelle (*application*) *identité de E*, notée Id_E, l'application « qui ne fait rien » $\left\{\begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x. \end{array}\right.$
- **Composition :** Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications. On appelle *composée de f suivie de g* l'application $g\circ f$ définie pour tout $x\in E$ par : $g\circ f(x) = g\big(f(x)\big)$.

  La composition est *associative* — pour toutes applications $f : E \longrightarrow F$, $g : F \longrightarrow G$ et $h : G \longrightarrow H$:
  $$h\circ(g\circ f) = (h\circ g)\circ f.$$
  En outre, pour toute application $f : E \longrightarrow F$: $\mathrm{Id}_F\circ f = f\circ\mathrm{Id}_E = f$ (*neutralité de l'identité pour la composition*).

Attention ! En général, la composition n'est possible que dans un seul sens, et quand elle est possible dans les deux, f et g n'ont aucune raison de commuter.

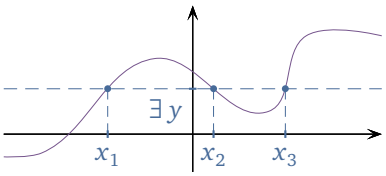
2 Injections, surjections, bijections

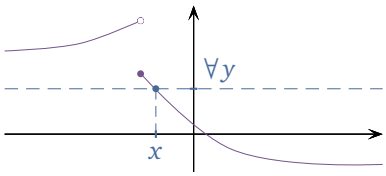
2.1 Injections

Définition (Injection) Soit $f : E \longrightarrow F$ une application. On dit que f est *injective sur E* ou que c'est une *injection sur E* si :
$$\forall x,x'\in E,\qquad f(x)=f(x') \quad\Longrightarrow\quad x=x',$$
ce qui revient à dire que tout élément de F possède AU PLUS un antécédent dans E par f.

Plus précisément, si f est injective, les éléments de son image $f(E)$ possèdent tous exactement un antécédent par f alors que les éléments de $F\setminus f(E)$ n'en possèdent aucun.

f N'est PAS injective, CERTAINS y ont plusieurs antécédents.

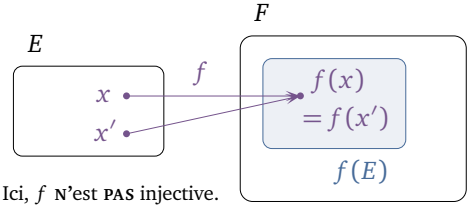




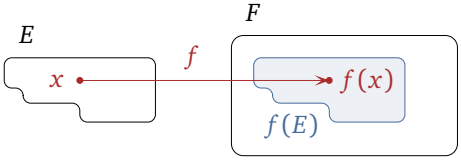
f est injective, AUCUN y n'a plusieurs antécédents, certains même n'en ont pas.

D'un point de vue calculatoire, une application injective est une application que l'on peut « simplifier » en cours de calcul. Dès que $f(x)=f(x')$, alors après « simplification » : $x=x'$.

On comprend également bien l'injectivité en contraposant sa définition. L'application f est injective lorsqu'elle donne des valeurs différentes à des points différents — si $x\neq x'$: $f(x)\neq f(x')$.



Ici, f N'est PAS injective.



On peut aussi dire les choses autrement. Parce que f distingue à l'arrivée les éléments qui le sont au départ, l'image de f est comme une copie de E à l'intérieur de F.

Exemple La fonction $z\longmapsto\dfrac{z}{z-\mathrm{i}}$ est injective sur $\mathbb{C}\setminus\{\mathrm{i}\}$.

Démonstration Soient $z,z'\in\mathbb{C}\setminus\{\mathrm{i}\}$. Si $\dfrac{z}{z-\mathrm{i}}=\dfrac{z'}{z'-\mathrm{i}}$: $z(z'-\mathrm{i})=z'(z-\mathrm{i})$, donc évidemment $z=z'$.

Exemple L'application $X \overset{f}{\longmapsto} X \cup \{0\}$ n'est pas injective sur $\mathscr{P}(\mathbb{N})$ car par exemple $f(\varnothing) = \{0\} = f(\{0\})$.

Théorème (Injectivité et composition) Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

(i) Si f et g sont injectives, $g \circ f$ l'est aussi.

(ii) Si $g \circ f$ est injective, f l'est aussi.

Attention ! Dans l'assertion (ii), g n'a aucune raison d'être injective. Pensez par exemple aux fonctions $x \overset{f}{\longmapsto} e^x$ et $x \overset{g}{\longmapsto} x^2$ de $\mathbb{R}$ dans $\mathbb{R}$.

Démonstration

(i) Soient $x, x' \in E$. Faisons l'hypothèse que $g \circ f(x) = g \circ f(x')$ et montrons que $x = x'$. Or tout simplement, par injectivité de g : $f(x) = f(x')$, puis par injectivité de f : $x = x'$.

(ii) Soient $x, x' \in E$. Faisons l'hypothèse que $f(x) = f(x')$ et montrons que $x = x'$. Composons d'abord par g : $g\big(f(x)\big) = g\big(f(x')\big)$. Alors par injectivité de $g \circ f$: $x = x'$.

Le théorème suivant a été démontré et étudié au chapitre « Rappels et compléments sur les fonctions ».

Théorème (Injectivité et stricte monotonie) Soit $f : E \longrightarrow \mathbb{R}$ une fonction où E est une partie de $\mathbb{R}$.
Si f est strictement monotone, f est injective.

Attention ! La réciproque est fausse en général comme le montre le graphe de la fonction injective représentée un peu plus haut. Cette fonction est injective sans être monotone, mais du coup elle N'EST PAS continue. Nous verrons plus tard qu'une fonction injective et continue sur un intervalle y est toujours strictement monotone.

2.2 Surjections

Définition (Surjection) Soit $f : E \longrightarrow F$ une application. On dit que f est *surjective de E SUR F* ou que c'est une *surjection de E SUR F* si :

$$\forall y \in F, \quad \exists x \in E, \quad y = f(x), \qquad \text{ce qui revient à dire que l'image de } f \text{ est égale à } F : \quad f(E) = F,$$

ou encore que tout élément de F possède AU MOINS un antécédent dans E par f.

L'application f est bien sûr à valeurs dans son image $f(E)$ et tout élément de $f(E)$ possède un antécédent par f, donc…

Toute application est surjective de son ensemble de définition SUR SON IMAGE.

Attention, on ne dit pas que f est surjective de E « dans » F mais qu'elle l'est de E SUR F, car f atteint alors tous les éléments de F. En ce sens, E « couvre » F à travers f. Cette idée d'une « couverture » justifie l'emploi de la préposition « sur ».

Exemple L'application $X \longmapsto X \cup \{0\}$ n'est pas surjective de $\mathscr{P}(\mathbb{N})$ sur $\mathscr{P}(\mathbb{N})$ car par exemple, $\varnothing$ n'a pas d'antécédent par f, il n'existe pas de partie X de $\mathbb{N}$ pour laquelle $\varnothing = X \cup \{0\}$.

Théorème (Surjectivité et composition) Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

(i) Si f et g sont surjectives, $g \circ f$ l'est aussi.

(ii) Si $g \circ f$ est surjective, g l'est aussi.

Attention ! Dans l'assertion (ii), f n'a aucune raison d'être surjective. Pensez par exemple aux fonctions :

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^x - 1 \end{array} \right. \qquad \text{et} \qquad g : \left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}_+ \\ x & \longmapsto & x^2. \end{array} \right.$$

Démonstration

(i) Soit $y \in G$. Montrons que $y = g \circ f(x)$ pour un certain $x \in E$. Or par surjectivité de g : $y = g(t)$ pour un certain $t \in F$ et par surjectivité de f : $t = f(x)$ pour un certain $x \in E$, donc en effet : $y = g(t) = g\big(f(x)\big) = g \circ f(x)$.

(ii) Soit $y \in G$. Par surjectivité de $g \circ f$: $y = g \circ f(t)$ pour un certain $t \in E$, donc : $y = g(x)$ pour $x = f(t)$.

2.3 Bijections

Définition **(Réciproque)** Soit $f : E \longrightarrow F$ une application. On appelle *réciproque de f sur F* toute application $g : F \longrightarrow E$ pour laquelle $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$.

En termes simples, g défait le travail effectué par f — et vice versa. Ce que l'une tricote, l'autre le détricote.

Définition-théorème **(Bijection)** Soit $f : E \longrightarrow F$ une application. Les assertions suivantes sont équivalentes :

(i) Tout élément de F possède UN ET UN SEUL antécédent dans E par f : $\forall y \in F,\quad \exists ! x \in E,\quad y = f(x)$.

(ii) f est injective sur E et surjective de E sur F.

(iii) f possède une réciproque sur F.

On dit dans ces conditions que f est *bijective de E SUR F* ou que c'est une *bijection de E SUR F*.

En outre, f ne possède alors qu'une seule réciproque, notée f^{-1}. Pour tous $x \in E$ et $y \in F$:

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

Dans le cas d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$, cette équivalence signifie géométriquement que le graphe de f et celui de f^{-1} sont symétriques l'un de l'autre par rapport à la droite d'équation $y = x$.

Exemple L'application Id_E est bijective de E sur E de réciproque elle-même car $\mathrm{Id}_E \circ \mathrm{Id}_E = \mathrm{Id}_E$.

Exemple Soient $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$. La fonction $x \longmapsto ax + b$ est bijective de $\mathbb{R}$ sur $\mathbb{R}$ de réciproque $x \longmapsto \dfrac{x-b}{a}$.

Démonstration Il nous suffit de montrer que les fonctions $x \overset{f}{\longmapsto} ax + b$ et $x \overset{g}{\longmapsto} \dfrac{x-b}{a}$ de $\mathbb{R}$ dans $\mathbb{R}$ sont réciproques l'une de l'autre. Or pour tout $x \in \mathbb{R}$: $g \circ f(x) = \dfrac{(ax+b)-b}{a} = x$ et $f \circ g(x) = a \times \dfrac{x-b}{a} + b = x$.

Exemple Soit $f : E \longrightarrow E$ une *involution de E*, i.e. une application pour laquelle $f \circ f = \mathrm{Id}_E$. Alors f est une bijection et $f^{-1} = f$.

Théorème **(Bijectivité, réciproque et composition)** Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.

(i) Si f est bijective de E sur F, f^{-1} est bijective de F sur E et : $\left(f^{-1}\right)^{-1} = f$.

(ii) Si f et g sont bijectives, $g \circ f$ l'est aussi et : $\left(g \circ f\right)^{-1} = f^{-1} \circ g^{-1}$.

Attention ! Gare à l'ordre ! C'est bien : $\left(g \circ f\right)^{-1} = f^{-1} \circ g^{-1}$ et non pas : $\left(g \circ f\right)^{-1} = g^{-1} \circ f^{-1}$. Si vous cachez un trésor dans un coffre (f), puis ce coffre sous terre (g), et si ensuite vous voulez récupérer votre trésor (défaire $g \circ f$), vous devez d'abord déterrer le coffre (g^{-1}), puis l'ouvrir (f^{-1}) — i.e. appliquer la composée $f^{-1} \circ g^{-1}$.

Démonstration

(i) Les égalités : $f^{-1} \circ f = \mathrm{Id}_E$ et $f \circ f^{-1} = \mathrm{Id}_F$ — qui expriment la bijectivité de f — expriment pour la même raison la bijectivité de f^{-1} et cela montre bien que $\left(f^{-1}\right)^{-1} = f$.

(ii) Pour commencer : $\left(f^{-1} \circ g^{-1}\right) \circ \left(g \circ f\right) = f^{-1} \circ \left(g^{-1} \circ g\right) \circ f = f^{-1} \circ \mathrm{Id}_F \circ f = f^{-1} \circ f = \mathrm{Id}_E$ et de même : $\left(g \circ f\right) \circ \left(f^{-1} \circ g^{-1}\right) = \mathrm{Id}_G$, donc $g \circ f$ est bijective de réciproque $f^{-1} \circ g^{-1}$.

Et comment montre-t-on concrètement qu'une application est bijective ? Le tableau suivant résume la marche à suivre.

Priorité	Ce qu'on fait	Ce qu'on obtient
1	Si on connaît spontanément une expression explicite de f^{-1}, on appelle g la fonction en question et on vérifie simplement que $g \circ f = \mathrm{Id}_E$ et $f \circ g = \mathrm{Id}_F$.	Bijectivité + Réciproque
2	Si on ne connaît pas spontanément f^{-1}, on peut essayer d'en trouver une expression explicite via l'équivalence : $y = f(x) \quad \Longleftrightarrow \quad x = f^{-1}(y)$.	Bijectivité + Réciproque
3	Si on ne se sent pas capable de trouver une expression explicite de f^{-1}, on montre en deux temps que f est à la fois injective et surjective.	Bijectivité

Exemple L'application $z \overset{f}{\longmapsto} \dfrac{z+\mathrm{i}}{z-\mathrm{i}}$ est bijective de $\mathbb{C}\setminus\{\mathrm{i}\}$ sur $\mathbb{C}\setminus\{1\}$ de réciproque $z \longmapsto \mathrm{i}\dfrac{z+1}{z-1}$.

Démonstration Pour tout $z \in \mathbb{C}\setminus\{\mathrm{i}\}$ et pour tout $\zeta \in \mathbb{C}$:

$$\zeta = f(z) \iff \frac{z+\mathrm{i}}{z-\mathrm{i}} = \zeta \iff z+\mathrm{i} = \zeta z - \mathrm{i}\zeta \iff \mathrm{i}(\zeta+1) = z(\zeta-1).$$

On peut alors exprimer z en fonction de ζ si et seulement si $\zeta \neq 1$. Il en découle que 1 n'a pas d'antécédent par f, et plus précisément que $f\big(\mathbb{C}\setminus\{\mathrm{i}\}\big) = \mathbb{C}\setminus\{1\}$.

Achevons maintenant nos calculs. Pour tous $z \in \mathbb{C}\setminus\{\mathrm{i}\}$ et $\zeta \in \mathbb{C}\setminus\{1\}$: $\zeta = f(z) \iff z = \mathrm{i}\dfrac{\zeta+1}{\zeta-1}$, donc f est bijective de $\mathbb{C}\setminus\{\mathrm{i}\}$ sur $\mathbb{C}\setminus\{1\}$ de réciproque $\zeta \longmapsto \mathrm{i}\dfrac{\zeta+1}{\zeta-1}$.

Exemple L'application $(x,y) \overset{g}{\longmapsto} (x+y, xy)$ de $\mathbb{R}^2$ dans $\mathbb{R}^2$ n'est pas injective car par exemple $g(0,1) = (1,0) = g(1,0)$, mais elle est bijective de $\big\{(x,y) \in \mathbb{R}^2 \mid \ x \leqslant y\big\}$ sur $\big\{(x,y) \in \mathbb{R}^2 \mid \ x^2 - 4y \geqslant 0\big\}$.

Démonstration Pour tous $(x,y),(a,b) \in \mathbb{R}^2$:

$$(a,b) = g(x,y) \iff \begin{cases} x+y = a \\ xy = b \end{cases}$$
$$\iff x \text{ et } y \text{ sont les deux racines (éventuellement égales) du polynôme } X^2 - aX + b.$$

Le couple (a,b) possède ainsi un antécédent (x,y) par g si et seulement si le polynôme $X^2 - aX + b$ possède deux racines dans $\mathbb{R}$, i.e. si et seulement si le discriminant $a^2 - 4b$ est positif ou nul. Conclusion :

$$g\big(\mathbb{R}^2\big) = \big\{(a,b) \in \mathbb{R}^2 \mid \ a^2 - 4b \geqslant 0\big\}.$$

Poursuivons sous l'hypothèse additionnelle que $a^2 - 4b \geqslant 0$:

$$(a,b) = g(x,y) \iff (x,y) = \left(\frac{a+\sqrt{a^2-b}}{2}, \frac{a-\sqrt{a^2-b}}{2}\right) \text{ ou } (x,y) = \left(\frac{a-\sqrt{a^2-b}}{2}, \frac{a+\sqrt{a^2-b}}{2}\right).$$

Il est ainsi clair que le couple (a,b) possède exactement un antécédent par g si $a^2-4b = 0$ et deux si $a^2-4b > 0$.

Posons pour finir $E = \big\{(x,y) \in \mathbb{R}^2 \mid \ x \leqslant y\big\}$. Sous l'hypothèse additionnelle que $(x,y) \in E$:

$$(a,b) = g(x,y) \iff (x,y) = \left(\frac{a-\sqrt{a^2-b}}{2}, \frac{a+\sqrt{a^2-b}}{2}\right),$$

donc $g_{|E}$ est bijective de E sur $\big\{(a,b) \in \mathbb{R}^2 \mid \ a^2-4b \geqslant 0\big\}$ de réciproque $(a,b) \longmapsto \left(\dfrac{a-\sqrt{a^2-b}}{2}, \dfrac{a+\sqrt{a^2-b}}{2}\right)$.

Théorème (Bijectivité et image réciproque) Soit f une bijection de E sur F et B une partie de F. Alors :

$$f^{\leftarrow}(B) = f^{-1}(B),$$

où l'on rappelle que $f^{\leftarrow}(B)$ est l'image RÉCIPROQUE de B par f et $f^{-1}(B)$ l'image DIRECTE de B par f^{-1}.

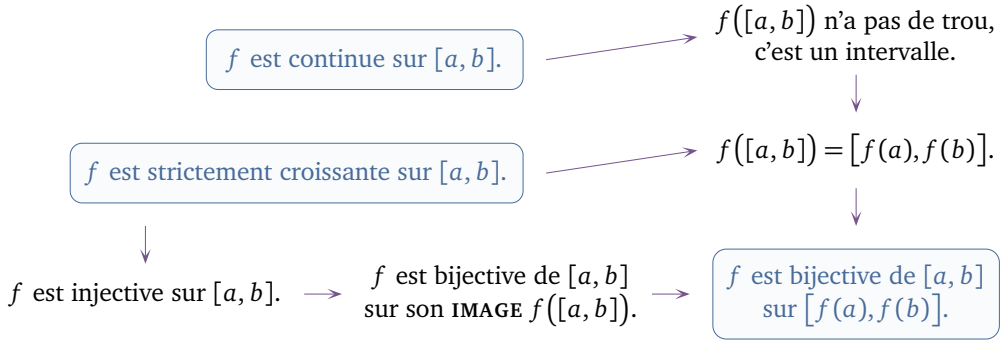
Démonstration Pour tout $x \in E$: $x \in f^{-1}(B) \iff \exists\, b \in B,\ x = f^{-1}(b)$
$\iff \exists\, b \in B,\ f(x) = b \iff f(x) \in B \iff x \in f^{\leftarrow}(B)$. ∎

Attention ! Grâce à ce théorème, nous écrirons désormais TOUJOURS $f^{-1}(B)$ et plus jamais $f^{\leftarrow}(B)$. La notation $f^{\leftarrow}(B)$ n'existe pas en réalité, nous l'avons juste introduite pour ne pas nous emmêler les pinceaux dans un premier temps.

- Dans le cas où f est bijective, nous venons de voir que l'image réciproque de B par f est exactement l'image directe de B par f^{-1}. La confusion des notations $f^{-1}(B)$ et $f^{\leftarrow}(B)$ n'est donc pas gênante.
- Et dans le cas où f n'est pas bijective ? Dans ce cas, de toute façon, IL N'Y A PAS de réciproque f^{-1}, donc pas d'image directe de B par f^{-1}. La notation $f^{-1}(B)$ ne pose donc pas problème dans ce cas non plus.

En guise de conclusion : La notation $f^{-1}(B)$ NE requiert PAS la bijectivité de f !

Nous démontrerons le TVI et son corollaire strictement monotone plus tard dans l'année, mais rien ne nous empêche d'en comprendre dès maintenant les tenants et les aboutissants.



3 Équipotence

Le contenu de ce paragraphe est tout à fait hors programme et ne vous est présenté qu'à titre culturel.

Définition **(Équipotence)** On dit que F est *équipotent à* E s'il existe une bijection de E sur F.

Pourquoi ce mot « équipotent » et pour quoi faire ? Issu du latin, « équipotent » veut dire « de même puissance ». En quel sens ? L'existence d'une bijection de E sur F nous garantit qu'on peut faire se correspondre parfaitement les éléments de E et les éléments de F, associer à tout élément de E un et un seul élément de F et vice versa. Dire que F est équipotent à E revient ainsi à dire que F a exactement le même nombre d'éléments que E.

Intuitivement, de même, l'existence d'une injection de E dans F signifie qu'il y a moins d'éléments dans E que dans F — éventuellement autant — puisqu'on peut dans ce cas trouver dans F une copie de E qui n'est pas forcément F tout entier. Quant à l'existence d'une surjection de E sur F, elle indique au contraire que c'est E qui a plus d'éléments que F — éventuellement autant — puisqu'on peut associer à tout élément de F au moins un antécédent, peut-être plusieurs, ce qui fait qu'en un sens E couvre F à travers f.

Théorème **(Propriétés de la relation d'équipotence)**

- **Symétrie :** Si F est équipotent à E, E est équipotent à F. On peut dire sans ambiguïté que E et F sont *équipotents*.
- **Transitivité :** Si F est équipotent à E et si G est équipotent à F, G est équipotent à E.

Démonstration La symétrie repose sur le fait que la réciproque d'une bijection est une bijection, la transitivité sur le fait que la composée de deux bijections est une bijection.

Je ne démontrerai pas l'important théorème que voici, mais sa preuve est tout à fait accessible.

Théorème **(Théorème de Cantor-Bernstein)** S'il existe une injection de E dans F et une injection de F dans E, E et F sont équipotents.

Bref, si E a moins d'éléments que F et F moins d'éléments que E, E et F en ont autant !

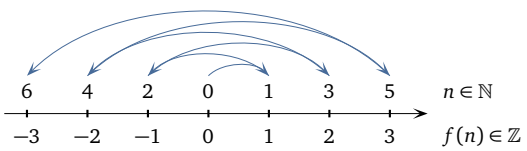
On donne ci-dessous des exemples d'équipotence dont certains sont vraiment surprenants au premier abord. Nous allons notamment voir que deux ensembles peuvent être équipotents alors que l'un d'entre eux est inclus STRICTEMENT dans l'autre.

Exemple $\mathbb{R}$ et $\left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ sont équipotents alors qu'ils n'ont pas la même longueur. Longueur et nombre de points n'ont donc aucun rapport ! Plus généralement, tout intervalle qui n'est ni l'ensemble vide ni un singleton est équipotent à $\mathbb{R}$.

Démonstration Tout simplement, la fonction tangente est bijective de $\left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ sur $\mathbb{R}$.

Exemple $\mathbb{N}$ et $\mathbb{Z}$ sont équipotents.

Démonstration L'application f représentée ci-contre est bijective de $\mathbb{N}$ sur $\mathbb{Z}$. Trouvez-en une expression explicite !



Exemple $\mathbb{N}$ et $\mathbb{N}^2$ sont équipotents.

Démonstration Nous allons montrer que l'application $(p,q) \overset{g}{\longmapsto} 2^p(2q+1)$ est bijective de $\mathbb{N}^2$ sur $\mathbb{N}^*$. On pourrait le faire en utilisant la décomposition des entiers en produit de facteurs premiers, mais comme nous n'avons pas encore établi ce résultat, nous allons procéder autrement. À condition de composer ensuite par la bijection $n \longmapsto n-1$ de $\mathbb{N}^*$ sur $\mathbb{N}$, on aura bien obtenu une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$.

- Pour l'injectivité, soient $(p,q),(p',q') \in \mathbb{N}^2$ deux couples pour lesquels $g(p,q) = g(p',q')$. Quitte à les permuter, on peut supposer $p \leqslant p'$ sans perte de généralité. Ainsi $2^{p'-p}(2q'+1) = 2q+1$, égalité dans laquelle $2^{p'-p}$, $2q+1$ et $2q'+1$ sont des entiers. Comme $2q+1$ est impair, forcément $p = p'$, donc $2q+1 = 2q'+1$, et enfin $(p,q) = (p',q')$.
- Pour la surjectivité, récurrence **forte**, nous allons montrer que pour tout $n \in \mathbb{N}^*$, tout entier de $[\![1,n]\!]$ possède un antécédent par g.

  Initialisation : 1 possède un antécédent par g puisque $g(0,0) = 1$.

  Hérédité : Soit $n \in \mathbb{N}^*$. On suppose que tout élément de $[\![1,n]\!]$ possède un antécédent par g. Et $n+1$?

  Si $n = 2q$ est pair avec $q \in \mathbb{N}$: $\quad n+1 = 2q+1 = g(0,q), \quad$ donc $n+1$ possède un antécédent par g.

  Supposons à présent n impair. Dans ce cas, $n+1$ est pair : $\quad n+1 = 2m \quad$ pour un certain $m \in \mathbb{N}$, et plus précisément $m \in [\![1,n]\!]$. Par hypothèse de récurrence, m possède donc un antédécent (p,q) par g, donc : $n+1 = 2m = 2\,g(p,q) = 2^{p+1}(2q+1) = g(p+1,q), \quad$ donc $n+1$ possède un antécédent par g.

Pour que vous saisissiez bien l'incroyable portée des deux exemples qui suivent, rappelons que $\mathbb{Q}$ et $\mathbb{R}\setminus\mathbb{Q}$ sont denses dans $\mathbb{R}$ et qu'à ce titre, entre deux rationnels distincts il y a toujours un irrationnel, et entre deux irrationnels distincts il y a toujours un rationnel. Intuitivement, $\mathbb{Q}$ et $\mathbb{R}\setminus\mathbb{Q}$ sont donc comme deux peignes en vis-à-vis dont les dents s'alternent et se croisent, entre deux dents « rationnelles » se trouve une dent « irrationnelle » et vice versa.

Exemple $\mathbb{N}$ et $\mathbb{Q}$ sont équipotents. On peut donc numéroter les rationnels, il y a un rationnel n°0, un rationnel n°1, un rationnel n°2, etc.

Démonstration Contentons-nous d'un « sketch of the proof » comme disent les anglo-saxons — un aperçu de la preuve. Nous conservons dans cet exemple les notations f et g des deux exemples précédents.

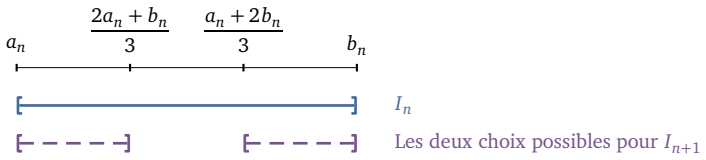
- L'application $n \longmapsto n$ est injective de $\mathbb{N}$ dans $\mathbb{Q}$. En vertu du théorème de Cantor-Bernstein, il nous suffit dès lors d'exhiber une injection de $\mathbb{Q}$ dans $\mathbb{N}$ pour montrer que $\mathbb{N}$ et $\mathbb{Q}$ sont équipotents.
- Rappelons qu'une fraction $r = \dfrac{p}{q}$ est irréductible lorsqu'aucune simplification n'est plus envisageable entre son numérateur et son dénominateur — sauf ± 1, bien sûr. Avec ces notations, l'application qui, à $r \in \mathbb{Q}$, associe $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$ est bien définie et injective. Nous disposons donc d'une injection h de $\mathbb{Q}$ dans $\mathbb{Z}\times\mathbb{N}^*$.
- L'application $n \longmapsto n-1$ est très clairement une bijection de $\mathbb{N}^*$ sur $\mathbb{N}$ — de réciproque $n \longmapsto n+1$. Comme par ailleurs f est bijective de $\mathbb{N}$ sur $\mathbb{Z}$, l'application produit $(m,n) \longmapsto \big(f^{-1}(m), n-1\big)$ est une bijection de $\mathbb{Z}\times\mathbb{N}^*$ sur $\mathbb{N}^2$ sur nous noterons i.
- L'application $h \circ i \circ g$ est finalement injective de $\mathbb{Q}$ dans $\mathbb{N}$ par composition : $\quad \mathbb{Q} \overset{h}{\longrightarrow} \mathbb{Z}\times\mathbb{N}^* \overset{i}{\longrightarrow} \mathbb{N}^2 \overset{g}{\longrightarrow} \mathbb{N}$.

Exemple $\mathbb{R}$ et $\mathbb{Q}$ **ne** sont **pas** équipotents. Il y a donc infiniment plus d'éléments dans $\mathbb{R}$ que dans $\mathbb{Q}$, donc a fortiori infiniment plus d'irrationnels que de rationnels. Le peigne des rationnels et le peigne des irrationnels ont donc à la fois des dents parfaitement alternées (au sens de la remarque faite un peu plus haut) **et** pas le même nombre de dents !

Démonstration Parce que $\mathbb{N}$ et $\mathbb{Q}$ sont équipotents, montrer que $\mathbb{R}$ et $\mathbb{Q}$ ne le sont pas revient à montrer que $\mathbb{R}$ et $\mathbb{N}$ ne le sont pas non plus. Et pour montrer qu'il n'existe pas de bijection de $\mathbb{N}$ sur $\mathbb{R}$, nous allons en fait prouver qu'aucune application de $\mathbb{N}$ dans $\mathbb{R}$ ne peut être surjective, ce sera suffisant.

Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{R}$ une application quelconque. Nous allons montrer que φ n'est pas surjective de $\mathbb{N}$ sur $\mathbb{R}$.

- L'un au moins des intervalles $\left[0,\dfrac{1}{3}\right]$ et $\left[\dfrac{2}{3},1\right]$ **ne** contient **pas** $\varphi(0)$, nous le notons I_0 — si les deux intervalles conviennent, on choisit celui de gauche par exemple. Par construction : $\quad \varphi(0) \notin I_0$. $\quad$ Notons a_0 et b_0 les bornes de I_0, de sorte que $I_0 = [a_0,b_0]$. L'intervalle I_0 a pour longueur $\dfrac{1}{3}$.
- Ensuite on répète. Pour tout $n \in \mathbb{N}$, une fois les intervalles $I_0, I_1, \dots, I_n$ construits, on construit l'intervalle I_{n+1} de la façon suivante. L'un au moins des intervalles $\left[a_n, \dfrac{2a_n+b_n}{3}\right]$ et $\left[\dfrac{a_n+2b_n}{3}, b_n\right]$ **ne** contient **pas** $\varphi(n+1)$, nous le notons I_{n+1} — si les deux intervalles conviennent, on choisit celui de gauche par exemple. Par construction : $\quad \varphi(n+1) \notin I_{n+1}$. $\quad$ Notons a_{n+1} et b_{n+1} les bornes de I_{n+1} : $\quad I_{n+1} = [a_{n+1}, b_{n+1}]$. L'intervalle I_{n+1} a pour longueur $\dfrac{1}{3^{n+1}}$ — la longueur est divisée par 3 à chaque étape.



- Nous avons finalement construit une suite d'intervalles $(I_n)_{n\in\mathbb{N}}$ qui sont emboîtés les uns dans les autres : $\ldots \subset I_3 \subset I_2 \subset I_1 \subset I_0$ et dont la longueur est toujours divisée par 3 d'un rang au suivant. Les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ vérifient donc les propriétés suivantes :
$$a_0 \leqslant a_1 \leqslant a_2 \leqslant \ldots \leqslant b_2 \leqslant b_1 \leqslant b_0 \qquad \text{et pour tout } n\in\mathbb{N} : \quad b_n - a_n = \frac{1}{3^{n+1}}.$$
Ainsi $(a_n)_{n\in\mathbb{N}}$ est croissante, $(b_n)_{n\in\mathbb{N}}$ décroissante et $\lim\limits_{n\to+\infty}(b_n-a_n)=0$. Ces suites sont donc adjacentes, donc convergentes de même limite ℓ en vertu du théorème des suites adjacentes.
- Par construction : $a_n \leqslant \ell \leqslant b_n$ pour tout $n\in\mathbb{N}$ avec $\varphi(n)\notin I_n = [a_n, b_n]$, donc $\ell \neq \varphi(n)$. En d'autres termes, φ ne prend pas la valeur ℓ, donc n'est pas surjective !

Exemple On peut montrer que $\mathbb{R}$, $\mathbb{C}/\mathbb{R}^2$ et $\mathbb{R}^3$ sont équipotents. Il y a donc autant de points sur une droite ou sur un plan que dans notre espace à trois dimensions.

Nous terminerons ce chapitre en beauté par un petit résultat tout bête, mais d'une portée épistémologique et historique considérable.

Théorème (Théorème de Cantor) Il n'existe pas de surjection de E sur $\mathscr{P}(E)$.

Démonstration Soit $\varphi : E \longrightarrow \mathscr{P}(E)$ une application. On pose $A = \big\{x\in E \mid \quad x\notin\varphi(x)\big\}$. Comme A est une partie de E, on peut se demander si A possède ou non un antécédent par φ. Pour tout $x\in E$:

— si $x\in A$: $\quad x\notin\varphi(x)$, $\quad$ donc $\varphi(x)\neq A$,

— si $x\notin A$: $\quad x\in\varphi(x)$, $\quad$ donc $\varphi(x)\neq A$.

Dans les deux cas : $\quad A\neq\varphi(x)$, $\quad$ et ce pour tout x, donc A n'a pas d'antécédent par f. A fortiori, f n'est pas surjective de E sur $\mathscr{P}(E)$.

Dans la mesure où l'application $x\longmapsto\{x\}$ est injective de E dans $\mathscr{P}(E)$, le théorème de Cantor montre au fond que E est toujours strictement plus petit que $\mathscr{P}(E)$ en termes d'équipotence. Il en découle un procédé de construction simple d'infinis de tailles DIFFÉRENTES toujours plus grandes : $\mathbb{N}$, $\mathscr{P}(\mathbb{N})$, $\mathscr{P}\big(\mathscr{P}(\mathbb{N})\big)$, $\mathscr{P}\Big(\mathscr{P}\big(\mathscr{P}(\mathbb{N})\big)\Big)\ldots$ Il n'est pas trop dur de montrer que $\mathscr{P}(\mathbb{N})$ et $\mathbb{R}$ sont équipotents.

À la fin du XIX$^{\text{ème}}$ siècle, Cantor se demande s'il existe ou non entre $\mathbb{N}$ et $\mathscr{P}(\mathbb{N})$ un infini de taille intermédiaire mais n'obtient aucun résultat ni dans un sens ni dans l'autre. L'énoncé selon lequel il N'Y A PAS de tel infini intermédiaire s'appelle depuis l'*hypothèse du continu*.

En 1938, Gödel montre que l'hypothèse du continu ne réfute pas le cadre traditionnel dit *ZFC* des mathématiques. Ce résultat est compliqué à comprendre. Gödel n'a pas montré que l'hypothèse du continu est vraie, mais que si on l'ajoute aux axiomes usuels, la théorie obtenue n'est ni plus ni moins contradictoire que la théorie usuelle ZFC.

En 1963, Cohen montre que l'hypothèse du continu n'est pas démontrable dans la théorie usuelle ZFC. L'hypothèse du continu est donc un de ces énoncés qu'on dit *indécidables*, impossible à prouver, impossible à réfuter.