Applications, relations 10

10.1 Applications entre ensembles

10.1.1 Définitions

Définition 10.1 – Une **application** est un triplet de la forme $f = (E, F, \Gamma)$, où E et F sont deux ensembles et Γ est une partie de $E \times F$ telle que

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

On dit que f est une application de E dans F, E est appelé ensemble de départ de f et F est appelé l'ensemble d'arrivée de F.
Si $(x, y) \in \Gamma$, on note $y = f(x)$.
L'ensemble $\Gamma = \{(x, f(x)),\ x \in E\}$ est appelé **graphe de** f.

Explication
Cela revient à dire que **tout** élément de l'ensemble de départ admet une **unique** image par f.

Pour une application de $\mathbf{R}$ dans $\mathbf{R}$, alors le graphe de f est exactement ce dont on a l'habitude : l'ensemble des couples (x, y) où $y = f(x)$.
Et la condition sur l'existence et l'unicité d'une image a déjà été évoquée précédemment : elle signifie que toute droite verticale rencontre le graphe en un unique point.
En particulier, deux applications f et g sont égales si et seulement si :

- elles ont le même ensemble de départ
- elles ont le même ensemble d'arrivée
- pour tout élément x de leur ensemble de départ, $f(x) = g(x)$.

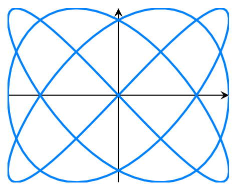


Figure 10.1– Une partie de $\mathbf{R} \times \mathbf{R}$ qui n'est pas le graphe d'une application.

Ainsi, les deux applications $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 \end{array} \right.$ et $g : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R}_+ \\ x & \longmapsto & x^2 \end{array} \right.$ ne sont pas égales car elles n'ont pas le même ensemble d'arrivée[1].

[1] Mais pourtant elles ont même ensemble de départ, et prennent partout les mêmes valeurs.

Définition 10.2 (Identité) – Soit E un ensemble. On appelle **identité de** E l'application $\mathrm{id}_E : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x \end{array} \right.$.

Définition 10.3 (Image, antécédent) – Soit $f : E \to F$ une application.

- Si $x \in E$, et si $y = f(x)$, on dit que y est l'image de x par f.
- Si $y \in F$, et si il existe $x \in E$ tel que $y = f(x)$, on dit que x est un antécédent de y par f.

⚠ L'image d'un élément de l'ensemble de départ est toujours unique, par définition d'une application.
En revanche, un élément de l'ensemble d'arrivée peut ne pas posséder d'antécédents, ou en posséder plusieurs. On prendra donc bien garde à dire **un** antécédent de y et surtout pas[2] l'antécédent de y par f.

Par exemple, si on considère l'application $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 \end{array} \right.$, alors 0 possède un unique antécédent par f qui est 0, 1 possède deux antécédents par f qui sont -1 et 1 et -1 ne possède aucun[3] antécédent par f.

[2] Sauf si pour une raison ou une autre, on sait déjà qu'un tel antécédent est unique.

[3] Le carré d'un nombre réel ne peut être négatif.

Définition 10.4 – Soient E et F deux ensembles. L'ensemble de toutes les applications de E dans F est noté $\mathscr{F}(E,F)$ ou F^E.

Notation

La notation F^E sera motivée plus tard, lorsque nous compterons le nombre d'éléments de $\mathscr{F}(E,F)$ dans le cas où E et F sont finis. Attention au fait que c'est l'espace de départ qui est en exposant.

Exemple 10.5

Il est tout à fait possible de considérer des applications elles-mêmes définies sur des ensembles d'applications. Par exemple, il est possible de considérer l'application $D : \left| \begin{array}{ccc} \mathscr{C}^1(\mathbf{R},\mathbf{R}) & \longrightarrow & \mathscr{F}(\mathbf{R},\mathbf{R}) \\ f & \longmapsto & f' \end{array}\right.$, qui à une fonction associe sa dérivée.

Notons alors $h : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & 0 \end{array}\right.$ la fonction nulle sur $\mathbf{R}$.

Une fonction f de classe $\mathscr{C}^1$ est alors un antécédent de h par D si et seulement si $f' = h$, soit si et seulement si f' est nulle. Ce qui est le cas si et seulement si f est constante.

Définition 10.6 – Si I et E sont deux ensembles, on note parfois $(a_i)_{i\in I}$ au lieu de $a : \left| \begin{array}{ccc} I & \longrightarrow & F \\ i & \longmapsto & a(i) \end{array}\right.$, et on parle alors de famille d'éléments de E indexée par I au lieu de parler d'application.

En particulier, une suite, qui est une famille indicée par $\mathbf{N}$ n'est rien d'autre qu'une application de $\mathbf{N}$ dans $\mathbf{R}$ (ou dans $\mathbf{C}$ pour les suites complexes).
On préfère alors largement[4] la notation $(u_n)_{n\in\mathbf{N}}$ à $u : n \mapsto u(n)$.
L'ensemble des suites réelles est donc noté $\mathscr{F}(\mathbf{N},\mathbf{R})$, ou encore $\mathbf{R}^{\mathbf{N}}$.

[4] Par habitude...

10.1.2 Composition d'applications

Définition 10.7 – Soient E, F, G trois ensembles, et soient $f \in \mathscr{F}(E,F)$ et $g \in \mathscr{F}(F,G)$ deux applications. On appelle composée de g et f, et on note $g \circ f$ l'application de E dans G définie par :

$$\forall x \in E,\ (g\circ f)(x) = g(f(x)).$$

Remarque

Si on veut que la composition ait bien un sens, il faut nécessairement que l'espace d'arrivée de f soit l'espace de départ de g, afin qu'on puisse bien appliquer g à $f(x)$.

⚠ Le sens dans lequel on effectue la composition est important : même dans les cas où $g\circ f$ et $f \circ g$ sont toutes les deux bien définies[5], en règle générale ces deux applications ne sont pas égales.

Par exemple, si $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \sin(x) \end{array}\right.$ et $g : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x+2\pi \end{array}\right.$, alors $\forall x \in \mathbf{R}$,

$$(g\circ f)(x) = g(\sin(x)) = \sin(x) + 2\pi \neq \sin(x+2\pi) = \sin(g(x)) = (f\circ g)(x).$$

[5] C'est-à-dire lorsque $G = E$, soit

$$f : E \to F$$

et $g : F \to E$.

Notons qu'on a toujours, pour $f : E \to F$,

$$\mathrm{id}_F \circ f = f \circ \mathrm{id}_E = f.$$

Terminologie

On dit que id est un élément neutre pour la composition.

Dans le cas particulier où l'espace de départ et l'espace d'arrivée de f sont égaux, alors on peut composer f avec elle-même. Puis composer cette composée avec f, etc.

Définition 10.8 – Soit E un ensemble et soit $f : E \to E$.
On pose alors $f^0 = \mathrm{id}_E$ et pour tout $n \in \mathbf{N}$, on pose $f^{n+1} = f \circ f^n$.
Autrement dit, pour tout $n \in \mathbf{N}^*$, on a $f^n = \underbrace{f\circ f \circ \cdots \circ f}_{n \text{ fois}}$.

Cette notation a un léger inconvénient, c'est qu'elle peut être confondue avec le produit (pour peu que E soit un espace dans lequel on a un produit clairement défini). Lorsqu'il y risque de confusion, on note parfois $f^{\circ n}$ au lieu de f^n.

Il est alors très facile de se convaincre que pour tous $k, n \in \mathbf{N}$, $f^k \circ f^n = f^n \circ f^k = f^{k+n}$. En revanche, lorsqu'on compose trois applications ou plus, l'ordre dans lequel la composition est effectuée n'a pas d'importance, comme le prouve la proposition suivante :

Proposition 10.9 (Associativité de la composition) : *Soient $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications. Alors $(h \circ g) \circ f = h \circ (g \circ f)$.*

Démonstration. Commençons par noter que $h \circ (g \circ f)$ et $(h \circ g) \circ f$ ont toutes deux E comme espace de départ et H comme espace d'arrivée. De plus, pour $x \in E$, on a

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

et

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

Et ceci étant vrai pour tout $x \in E$, on a bien $(h \circ g) \circ f = h \circ (g \circ f)$. □

10.1.3 Restriction, prolongements

Définition 10.10 – Soit $f : E \to F$ et soit A une partie de E. On appelle **restriction de f à A** l'application $f_{|A} : \left| \begin{array}{ccc} A & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$.
Autrement dit, $f_{|A}$ n'est rien d'autre que l'application f, mais vue comme une application définie sur A uniquement[6].

[6] Donc avec un ensemble de départ plus petit.

Exemple 10.11

La fonction cos n'est pas monotone sur $\mathbf{R}$, car $f(0) = f(2\pi) = 1$.
En revanche, $\cos_{[0,\pi]} : \left| \begin{array}{ccc} [0,\pi] & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \cos x \end{array} \right.$ est strictement décroissante sur $[0, \pi]$.

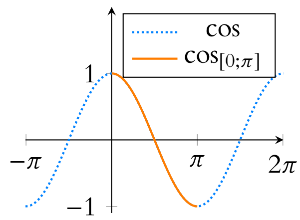


FIGURE 10.2– Les graphes de cos et $\cos_{[0,\pi]}$.

Définition 10.12 – Soit $f : E \to F$ et soit E' un ensemble tel que $E \subset E'$. On appelle **prolongement de f à E'** toute application $g : E' \to F$ telle que $\forall x \in E,\ f(x) = g(x)$.

Autrement dit
Un prolongement de f à E' est toute application définie sur un ensemble E' contenant E, telle que $g : E' \to F$ telle que $g_{|E} = f$.

On prendra garde au fait qu'un prolongement de f n'est pas nécessairement unique.
Par exemple, les deux fonctions $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \begin{cases} 0 & \text{si } x < 0 \\ x & \text{si } x \geqslant 0 \end{cases} \end{array} \right.$ et $g : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & |x| \end{array} \right.$ sont deux prolongement à $\mathbf{R}$ de la fonction $\mathrm{id}_{[0,+\infty[}$, puisque pour tout $x \geqslant 0$, $f(x) = g(x) = x$.

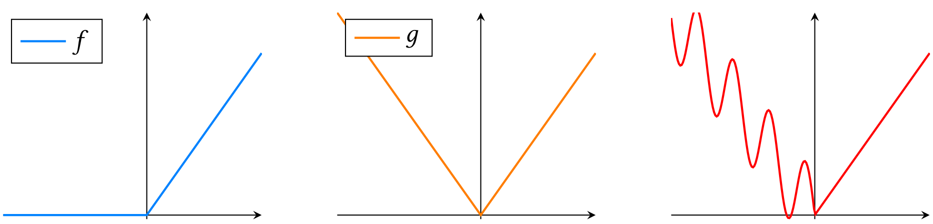


FIGURE 10.3 – Trois prolongements possibles de $\mathrm{id}_{[0,+\infty[}$.

Définition 10.13 – Soit $f : E \to F$, et soit B une partie de F. On dit que f est à valeurs dans B si pour tout $x \in E$, $f(x) \in B$.

Exemples 10.14

La fonction $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & \sqrt{x+1} \end{array} \right.$ est à valeurs dans $[1, +\infty[$.

L'application $g : \left| \begin{array}{ccc} \mathbf{R}^2 & \longrightarrow & \mathbf{R}^2 \\ (x,y) & \longmapsto & (x^2, y^3) \end{array} \right.$ est à valeurs dans $\mathbf{R}_+ \times \mathbf{R}$.

Définition 10.15 – Soit $f : E \to F$ et soit B une partie de F telle que $\operatorname{Im}(f) \subset B$ (autrement dit, telle que $\forall x \in E,\ f(x) \in B$).
La corestriction de f à B est alors l'application $f^{|B} : \left| \begin{array}{ccc} E & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array} \right.$.

La plupart du temps on confond[7] f et $f^{|B}$, par exemple, lorsqu'on dit que Arctan réalise une bijection de $\mathbf{R}$ sur $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$, il faudrait plutôt dire que $\operatorname{Arctan}^{|]-\frac{\pi}{2},\frac{\pi}{2}[}$ est une bijection, mais cette notation est inutilement lourde, et on préfère se contenter d'une phrase qui précisera quels sont les ensembles de départ et d'arrivée que l'on considère.

[7] Abusivement !

Définition 10.16 – Soit $f : E \to E$ et soit $A \subset E$. On dit que A est **stable par f** si pour tout $x \in A$, $f(x) \in A$.

Exemple 10.17

Pour tout $\alpha \in \mathbf{R}_+$, $[0,1]$ est stable par $f_\alpha : x \mapsto x^\alpha$.
En effet, si $0 \leqslant x \leqslant 1$, alors par croissance de f_α, $0 = f_\alpha(0) \leqslant f_\alpha(x) \leqslant f_\alpha(1) = 1$.
Donc $f_\alpha(x) \in [0,1]$.

Définition 10.18 – Soit $f : E \to F$ et soit A une partie de E stable par f. On appelle **application induite par f sur A** l'application

$$u_{|A}^{|A} : \left| \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & u(x) \end{array} \right. .$$

10.1.4 Image directe, image réciproque

Définition 10.19 – Soit $f \in \mathscr{F}(E,F)$, et soit $A \subset E$. On appelle **image directe** de A par f et on note $f(A)$ la partie de F définie par

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

Rédaction Quand on souhaite prendre un élément dans $f(A)$, la rédaction n'est surtout pas «soit $f(x) \in f(A)$», mais «soit $y \in f(A)$. Alors il existe $x \in A$ tel que $y = f(x)$».

L'image directe de A est donc l'ensemble des élément de F qui possèdent au moins un antécédent dans A. C'est également l'ensemble des images de tous les éléments de A.

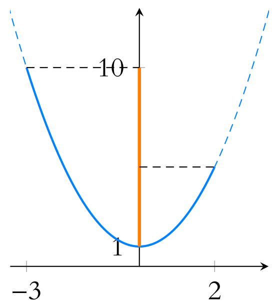


FIGURE 10.4– L'image (en orange) de $[-3, 2]$ par $x \mapsto x^2 + 1$.

Exemples 10.20

- Si $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2+1 \end{array} \right.$, alors $f(\mathbf{R}) = f([0,+\infty[) = f(]-\infty, 0]) = [1, +\infty[$ et $f(]-3,2[) = [1, 10[$.
- $\sin(\mathbf{R}) = [-1,1]$ et $\operatorname{Arctan}([0,+\infty[) = \left[0, \frac{\pi}{2}\right[$.
- L'image de $\mathbf{R}$ par la fonction $z \mapsto e^{i\theta}$ est $\mathbf{U}$.

En revanche, l'image de $\mathbf{C}$ par la même application est $\mathbf{C}^*$. En effet, si $z = re^{i\theta} \in \mathbf{C}^*$,

alors $r \neq 0$ et donc $z = e^{\ln r + i\theta}$ est bien dans l'image de l'exponentielle.
▶ On a toujours $f(\emptyset) = \emptyset$, et si $A \neq \emptyset$, alors $f(A) \neq \emptyset$. En effet, dans ce cas, A contient au moins un élément x, et donc $f(A)$ contient au moins l'élément $f(x)$.

Définition 10.21 – Soit $f \in \mathscr{F}(E, F)$. On appelle alors image de f et on note $\mathrm{Im}(f)$ l'ensemble $f(E)$.

Pour le dire autrement, $\mathrm{Im}(f)$ est l'ensemble des éléments de F qui admettent au moins un antécédent par f.

Définition 10.22 – Soit $f \in \mathscr{F}(E, F)$, et soit $B \subset F$. On appelle **image réciproque de** B **par** f la partie de E définie par

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

⚠ Attention ! On ne peut considérer que l'image réciproque d'une partie de F (l'ensemble d'arrivée), et cette image réciproque est une partie de E (l'ensemble de départ).

⚠ La notation $f^{-1}(B)$, bien qu'étant celle que tout le monde utilise est source de confusion : la fonction s'appelle toujours f, et il n'y a pas nécessairement d'application nommée f^{-1} derrière cette notation.

Toutefois, il se peut qu'un tel f^{-1} existe[8], et alors comment savoir si $f^{-1}(B)$ désigne l'image réciproque de B par f ou l'image directe de B par f^{-1} ?
Bonne nouvelle, il s'agit de la même chose comme nous le prouverons plus loin.

[8] Cf. ci-dessous, mais vous connaissez déjà la notion de bijection pour les fonctions définies sur (une partie de) $\mathbf{R}$.

Exemples 10.23

Si $f : A \to \mathbf{R}$, où A est une partie de $\mathbf{R}$, alors déterminer l'image réciproque d'un singleton $\{y\}$, c'est trouver l'ensemble des solutions à l'équation $y = f(x)$.
De même, déterminer l'image réciproque d'un intervalle $[a, b]$, c'est résoudre l'inéquation $a \leqslant f(x) \leqslant b$, d'inconnue $x \in A$.
Contrairement à l'image directe, on peut avoir $f^{-1}(B) = \emptyset$ sans que B soit vide.
Par exemple, pour la fonction sin : $\mathbf{R} \to \mathbf{R}$, on a $\sin^{-1}([3, 4]) = \emptyset$.

10.2 Injections, surjections, bijections

10.2.1 Définitions

Définition 10.24 (Injection) – Soient E et F deux ensembles et soit f une application de E dans F. On dit que f est injective (ou encore que f est une injection) si elle vérifie l'une des trois propriétés équivalentes suivantes :

i) $\forall (x, x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'$
ii) pour tout $y \in F$, l'équation $y = f(x)$ possède au plus une solution $x \in E$
iii) tout élément de F possède **au plus** un antécédent par f.

☠ Danger ! Cela ne veut pas dire que tout élément a un antécédent, mais qu'il ne peut pas en avoir deux distincts !

Démonstration. Il faut prouver que ces trois points sont bien équivalents. Montrons pour cela que *i)* ⇒ *ii)* ⇒ *iii)* ⇒ *i)* (on parle de raisonnement circulaire).
▶ *i)* ⇒ *ii)*. Supposons que $\forall (x, x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'$.
Soit alors $y \in F$, et supposons que x_1, x_2 sont deux solutions de $y = f(x)$.
Alors $f(x_1) = y = f(x_2)$, et donc $x_1 = x_2$. Donc l'équation $y = f(x)$ possède au plus une solution.
▶ *ii)* ⇒ *iii)* Par définition, un antécédent de $y \in F$ est une solution de $y = f(x)$.
Donc pour $y \in F$, $y = f(x)$ possède au plus une solution si et seulement si y possède au plus un antécédent. Nous avons donc prouvé plus qu'annoncé : *ii)* ⇔ *iii)*.

☠ Danger ! Rien ne garantit qu'elle en possède toujours une !

▶ *iii)* ⇒ *i)*. Supposons que tout élément de F possède au plus un antécédent, et soient $(x, x') \in E^2$ tels que $f(x) = f(x')$.

Alors, par définition, x est un antécédent de $f(x)$. Mais puisque $f(x') = f(x)$, x' est aussi un antécédent de $f(x)$.
Et donc $x = x'$. Donc *iii)* $\Rightarrow$ *i)*, de sorte que nos trois assertions sont bien équivalentes. □

Exemples 10.25

- Pour tout ensemble E, id_E est injective.
En effet, si $x, y \in E$ sont tels que $\mathrm{id}_E(x) = \mathrm{id}_E(y)$, alors $x = \mathrm{id}_E(x) = \mathrm{id}_E(y) = y$.
- $f : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 \end{array} \right.$ n'est pas injective, puisque $f(2) = 4 = f(-2)$.
En revanche, $f : \left| \begin{array}{ccc} \mathbf{R}_+ & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 \end{array} \right.$ est injective.

Méthode
Si vous trouvez deux éléments distincts de même image, vous avez tout de suite prouvé que votre application n'est pas injective.

Proposition 10.26 : *Soit A une partie de $\mathbf{R}$ et soit $f : A \to \mathbf{R}$. Si f est strictement monotone, alors elle est injective.*

⚠ Attention !
Ce résultat est faux si on se contente d'applications monotones.

Démonstration. Donnons la preuve dans le cas d'une fonction strictement croissante.
Soient donc $x, x' \in E$ tels que $f(x) = f(x')$.
On ne peut avoir $x < x'$ car on aurait alors $f(x) < f(x')$.
De même, $x' < x$ impliquerait $f(x') < f(x)$.
Donc nécessairement, $x = x'$. □

Définition 10.27 (Surjection) – Soit f une application de E dans F. On dit que f est surjective si tout élément de F possède au moins un antécédent par f. Autrement dit si pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$.

Notons que cela revient à dire que pour tout $y \in F$, l'équation $y = f(x)$, d'inconnue $x \in E$ possède au moins une solution.
En particulier, f est surjective si et seulement si $\mathrm{Im}(f) = F$.

Exemples 10.28

L'application $f : \left| \begin{array}{ccc} \mathbf{R}^2 & \longrightarrow & \mathbf{R} \\ (x,y) & \longmapsto & x^2 + y \end{array} \right.$ est surjective.
En effet, le réel x admet pour antécédent $(0, x)$.
- L'application $g : \left| \begin{array}{ccc} \mathbf{C} & \longrightarrow & \mathbf{C} \\ z & \longmapsto & z^2 - 2z + 5 \end{array} \right.$ est surjective.
En effet, pour $\alpha \in \mathbf{C}$, l'équation $f(z) = \alpha \Leftrightarrow z^2 - 2z + (5 - \alpha)$ possède toujours une solution[9] dans $\mathbf{C}$.
En revanche, $h : \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & x^2 - 2x + 5 \end{array} \right.$ n'est pas surjective, car 0 n'admet pas d'antécédent : l'équation $x^2 - 2x + 5 = 0$ n'admet pas de solution réelle.

[9] Et le plus souvent deux solutions.

10.2.2 Liens avec la composition

Proposition 10.29 : *Soient $f : E \to F$ et $g : F \to G$.*
1. *Si f et g sont injectives, alors $g \circ f$ est injective.*
2. *Si $g \circ f$ est injective, alors f est injective.*
3. *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
4. *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration. 1. Soient $x, y \in E$ tels que $(g \circ f)(x) = (g \circ f)(y) \Leftrightarrow g(f(x)) = g(f(y))$. Puisque g est injective, alors $f(x) = f(y)$. Et donc par injectivité de f, $x = y$. Ainsi, $g \circ f$ est injective.

2. Supposons $g \circ f$ injective, et soient $x, y \in E$ tels que $f(x) = f(y)$. Alors[10] $g(f(x)) = g(f(y))$, et donc par injectivité de $g \circ f$, $x = y$. Donc f est injective.

3. Supposons f et g surjectives, et soit $z \in G$.
Par surjectivité de g, il existe $y \in F$ tel que $z = g(y)$.
Et par surjectivité de f, il existe $x \in E$ tel que $y = f(x)$, et donc $z = (g \circ f)(x)$.
Ainsi, tout élément de G possède un antécédent par $g \circ f$, qui est donc surjective.

4. Supposons $g \circ f$ surjective.
Alors pour tout $y \in G$, il existe un élément $x \in E$ tel que $y = (g \circ f)(x) = g(f(x))$.
Et donc en posant $z = f(x)$, il existe $z \in F$ tel que $y = g(z)$: g est surjective.

□

[10] Deux éléments égaux ont même image par g !

Remarque. Toutes ces implications ne sont en aucun cas des équivalences, et c'est d'ailleurs un bon exercice que de chercher des cas où les implications réciproques sont fausses.

10.2.3 Bijections

Définition 10.30 – Une application $f : E \to F$ est dite **bijective** si elle est à la fois injective et surjective.
Autrement si tout élément F possède un unique antécédent par f :

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

Explication
La surjectivité garantit l'existence d'au moins un antécédent, l'injectivité fournit alors l'unicité.

Remarque. On dit généralement que f est une bijection, ou mieux : qu'elle réalise une bijection de E sur F.
En particulier, on utilisera cette terminologie lorsque que f est injective, mais que son image n'est pas F tout entier. Dans ce cas, f n'est pas bijective, mais en revanche sa corestriction à $\operatorname{Im} f$ l'est.
Comme on ne fait généralement pas vraiment la différence entre f et $f^{|\operatorname{Im} f}$, on dit généralement que «f réalise une bijection de E sur $\operatorname{Im} f$» plutôt que $f^{|\operatorname{Im} f}$ est bijective».
Par exemple, l'exponentielle réalise une bijection de $\mathbf{R}$ sur $\mathbf{R}_+^*$, plutôt que $\exp^{|\mathbf{R}_+^*}$ est bijective.

Exemples 10.31

- id_E est toujours bijective.
- Le théorème de la bijection stipule que si f est continue sur $[a, b]$, strictement croissante (resp. décroissante), alors f réalise une bijection de $[a, b]$ sur $[f(a), f(b)]$ (resp. $[f(b), f(a)]$).
L'injectivité provient en fait de la stricte monotonie, et la surjectivité du théorème des valeurs intermédiaires[11].

[11] Que nous prouverons rigoureusement bientôt.

Proposition 10.32 : *Soit $f : E \to F$. Alors f est une bijection si et seulement si il existe $g : F \to E$ telle que* $\begin{cases} g \circ f = \mathrm{id}_E \\ f \circ g = \mathrm{id}_F \end{cases}$.
*Un tel g, lorsqu'il existe est unique. On l'appelle **bijection réciproque de** f, on le note f^{-1}, et il s'agit de l'application qui à tout $x \in F$ associe son unique antécédent par f.*

Démonstration. Supposons que f soit bijective. Alors tout élément $x \in F$ possède un unique antécédent par f. Notons $g(x)$ cet antécédent, définissant ainsi une application $g : F \to E$.
Par définition[12], pour tout $x \in F$, on a $f(g(x)) = x = \mathrm{id}_F(x)$, et donc $f \circ g = \mathrm{id}_F$.
D'autre part, pour $x \in E$, $f(x) \in F$ possède x comme antécédent, nécessairement unique car f est bijective, et donc $g(f(x)) = x = \mathrm{id}_E(x)$, de sorte que $g \circ f = \mathrm{id}_E$.

[12] $g(x)$ est un antécédent de x par f.

Inversement, supposons qu'il existe $g : F \to E$ tel que $\begin{cases} g \circ f = \mathrm{id}_E \\ f \circ g = \mathrm{id}_F \end{cases}$.
Puisque $g \circ f = \mathrm{id}_E$ est injective, alors par la proposition 10.29, f est injective.
De même, $f \circ g = \mathrm{id}_F$ est surjective, et donc f est surjective.
Donc f est une bijection.

Il reste à prouver l'unicité de g. Supposons donc qu'il existe deux applications g_1 et g_2 de F dans E telles que $\begin{cases} g_1 \circ f = g_2 \circ f = \mathrm{id}_E \\ f \circ g_1 = f \circ g_2 = \mathrm{id}_F \end{cases}$.
Composons alors à droite la première relation par g_1. Il vient alors

$$g_2 \circ f \circ g_1 = \mathrm{id}_E \circ g_1 \Leftrightarrow g_2 \circ \mathrm{id}_F = g_1 \Leftrightarrow g_2 = g_1.$$

□

Remarquons que si f est bijective, alors pour $x \in E$ et $y \in F$, on a $y = f(x) \Leftrightarrow x = f^{-1}(y)$.

Danger ! Ceci ne vaut que si vous savez déjà f bijective. Sans ça, il est **interdit** d'écrire f^{-1}.

Corollaire 10.33 – *Si $f : E \to F$ est bijective, alors $f^{-1} : F \to E$ est bijective, et $(f^{-1})^{-1} = f$.*

Démonstration. On a $f \circ f^{-1} = \mathrm{id}_F$ et $f^{-1} \circ f = \mathrm{id}_E$.
Par la proposition précédente, ceci prouve que f^{-1} est bijective et que sa bijection réciproque est f. □

Exemple 10.34 Détermination d'une bijection réciproque

Soit f l'application $f : \left| \begin{array}{ccc} \mathbf{R}^3 & \longrightarrow & \mathbf{R}^3 \\ (x,y,z) & \longmapsto & (y-3z, -x+y-z, -x+y) \end{array} \right.$.
Nous allons prouver que f est bijective, et déterminer du même coup sa bijection réciproque.

Soit $(a,b,c) \in \mathbf{R}^3$. Alors pour $(x,y,z) \in \mathbf{R}^3$, on a

$$(a,b,c) = f(x,y,z) \Leftrightarrow \begin{cases} y - 3z = a \\ -x+y-z = b \\ -x+y = c \end{cases} \Leftrightarrow \begin{cases} x - y = -c \\ y - 3z = a \\ z = -b+c \end{cases} \Leftrightarrow \begin{cases} x = a - 3b + 2c \\ y = a - 3b + 3c \\ z = -b + c \end{cases}$$

Ainsi, tout élément de $\mathbf{R}^3$ possède un **unique** antécédent, donc f est bijective.
Mieux : nous avons déterminé quel est l'unique antécédent de $(a,b,c) \in \mathbf{R}^3$ par f, donc nous connaissons f^{-1} : il s'agit de l'application

$$f^{-1} : \left| \begin{array}{ccc} \mathbf{R}^3 & \longrightarrow & \mathbf{R}^3 \\ (a,b,c) & \longmapsto & (a-3b+2c, a-3b+3c, -b+c) \end{array} \right. .$$

Il est bien entendu possible de vérifier qu'alors $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_{\mathbf{R}^3}$, mais ce n'est pas indispensable !

Proposition 10.35 : *Soient $f : E \to F$ et $g : F \to G$ deux bijections. Alors $g \circ f$ est une bijection de E dans G, et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Démonstration. Notons que $g \circ f : E \to G$ et $f^{-1} \circ g^{-1} : G \to E$. On a alors

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

Et de même,

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

Et donc $g \circ f$ est bijective, de réciproque égale à $f^{-1} \circ g^{-1}$. □

⚠ On prendra bien garde au fait que l'ordre change lorsqu'on passe à la bijection réciproque : la bijection réciproque de $g \circ f$ n'est pas $g^{-1} \circ f^{-1}$!
De toutes façons, si $E \neq G$, $g^{-1} \circ f^{-1}$ n'a aucun sens[13], alors que $f^{-1} \circ g^{-1}$ est bien définie.
Une analogie simple mais efficace : le matin vous commencez par mettre vos chaussettes (c'est f), puis vous enfilez vos chaussures (c'est g).
Le soir, pour vous déshabiller (c'est donc $(g \circ f)^{-1}$) vous commencez par enlever vos chaussures (donc g^{-1}), puis vous enlevez vos chaussettes (c'est f^{-1}). Et sûrement pas le contraire !

[13] L'espace de départ de g^{-1} n'est pas l'espace d'arrivée de f^{-1}.

Corollaire 10.36 – *Si $f : E \to E$ est bijective, alors $\forall n \in \mathbf{N}$, f^n est bijective, et $(f^n)^{-1} = (f^{-1})^n = \underbrace{f^{-1} \circ f^{-1} \circ \cdots \circ f^{-1}}_{n \text{ fois}}$.*

Démonstration. Par récurrence sur n. □

Définition 10.37 – Si $f : E \to E$ est bijective[14], alors pour n entier strictement négatif, on note $f^n = (f^{-1})^{|n|}$.

[14] Et seulement dans ce cas-là, bijective avec espace de départ et d'arrivée égaux.

Remarques. ► La valeur absolue est confusante : on a bien $f^{-2} = f^{-1} \circ f^{-1}$, $f^{-3} = f^{-1} \circ f^{-1} \circ f^{-1}$, etc.
► On a alors, pour tous $(k, n) \in \mathbf{Z}^2$, $f^n \circ f^k = f^{n+k}$.

Prouvons à présent un fait énoncé précédemment : si $f : E \to F$ est bijective, alors l'image réciproque de $B \subset F$ par f et l'image directe de B par f^{-1} sont égales (et donc la notation $f^{-1}(B)$ ne prête pas à confusion).
Notons $A_1 = \{x \in E \mid f(x) \in B\}$ l'image réciproque de B par f^{-1} et $A_2 = \{f^{-1}(y), , y \in B\}$ l'image directe de B par f^{-1}. Alors

$$x \in A_1 \Leftrightarrow f(x) \in B \Leftrightarrow \exists y \in B,\ f(x) = y \Leftrightarrow \exists y \in B,\ x = f^{-1}(y) \Leftrightarrow x \in A_2.$$

Et donc on a bien $A_1 = A_2$.

10.2.4 Fonction indicatrice d'une partie

Nous définissons à présent des fonctions qui sont d'apparence assez simple, mais sont en fait assez utiles, et nous nous en servirons notamment en probabilités.

Définition 10.38 – Soit E un ensemble, et soit A une partie de E. On appelle fonction indicatrice de A et on note $\mathbb{1}_A$ la fonction définie sur E par

$$\forall x \in E,\ \mathbb{1}_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

Autrement dit, un élément $x \in E$ est dans A si et seulement si $\mathbb{1}_A(x) = 1$.
Notons que $\mathbb{1}_A$ ne prend que les valeurs 0 et 1 (et même que la valeur 0 si $A = \emptyset$), et qu'en particulier, $\mathbb{1}_A^2 = \mathbb{1}_A$.
Beaucoup de propriétés ensemblistes se lisent sur les fonctions indicatrices :

Exercice
Inversement, montrer que si $f : E \to \mathbf{R}$ vérifie $f^2 = f$, alors il existe $A \in \mathscr{P}(E)$ telle que $f = \mathbb{1}_A$.

Proposition 10.39 : *Soit E un ensemble, et soient $A, B \in \mathscr{P}(E)$. Alors*
- ► $A \subset B \Leftrightarrow \mathbb{1}_A \leqslant \mathbb{1}_B$ *(c'est-à-dire si et seulement si $\forall x \in E$, $\mathbb{1}_A(x) \leqslant \mathbb{1}_B(x)$)*
- ► $\mathbb{1}_{\overline{A}} = 1 - \mathbb{1}_A$
- ► $\mathbb{1}_{A \cap B} = \mathbb{1}_A \mathbb{1}_B$
- ► $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A \cap B}$

Démonstration. ► Supposons $A \subset B$. Alors pour $x \in A$, $x \in B$, et donc $\mathbb{1}_A(x) = 1 = \mathbb{1}_B(x)$.
Et pour $x \in E \setminus A$, $\mathbb{1}_A(x) = 0 \leqslant \mathbb{1}_B(x)$.

Inversement, si $\mathbb{1}_A \leqslant \mathbb{1}_B$, alors pour $x \in A$, on a $\mathbb{1}_A(x) = 1$, et donc[15] nécessairement, $\mathbb{1}_B(x) = 1$, de sorte que $x \in B$.
Donc $A \subset B$.
► Pour $x \in E$, on a deux cas de figure :
Soit $x \in A$, et alors $1 - \mathbb{1}_A(x) = 0 = \mathbb{1}_{\overline{A}}(x)$.
Soit $x \notin A$, et alors $1 - \mathbb{1}_A(x) = 1 = \mathbb{1}_{\overline{A}}(x)$.
Donc on a bien $\mathbb{1}_{\overline{A}} = 1 - \mathbb{1}_A$.
► Si A et B sont deux parties de E, alors $\mathbb{1}_{A\cap B} = \mathbb{1}_A \mathbb{1}_B$.
En effet, si $x \in A \cap B$, alors $\mathbb{1}_A(x) = \mathbb{1}_B(x) = 1$, et donc $\mathbb{1}_A(x)\mathbb{1}_B(x) = 1 = \mathbb{1}_{A\cap B}(x)$.
Inversement, si $x \notin A \cap B$, alors $x \notin A$ ou $x \notin B$, de sorte que $\mathbb{1}_A(x) = 0$ ou $\mathbb{1}_B(x) = 0$, et donc $\mathbb{1}_A(x)\mathbb{1}_B(x) = 0 = \mathbb{1}_{A\cap B}(x)$.
Ainsi, pour tout $x \in E$, $\mathbb{1}_{A\cap B}(x) = \mathbb{1}_A(x)\mathbb{1}_B(x)$, et donc $\mathbb{1}_{A\cap B} = \mathbb{1}_A \mathbb{1}_B$.
► Nous pourrions là aussi distinguer plusieurs cas, mais notons plutôt que $A \cup B = \overline{\overline{A} \cap \overline{B}}$ et donc

$$\mathbb{1}_{A\cup B} = 1 - \mathbb{1}_{\overline{A}}\mathbb{1}_{\overline{B}} = 1 - (1 - \mathbb{1}_A)(1 - \mathbb{1}_B) = 1 - 1 + \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A\mathbb{1}_B.$$

□

[15] $\mathbb{1}_B(x) \in \{0, 1\}$.

Proposition 10.40 : *Soit E un ensemble. Alors $f : \left|\begin{array}{ccc} \mathscr{P}(E) & \longrightarrow & \mathscr{F}(E, \{0,1\}) \\ A & \longmapsto & \mathbb{1}_A \end{array}\right.$ est une bijection de $\mathscr{P}(E)$ sur $\mathscr{F}(E, \{0,1\})$.*
Autrement dit, une partie de E est entièrement caractérisée par sa fonction indicatrice.

Démonstration. Montrons que f est injective. Soient donc A, B deux parties de E telles que $f(A) = f(B) \Leftrightarrow \mathbb{1}_A = \mathbb{1}_B$.
Alors pour tout $x \in E$, on a $\mathbb{1}_A(x) = \mathbb{1}_B(x)$.
Et par conséquent,

$$x \in A \Leftrightarrow \mathbb{1}_A(x) = 1 \Leftrightarrow \mathbb{1}_B(x) = 1 \Leftrightarrow x \in B.$$

Donc $A = B$, de sorte que f est injective.

Prouvons à présent que f est bijective. Soit $\chi : E \to \{0, 1\}$.
Il s'agit de prouver qu'il existe $A \in \mathscr{P}(E)$ tel que $\chi = \mathbb{1}_A$.
Posons $A = \chi^{-1}(\{1\}) = \{x \in E \mid \chi(x) = 1\}$.
Alors $A \subset E$, et on a, pour tout $x \in E$,

$$\mathbb{1}_A(x) = 1 \Leftrightarrow x \in A \Leftrightarrow \chi(x) = 1.$$

Et donc $\mathbb{1}_A = \chi$, de sorte que $\chi = f(A)$.
Donc f est surjective, et par conséquent bijective. □

Remarque. Notons au passage que la preuve de la surjectivité nous a donné l'unique antécédent de χ par f, et donc la bijection réciproque de f est

$$f^{-1} : \left|\begin{array}{ccc} \mathscr{F}(E, \{0,1\}) & \longrightarrow & \mathscr{P}(E) \\ \chi & \longmapsto & \chi^{-1}(\{1\}) \end{array}\right. .$$

10.3 INTRODUCTION À LA NOTION DE CARDINAL

10.3.1 Ensembles finis

Définition 10.41 – Un ensemble E est dit **fini** s'il est vide ou s'il existe un entier $n \in \mathbf{N}^*$ et une bijection $\varphi : [\![1, n]\!] \to E$.
Si un tel n n'existe pas, on dit que E est infini.

L'intuition derrière cette définition est qu'un ensemble fini est un ensemble dont on peut «compter» les éléments.
C'est exactement ce que fait une bijection de $[\![1, n]\!]$ dans E : elle établit une correspondance entre les nombres de 1 à n et les éléments de E, telle qu'à chaque nombre correspond un unique élément de E et vice-versa.

Exemple 10.42

L'ensemble des élèves de MPSI2 est fini : on peut les numéroter à l'aide des éléments de $[\![1,48]\!]$.
Et il y a plein de manières de le faire : je peux prendre l'ordre alphabétique, votre classement au dernier DS, etc.

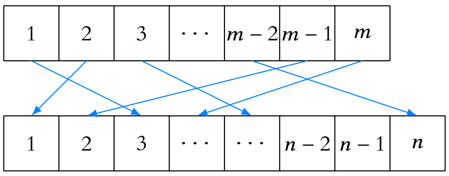
Lemme 10.43. Soient $(m,n) \in (\mathbf{N}^*)^2$. Alors il existe une injection $[\![1,m]\!] \to [\![1,n]\!]$ si et seulement si $m \leqslant n$.

Démonstration. Si $m \leqslant n$, il est clair que l'application $\varphi : \left| \begin{array}{ccc} [\![1,m]\!] & \longrightarrow & [\![1,n]\!] \\ k & \longmapsto & k \end{array}\right.$ est une injection.
Pour la réciproque, raisonnons par récurrence sur m, en prouvant la propriété $\mathscr{P}(m)$: «s'il existe $n \in \mathbf{N}^*$ et une injection de $[\![1,m]\!]$ dans $[\![1,n]\!]$, alors $m \leqslant n$.»
Pour $m = 1$, la proposition est évidemment vraie, puisqu'un élément $n \in \mathbf{N}^*$ est supérieur ou égal à 1.
Supposons donc $\mathscr{P}(m)$ vraie, et supposons qu'il existe une injection f de $[\![1,m+1]\!]$ dans $[\![1,n]\!]$.
Notons qu'on ne peut avoir $n = 1$, car alors on aurait $f(1) = f(2) = 1$, contredisant l'injectivité de f.
Alors, pour tout $k \in [\![1,m]\!]$, $f(k) \neq f(m+1)$.

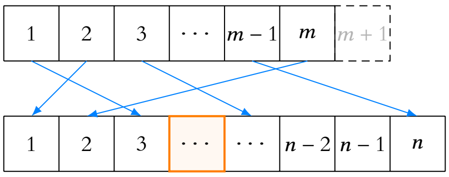
Soit alors $g : \left| \begin{array}{ccc} [\![1,m]\!] & \longrightarrow & [\![1,n-1]\!] \\ k & \longmapsto & \begin{cases} f(k) & \text{si } f(k) < f(m+1) \\ f(k)-1 & \text{si } f(k) > f(m+1) \end{cases} \end{array}\right.$

Alors g est injective. En voici la preuve en image :

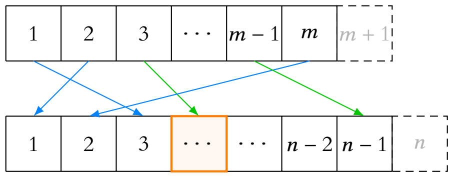
Un dessin ?
Je vois venir la question : «quand est-ce qu'un dessin est une preuve ?». La réponse est simple : quand c'est moi qui le fais !



Au départ f est une injection, donc deux éléments distincts pointent sur deux cases distinctes.



On «libère» la case $f(m+1)$ vers laquelle plus rien ne pointe.



Toutes les flèches qui arrivaient à droite de la case libérée sont décalées d'un rang vers la gauche. Il n'y a donc toujours pas deux flèches qui pointent vers la même case : g est une injection.

Notez bien que si jamais $f(m+1) = n$, alors g n'est rien d'autre que la restriction de f à $[\![1,m]\!]$: $\forall k \in [\![1,m-1]\!]$, $g(k) = f(k)$ (autrement dit, on n'a rien décalé, on a juste supprimé la dernière flèche).

Comme je sens qu'un dessin vous convainc moyennement, écrivons les détails.
Soient donc $k, \ell \in [\![1,m]\!]$ tels que $g(k) = g(\ell)$ Distinguons trois cas :

- si $f(k) < f(m+1)$ et $f(\ell) < f(m+1)$, alors $g(k) = f(k)$ et $g(\ell) = f(\ell)$.
  On a donc $f(k) = f(\ell)$, et par injectivité de f, alors $k = \ell$.
- Si $f(k) < f(m+1)$ et $f(\ell) > f(m+1)$, alors $g(k) = f(k) < f(m+1)$ et $g(k) = f(k) - 1 > f(m+1) - 1 \geqslant f(m+1)$.
  Comme nous avons supposé $g(k) = g(\ell)$, ce cas est impossible.
  De la même manière, on ne peut avoir $f(\ell) < f(m+1)$ et $f(k) > f(m+1)$.
- Si $f(k)$ et $f(\ell)$ sont tous les deux supérieurs[16] à $f(m+1)$, alors $g(k) = f(k) - 1$ et $g(\ell) = f(\ell) - 1$.
  Ces deux quantités étant égales par hypothèse, $f(k) = f(\ell)$ et donc par injectivité de f, nécessairement $\ell = k$.

[16] Strictement puisqu'ils ne peuvent être égaux à $f(m+1)$.

Conclusion : dans tous les cas, $g(k) = g(\ell)$ implique $k = \ell$, g est injective.
Au final, nous avons donc prouvé qu'il existe une injection de $[\![1,m]\!]$ dans $[\![1,n-1]\!]$.
Donc par hypothèse de récurrence, $m \leqslant n-1$ et donc $m+1 \leqslant n$. Ainsi, $\mathscr{P}(m+1)$ est vraie.
Par le principe de récurrence $\mathscr{P}(m)$ est vraie pour tout $m \in \mathbf{N}^*$. □

Heureux ?
Vous êtes vraiment plus convaincus par cette preuve que par le dessin ? Pas moi !

Proposition 10.44 : *Soient $(m,n) \in (\mathbf{N}^*)^2$. Alors il existe une bijection de $[\![1,m]\!]$ sur $[\![1,n]\!]$ si et seulement si $m = n$.*

Démonstration. Si $m = n$, il est évident que $\mathrm{id}_{[\![1,n]\!]}$ convient.
Inversement, si $f : [\![1,m]\!] \to [\![1,n]\!]$ est bijective, alors f est injective, donc $m \leqslant n$.
Mais $f^{-1} : [\![1,n]\!] \to [\![1,m]\!]$ est injective également, et donc $n \leqslant m$. □

Corollaire 10.45 – *Si E est un ensemble fini non vide, il existe un unique $n \in \mathbf{N}^*$ tel que E soit en bijection avec $[\![1,n]\!]$.*
Cet entier n est appelé le cardinal de E, et on le note $\mathrm{Card}(E)$ ou $\#E$.
Par convention, le cardinal de l'ensemble vide est nul.

Démonstration. Supposons qu'il existe deux entiers non nuls m et n et deux bijections $\varphi : [\![1,n]\!] \to E$ et $\psi : [\![1,m]\!] \to E$.
Alors $\psi^{-1} \circ \varphi : [\![1,n]\!] \to [\![1,m]\!]$ est une bijection, et donc $m = n$. □

⚠ Si n est unique, la bijection n'est l'est pas[17]
Si $\varphi : [\![1,n]\!] \to [\![1,n]\!]$ et $\psi : [\![1,n]\!] \to [\![1,n]\!]$ sont deux bijections, alors $\varphi \circ \psi$ est une bijection de $[\![1,n]\!]$ sur E.
Composer par une telle bijection revient à changer le «numéro» qu'on attribue à chaque élément de E.

[17] Sauf si $n = 1$.

Proposition 10.46 : *Soient $(a,b) \in \mathbf{Z}^2$ avec $a < b$. Alors $[\![a,b]\!]$ est de cardinal $b - a + 1$.*

Démonstration. Soit $\varphi : \left| \begin{array}{ccc} [\![1, b-a+1]\!] & \longrightarrow & [\![a,b]\!] \\ k & \longmapsto & k + a - 1 \end{array} \right.$.
Alors φ est injective car strictement croissante et surjective car si $\ell \in [\![a,b]\!]$, alors

$$\ell = \underbrace{\ell - a + 1}_{\in [\![1, b-a+1]\!]} + a - 1 = \varphi(\ell - a + 1).$$

Donc φ est bijective. □

Nous nous contentons pour l'instant de cette définition du cardinal, et continuons à nous en tenir à l'intuition pour la plupart des propriétés usuelles du cardinal (par exemple, une partie A d'un ensemble fini E est elle-même finie, et $\mathrm{Card}(A) \leqslant \mathrm{Card}(E)$), mais nous reviendrons sur cette notion plus tard dans l'année.

10.3.2 Équipotence (Hors programme)

Définition 10.47 – Deux ensembles E et F sont dits équipotents[18] s'il existe une bijection $E \to F$.

[18] Le terme est un peu tombé en désuétude, on dire plutôt que E et F sont en bijection.

L'idée est que deux ensembles qui sont en bijection sont sensiblement de la même taille, puisqu'à tout élément de l'un correspond un unique élément de l'autre.

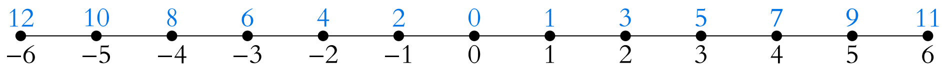
Contrairement à ce que l'on pourrait penser, les ensembles ne se résument pas aux ensembles finis vs. les ensembles infinis : deux ensembles infinis ne sont pas forcément équipotents.

Exemples 10.48

- $\mathbf{N}$ et $\mathbf{N}^*$ sont équipotents[19]
En effet, l'application $\varphi : \left| \begin{array}{ccc} \mathbf{N} & \longrightarrow & \mathbf{N}^* \\ n & \longmapsto & n+1 \end{array} \right.$ est une bijection.

[19] Et donc ont «autant d'éléments».

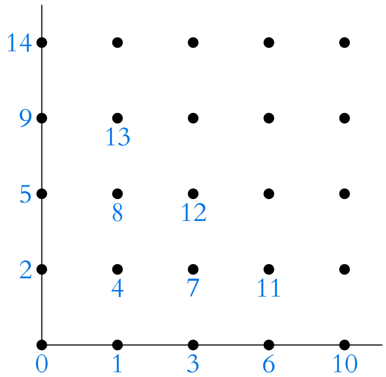
▸ $\mathbf{N}$ et $\mathbf{Z}$ sont équipotents. En effet, $\varphi : \mathbf{N} \to \mathbf{Z}$, $\quad n \mapsto \begin{cases} \left\lfloor \frac{n}{2} \right\rfloor + 1 & \text{si } n \text{ est impair} \\ -\frac{n}{2} & \text{si } n \text{ est pair} \end{cases}$. est une bijection.



▸ Plus surprenant, $\mathbf{N}^2$ et $\mathbf{N}$ sont équipotents. En effet,

$$\begin{aligned} \varphi : \mathbf{N} \times \mathbf{N} &\to \mathbf{N} \\ (p, q) &\mapsto \frac{(p+q+1)(p+q)}{2} + p \end{aligned}$$

est une bijection de $\mathbf{N} \times \mathbf{N}$ dans $\mathbf{N}$ (difficile), donc $\varphi^{-1} : \mathbf{N} \to \mathbf{N} \times \mathbf{N}$ est une bijection.



Proposition 10.49 (Théorème de Cantor) : *Soit E un ensemble, alors il n'existe pas de surjection de E sur $\mathscr{P}(E)$.*

Démonstration. Raisonnons par l'absurde et supposons qu'il existe un ensemble E et une surjection $f : E \to \mathscr{P}(E)$.
Soit alors $A = \{x \in E,\ x \notin f(x)\}$.
Alors A ne peut pas posséder d'antécédent par f. En effet, s'il existe $x \in E$ tel que $f(x) = A$, alors :

- soit $x \in A$, et donc $x \in f(x)$, donc $x \notin A$: absurde.
- soit $x \notin A$, et donc $x \notin f(x)$, donc $x \in A$: absurde.

□

Corollaire 10.50 – *Pour tout ensemble E, E et $\mathscr{P}(E)$ ne sont pas équipotents.*

Démonstration. Puisqu'il n'existe pas de surjection de E sur $\mathscr{P}(E)$, il n'existe pas non plus de bijection. □

Ceci permet donc de construire des ensembles de plus en plus «grands» : $\mathbf{N}$, $\mathscr{P}(\mathbf{N})$, $\mathscr{P}(\mathscr{P}(\mathbf{N}))$, etc, chacun étant «strictement plus grand» que le précédent.

10.4 Relations binaires

En maths, on a régulièrement envie de comparer plusieurs éléments, soit pour dire qu'ils partagent certaines propriétés, soit au contraire pour dire qu'ils diffèrent sur certains points et que tel élément est plus *trucmuche* que tel autre.
Par exemple que tel ensemble est plus petit que (= inclus dans) tel autre, qu'une suite tend plus rapidement vers 0 qu'une autre, que deux droites sont parallèles (= ont même direction), que deux fonctions ont même limite en $+\infty$, etc.

10.4.1 Définitions

Définition 10.51 (Relation binaire) – Soit E un ensemble non vide. On appelle **relation binaire** sur E toute partie $\mathscr{R}$ de $E \times E$.
On note alors $x \mathscr{R} y$ pour signifier que $(x, y) \in \mathscr{R}$.

Exemples 10.52

► L'ensemble $\mathscr{R} = \{(x, x), x \in E\}$ est une relation binaire sur tout ensemble E.
On a alors $x \mathscr{R} y \Leftrightarrow x = y$.
► La relation $\mathscr{R}$ définie sur $\mathbf{Z}$ par $p \mathscr{R} q$ si et seulement si p divise q est une relation binaire sur $\mathbf{Z}$.
► La relation $\mathscr{R}$ définie sur $\mathbf{R}$ par $x \mathscr{R} y \Leftrightarrow x^2 + y = 1$ est une relation binaire.

Définition 10.53 – Soit $\mathscr{R}$ une relation binaire sur E. On dit que $\mathscr{R}$ est :

- **réflexive** si $\forall x \in E, x \mathscr{R} x$
- **symétrique** si $\forall (x, y) \in E^2, x \mathscr{R} y \Rightarrow y \mathscr{R} x$
- **transitive** si $\forall (x, y, z) \in E^3, x \mathscr{R} y$ et $y \mathscr{R} z \Rightarrow x \mathscr{R} z$
- **antisymétrique** si $\forall (x, y) \in E^2, x \mathscr{R} y$ et $y \mathscr{R} x \Rightarrow x = y$.

Exemples 10.54

► La relation de divisibilité sur $\mathbf{Z}$ est réflexive (tout entier se divise), elle est transitive (si a divise b et b divise c, alors a divise c). Elle n'est pas réflexive puisque 2 divise 4 mais 4 ne divise pas deux.
► La relation «être frontalier de», définie sur l'ensemble des pays est une relation symétrique, mais elle n'est pas transitive.[20]

[20] Par exemple parce que la Norvège est frontalière de la Russie, que la Russie est frontalière de la Corée du Nord, mais la Norvège n'est pas frontalière de la Corée du Nord.

10.4.2 Relations d'équivalence

Définition 10.55 – Une relation binaire $\mathscr{R}$ qui est à la fois réflexive, symétrique et transitive est appelée **relation d'équivalence**.

Exemples 10.56

► Si $f : E \to F$, alors la relation $x \mathscr{R} y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence sur E.
En effet, on a toujours $f(x) = f(x)$, donc $x \mathscr{R} x$.
Si $x \mathscr{R} y$, alors $f(y) = f(x)$, et donc $y \mathscr{R} x$.
Et si $x \mathscr{R} y$ et $y \mathscr{R} z$, alors $f(x) = f(y) = f(z)$, et donc en particulier, $f(x) = f(z)$, de sorte que $x \mathscr{R} z$.
► Si $\alpha \neq 0$, alors la relation $x \sim y \Leftrightarrow x \equiv y \ [\alpha]$ est une relation d'équivalence sur $\mathbf{R}$.
Rappelons que $x \equiv y \ [\alpha]$ si et seulement si $\exists k \in \mathbf{Z}$ tel que $y = x + k\alpha$
En effet, on a toujours $x \equiv x \ [\alpha]$.
Si $x \equiv y \ [\alpha]$, alors il existe $k \in \mathbf{Z}$ tel que $y = x + k\alpha \Leftrightarrow x = y + \underbrace{(-k)}_{\in \mathbf{Z}} \alpha$, et donc $y \equiv x \ [\alpha]$.
Enfin, si $x \equiv y \ [\alpha]$ et $y \equiv z \ [\alpha]$, alors il existe deux entiers k_1 et k_2 tels que $y = x + k_1\alpha$ et $z = y + k_2\alpha$, de sorte que $z = x + (k_1 + k_2)\alpha$ et donc $z \equiv x \ [\alpha]$.
► De même, la relation de congruence modulo n est une relation d'équivalence sur $\mathbf{Z}$.

Remarque
Nous utilisons ici le fait que, sur n'importe quel ensemble, l'égalité est elle-même une relation d'équivalence !

► Sur l'ensemble $\mathbf{R}^{\mathbf{N}}$ des suites à valeurs réelles, on définit une relation $\sim$ par $(u_n) \sim (v_n) \Leftrightarrow \lim\limits_{n\to+\infty} (u_n - v_n) = 0$.
Alors $(u_n) \sim (u_n)$ puisque la suite nulle tend vers 0.
Si $(u_n) \sim (v_n)$, alors $\lim\limits_{n\to+\infty} (u_n - v_n) = 0$ de sorte que $\lim\limits_{n\to+\infty} (v_n - u_n) = 0$. Donc $\sim$ est symétrique.
Enfin, si $(u_n) \sim (v_n)$ et $(v_n) \sim (w_n)$, alors on à la fois $u_n - v_n \underset{n\to+\infty}{\longrightarrow} 0$ et $v_n - w_n \underset{n\to+\infty}{\longrightarrow} 0$, donc par somme de limites $u_n - w_n \underset{n\to+\infty}{\longrightarrow} 0$, de sorte que $(u_n) \sim (w_n)$. Donc $\sim$ est transitive, et donc est une relation d'équivalence sur $\mathbf{R}^{\mathbf{N}}$.

Définition 10.57 – Si $\mathscr{R}$ est une relation d'équivalence sur E et si $x \in E$, on appelle classe d'équivalence de E et on note $\mathrm{cl}(x)$ ou $\overline{x}$ (ou encore $\dot{x}$) l'ensemble défini par $\mathrm{cl}(x) = \overline{x} = \{y \in E \mid x \mathscr{R} y\}$.

Exemples 10.58

► Pour la relation de congruence modulo 2 sur $\mathbf{Z}$, alors la classe d'équivalence de $n \in \mathbf{Z}$ est l'ensemble des entiers de même parité que n.
► Pour la relation d'équivalence $x\mathscr{R}y \Leftrightarrow |x| = |y|$, alors la classe d'équivalence de $x \neq 0$ est $\{x, -x\}$, et la classe d'équivalence de 0 est $\{0\}$.
► Pour la relation $\sim$ précédemment introduite sur $\mathbf{R}^{\mathbf{N}}$, on prouve facilement que si une suite (u_n) converge vers une limite finie ℓ, alors la classe d'équivalence de (u_n) est l'ensemble des suites de limite ℓ.
C'est en revanche plus compliqué pour les suites de limite infinie, puisque $u_n = n$ et $v_n = n^2$ tendent toutes deux vers $+\infty$, mais leur différence ne tend pas vers 0. Donc elles ne sont pas dans la même classe d'équivalence.
Et c'est sans compter sur toutes les classes d'équivalence de suites divergentes, par exemple qu'y a-t-il dans la classe d'équivalence de $((-1)^n)_n$?

Proposition 10.59 : *Soit $\mathscr{R}$ une relation d'équivalence sur E. Alors :*

1. *Pour tout $x \in E$, $\overline{x} \neq \emptyset$.*
2. *Pour $(x, y) \in E^2$, on a soit $\overline{x} = \overline{y}$, soit $\overline{x} \cap \overline{y} = \emptyset$*
3. $\displaystyle\bigcup_{x\in E} \overline{x} = E$.

Autrement dit, les classes d'équivalence forment une partition de E.

En français

Deux classes d'équivalence sont soit égales, soit disjointes.

Rappel

On appelle partition de E toute famille de parties de E formée d'ensembles non vide, deux à deux disjoints, et dont l'union vaut E tout entier.

Démonstration. 1. On a toujours $x \in \overline{x}$ car $x \mathscr{R} x$, donc $\overline{x} \neq \emptyset$.

2. Soient $x, y \in E$ tels que $\overline{x} \cap \overline{y} \neq \emptyset$, et montrons que $\overline{x} = \overline{y}$.
Soit $z \in \overline{x} \cap \overline{y}$. Alors $x \mathscr{R} z$ et $y \mathscr{R} z$.
Par symétrie, on a donc $z \mathscr{R} y$ et par transitivité, $x \mathscr{R} y$.
En particulier, si $u \in \overline{x}$, alors $x \mathscr{R} u$ et donc $u \mathscr{R} x$. Puisque de plus $x \mathscr{R} y$, par transitivité, $u \mathscr{R} y$ et donc $y \mathscr{R} u$, de sorte que $u \in \overline{y}$.
Ainsi, nous venons de prouver que $\overline{x} \subset \overline{y}$.
On prouve de la même manière l'inclusion réciproque $\overline{y} \subset \overline{x}$ et donc $\overline{x} = \overline{y}$.

3. Puisque les classes d'équivalence sont incluses dans E par définition, on a $\displaystyle\bigcup_{x\in E} \overline{x} \subset E$.
Inversement, si $y \in E$, alors $y \in \overline{y}$ et donc $y \in \displaystyle\bigcup_{x\in E} \overline{x}$.
Et donc par double inclusion, on a bien $E = \displaystyle\bigcup_{x\in E} \overline{x}$.

□

Exemple 10.60

Pour la relation de congruence modulo 2, il y a deux classes d'équivalence, qui sont $\bar{0}$, l'ensemble des entiers pairs, et $\bar{1}$, l'ensemble des entiers impairs.
Ces deux ensembles sont disjoints, non vides, et leur union est bien $\mathbf{Z}$ tout entier.

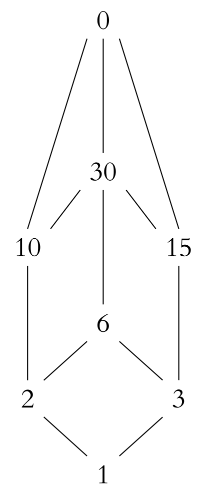
10.4.3 Relations d'ordre

Définition 10.61 – Une relation binaire $\preccurlyeq$ qui est à la fois réflexive, transitive et antisymétrique est appelée **relation d'ordre**.
On dit alors que $(E, \preccurlyeq)$ est un **ensemble ordonné.**

Exemples 10.62

▸ Sur $\mathbf{N}$ la relation de divisibilité : $a \mid b \Leftrightarrow \exists k \in \mathbf{N}, b = ka$ est une relation d'ordre.
En effet, on a toujours $a = 1a$, de sorte que $a \mid a$.
Si $a \mid b$ et $b \mid a$, alors il existe deux entiers k_1 et k_2 tels que $a = k_1 b$ et $b = k_2 a$, donc $a = k_1 k_2 a$. Ce qui implique que $k_1 k_2 = 1$, et donc $k_1 = k_2 = 1$, donc $a = b$. Donc la relation est antisymétrique.
Enfin, si $a \mid b$ et $b \mid c$, il existe deux entiers k_1 et k_2 tels que $b = k_1 a$ et $c = k_2 b$, de sorte que $c = (k_1 k_2) a$, et donc $a \mid c$: la relation est transitive.
En revanche, la relation de divisibilité sur $\mathbf{Z}$: $a \mid b \Leftrightarrow \exists k \in \mathbf{Z}, b = ka$ n'est pas une relation d'ordre car elle n'est pas antisymétrique : on a $1 \mid -1$ et $-1 \mid 1$ alors que $1 \neq -1$.
▸ Si E est un ensemble, la relation d'inclusion $A \subset B$ est une relation d'ordre sur $\mathscr{P}(E)$.
En effet, on a toujours $A \subset A$. Si $A \subset B$ et $B \subset A$, alors $A = B$.
Et enfin, si $A \subset B$ et $B \subset C$, alors $A \subset C$.
▸ Si E est un ensemble et si $(F, \preccurlyeq)$ est un ensemble ordonné, alors on définit une relation d'ordre (encore notée $\preccurlyeq$) sur $\mathscr{F}(E, F)$ par

$$f \preccurlyeq g \Leftrightarrow \forall x \in E,\ f(x) \preccurlyeq g(x).$$



Un moyen de représenter les relations de divisibilité sur quelques entiers.
Un trait indique que deux éléments sont comparables, celui du bas divisant celui du haut.

Si $\preccurlyeq$ est une relation d'ordre sur E, on note souvent $x \prec y$ pour signifier que $x \preccurlyeq y$ **et** $x \neq y$.
Cette relation binaire est encore transitive, mais ce n'est plus une relation d'ordre, notamment du fait qu'elle n'est pas réflexive : on n'a jamais $x \prec x$.

Exemple 10.63 **Ordre lexicographique**

Si $(E, \preccurlyeq)$ est un ensemble ordonné, alors on définit une relation d'ordre sur E^2 par

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 \prec x_2 \textbf{ ou } \begin{cases} x_1 = x_2 \\ y_1 \preccurlyeq y_2 \end{cases}$$

Alors $\preceq$ est une relation d'ordre sur E^2, qu'on appelle ordre lexicographique. En effet :

- Pour tout $(x, y) \in E^2$, on a toujours $(x, y) \preceq (x, y)$.
- Si $(x_1, y_1) \preceq (x_2, y_2)$ et $(x_2, y_2) \preceq (x_3, y_3)$.
  Alors soit $x_1 \prec x_2$, et puisque $x_2 \preccurlyeq x_3$, nécessairement, $x_1 \prec x_3$, de sorte que $(x_1, y_1) \preceq (x_3, y_3)$.
  Soit $x_1 = x_2$, et alors $y_1 \preccurlyeq y_2$. Mais alors deux nouveaux cas se présentent :
  — soit $x_2 \prec x_3$, et alors $x_1 \prec x_3$, de sorte que $(x_1, y_1) \preceq (x_3, y_3)$.
  — soit $x_2 = x_3$ et $y_2 \preccurlyeq y_3$, de sorte que $x_1 = x_2 = x_3$ et $y_1 \preccurlyeq y_2 \preccurlyeq y_3$, et donc $(x_1, y_1) \preceq (x_3, y_3)$.
  Dans tous les cas $\preceq$ est transitive.
- Enfin, si $(x_1, y_1) \preceq (x_2, y_2)$ et $(x_2, y_2) \preceq (x_1, y_1)$, Alors, puisque $(x_1, y_1) \preceq (x_2, y_2)$, soit $x_1 \prec x_2$, soit $x_1 = x_2$ et $y_1 \preccurlyeq y_2$.

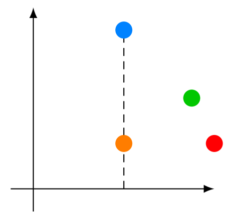


FIGURE 10.5– Pour l'ordre lexicographique sur $\mathbf{R}^2$, on a

● $\preceq$ ● $\preceq$ ● $\preceq$ ●

Mais $x_1 < x_2$ n'est pas possible puisque $(x_2, y_2) \preceq (x_1, y_1)$.
Donc $x_1 = x_2$. Et alors on a à la fois $y_1 \leqslant y_2$ et $y_2 \leqslant y_1$, donc par antisymétrie de $\leqslant$, $y_1 = y_2$, et donc $(x_1, y_1) = (x_2, y_2)$.
Donc $\preceq$ est antisymétrique, et donc est une relation d'ordre.

Remarque
Cette relation se généralise sans grande difficulté à E^n. Remarquons que c'est exactement l'ordre qu'on utilise dans un dictionnaire (d'où le nom) : on compare les premières lettres, si elles sont égales on compare les deuxièmes, etc.

Notons que sur le même principe, il est possible de définir une relation d'ordre sur $\mathbf{C}$, en comparant d'abord les parties réelles, puis les parties imaginaires. Malheureusement, cette relation se comporte très mal vis-à-vis des opérations, et n'est d'aucun intérêt pour faire des calculs, raison pour laquelle on ne l'utilise jamais.

Définition 10.64 – Une relation d'ordre $\preccurlyeq$ sur un ensemble E est dite **totale** si pour tout $(x, y) \in E^2$, $x \preccurlyeq y$ ou $y \preccurlyeq x$. On parle alors d'ensemble totalement ordonné.
On parle alors d'ordre total. Dans le cas contraire, on dit que $\preccurlyeq$ est un **ordre partiel**, et que $(E, \preccurlyeq)$ est partiellement ordonné.

Exemples 10.65

► La relation d'ordre lexicographique $\preceq$ sur $\mathbf{R}^2$ est un ordre total. En effet,soient (x_1, y_1) et (x_2, y_2) deux éléments de $\mathbf{R}^2$.
Alors soit $x_1 < x_2$, auquel cas $(x_1, y_1) \preceq (x_2, y_2)$, soit $x_2 < x_1$ auquel cas $(x_2, y_2) \preceq (x_1, y_1)$, soit $x_1 = x_2$.
Mais dans ce cas, on aura soit $y_1 \leqslant y_2$ et donc $(x_1, y_1) \preceq (x_2, y_2)$, soit $y_2 < y_1$ auquel cas $(x_2, y_2) \preceq (x_1, y_1)$.
► Sur $\mathscr{P}(E)$, la relation d'inclusion est un ordre partiel dès que E possède au moins deux éléments, car si x et y sont deux éléments distincts de E, on n'a ni $\{x\} \subset \{y\}$, ni $\{y\} \subset \{x\}$.
► La relation de divisibilité sur $\mathbf{N}$ est un ordre partiel car on n'a ni $2|3$, ni $3|2$.
► Même si $(F, \preccurlyeq)$ est totalement ordonné, l'ordre $\preccurlyeq$ défini précédemment sur $\mathscr{F}(E, F)$ n'est pas total dès que E contient plus de deux éléments.
Par exemple, $\mathscr{F}([0, 1], \mathbf{R})$ n'est pas totalement ordonné : deux fonctions f et g dont les graphes se croisent ne sont pas comparables, au sens où on n'a ni $f \leqslant g$, ni $g \leqslant f$.

Plus généralement
Si E est muni d'une relation d'ordre total, l'ordre lexicographique sur E^n est aussi total.

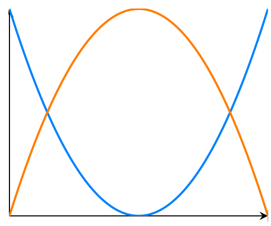


FIGURE 10.6– Deux fonctions non comparables de $[0, 1]$ dans $\mathbf{R}$. Aucune des deux n'est toujours plus grande (=au dessus) de l'autre.

Définition 10.66 – Soit $(E, \preccurlyeq)$ un ensemble ordonné, soit $A \subset E$ et soit $a \in A$.

1. On dit que a est le plus grand élément de A (ou le maximum de A) si $\forall x \in A$, $x \preccurlyeq a$. On note alors $a = \max(A)$.
2. On dit que a est le plus petit élément de A (ou le minimum de A) si $\forall x \in A$, $a \preccurlyeq x$. On note alors $a = \min(A)$.

Remarques. ► Un plus grand élément, s'il en existe un, est nécessairement unique. En effet, supposons que a et b soient tous deux le plus grand élément de A.
Alors on a $a \preccurlyeq b$ (car b est le maximum de A) et $b \preccurlyeq a$ (car a est le maximum de A).
Par antisymétrie, cela implique que $a = b$.
► Toute partie d'un ensemble ordonné n'a pas forcément de plus grand (resp. plus petit) élément. Par exemple, pour l'ordre usuel sur $\mathbf{R}$, $]0, 1[$ n'a ni plus grand ni plus petit élément, de même que $\mathbf{R}$ tout entier.
► Si $a_1, \dots, a_n$ sont des réels, alors on note $\max(a_1, \dots, a_n)$ au lieu de $\max\{a_1, \dots, a_n\}$ le plus grand élément de $\{a_1, \dots, a_n\}$.

Remarque
Ceci justifie bien qu'on dise **le** plus grand élément et pas **un** plus grand élément.

Exemple 10.67

L'ensemble ordonné $(\mathscr{P}(E), \subset)$ possède un plus grand élément, qui est E.
En effet, pour tout $A \in \mathscr{P}(E)$, on a $A \subset E$.

De même, il possède $\emptyset$ comme plus petit élément puisque pour tout $A \in \mathcal{P}(E)$, $\emptyset \subset A$.

Définition 10.68 – Soit $(E, \preccurlyeq)$ un ensemble ordonné, soit A une partie de E et soit $a \in E$. On dit que a est :

- un **majorant** de A si $\forall x \in A,\ x \preccurlyeq a$
- un **minorant** de A si $\forall x \in A,\ a \preccurlyeq x$.

Si A possède (au moins) un majorant, on dit qu'elle est majorée, et si elle possède au moins un minorant, on dit qu'elle est minorée.

Remarque

À la différence d'un plus grand (resp. petit) élément, un majorant (resp. minorant) n'a pas besoin de faire partie de A.
D'ailleurs, si $a \in A$ est un majorant de A si et seulement si c'est le plus grand élément de A.

⚠ Contrairement au plus petit élément, un majorant n'est pas nécessairement unique.

Exemples 10.69

► Pour l'ordre usuel sur $\mathbf{R}$, 1 est un majorant de $]0, 1[$. Tout réel supérieur ou égal à 1, est également un majorant de $]0, 1[$.
► Pour la relation de divisibilité sur $\mathbf{N}$, tout multiple de 6 est un majorant de $\{2, 3\}$.

Définition 10.70 – Soit $(E, \preccurlyeq)$ un ensemble ordonné, soit $A \in \mathcal{P}(E)$, et soit $a \in E$. On dit que a est :

- la **borne supérieure de** A si a est le plus petit des majorants de A. On note alors $a = \sup(A)$.
- la **borne inférieure de** A si a est le plus grand des minorants de A. On note alors $a = \inf(A)$.

Remarques. ► Pour le dire avec des quantificateurs : a est la borne supérieure de A si

$$a = \min\{x \in E \mid x \text{ majorant de } A\} = \min\{x \in E \mid \forall y \in A,\ y \preccurlyeq x\}.$$

Ou encore

$$x = \sup(A) \Leftrightarrow (\forall x \in E,\ (\forall y \in A \Rightarrow y \preccurlyeq x) \Rightarrow x \preccurlyeq a).$$

► La terminologie le laisse penser, mais une telle borne supérieure, **si elle existe** est unique, car c'est le plus petit élément de l'ensemble des majorants, et qu'un tel plus petit élément est unique. Idem pour la borne inférieure.
► Une borne supérieure (resp. inférieure) ne peut exister que pour un ensemble majoré (resp. minoré) faut de quoi l'ensemble des majorants (resp. minorants) est vide, et donc ne contient pas de plus grand (resp. petit) élément.

Exemple 10.71

► Dans $(\mathbf{N}, |)$, $\sup\{2, 3\} = 6$. En effet, nous avons déjà vu que les majorants de $\{2, 3\}$ sont les multiples de 6. Et donc si a est un majorant de $\{2, 3\}$, alors $6|a$.
► Une partie peut-être majorée sans avoir de borne supérieure.
Par exemple dans l'ensemble ordonné $(\mathbf{R} \setminus \{1\})$, $A = [0, 1[$ est majoré (par 2 par exemple), mais ne possède pas de borne supérieure.
En effet, l'ensemble des majorants de A est $]1, +\infty[$, qui ne possède pas de plus petit élément.
Vous allez me dire que je l'ai un peu fait exprès, la borne supérieure de $[0, 1[$ devant être égale à 1. En effet, mais nous verrons bientôt que des exemples moins triviaux existent, par exemple dans $\mathbf{Q}$, $\{x \in \mathbf{Q} \mid x^2 \preccurlyeq 2\}$ est majoré mais n'admet pas de borne supérieure.

Théorème 10.72 : *Si A possède un plus grand (resp. petit) élément, alors A possède une borne supérieure (resp. inférieure) et* $\sup A = \max A$ *(resp.* $\inf A = \min A$*).*

Démonstration. Par définition, $\max A$ est un majorant de A. Il s'agit donc de prouver que $\max A$ est le plus petit des majorants de A.
Soit donc M un majorant de A. Puisque $\max A \in A$, on a donc $\max A \leqslant M$.
Et donc $\max A$ est bien le plus petit des majorants de A : A possède une borne supérieure, qui est donc égale à $\max A$. □

Nous n'avons pas donné, et ne donnerons pas de définition précise de ce qu'est **N**. Cela dit, nous en avons une excellente intuition, qui nous suffira largement, mais nous oblige à **admettre** la propriété suivante :

Proposition 10.73 : *Toute partie non vide de* **N** *possède un plus petit*[21] *élément.*

[21] Au sens de la relation d'ordre usuelle.

Cette propriété est assez caractéristique de **N**, et n'est par exemple plus vraie pour une partie non vide de **Z**.

Elle nous permet alors de justifier la validité du raisonnement par récurrence :

Proposition 10.74 (Principe de récurrence simple) : *Soit $\mathscr{P}(n)$ une proposition logique dépendant d'un entier $n \in \mathbf{N}$.*
Supposons que :

- *il existe $n_0 \in \mathbf{N}$ tel que $\mathscr{P}(n_0)$ soit vraie*
- $\forall n \geqslant n_0,\ \mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$

Alors $\mathscr{P}(n)$ est vraie pour tout $n \geqslant n_0$.

Pour la culture

Il n'est en fait pas très dur de prouver que si le principe de récurrence est valable, alors toute partie non vide de **N** possède un plus petit élément.
Et donc dans les axiomes qui définissent **N**, on peut mettre soit un axiome garantissant l'existence d'un plus petit élément, soit le principe de récurrence. Généralement, c'est ce dernier choix qui est fait : le principe de récurrence ne peut alors pas être prouvé : c'est un axiome de construction de **N**.

Démonstration. Notons $A = \{n \in \mathbf{N} \mid n \geqslant n_0 \textbf{ et } (\textbf{non}\, \mathscr{P}(n))\}$.
Nous souhaitons donc prouver que A est vide, c'est-à-dire que $\mathscr{P}(n)$ est vraie pour tout $n \geqslant n_0$.
Raisonnons par l'absurde et supposons que $A \neq \emptyset$.
Alors A possède un plus petit élément n_1, qui est donc nécessairement supérieur ou égal à n_0, et même supérieur strict à n_0 puisque $\mathscr{P}(n_0)$ est vraie par hypothèse.
La proposition $\mathscr{P}(n_1 - 1)$ ne peut alors pas être vraie, puisque $\mathscr{P}(n_1 - 1) \Rightarrow \mathscr{P}(n_1)$.
Donc $n_1 - 1 \in A$, contredisant le fait que n_1 est le plus petit élément de A.
On en déduit que $A = \emptyset$ et donc pour tout $n \geqslant n_0$, $\mathscr{P}(n)$ est vraie. □

Rappelons que nous avons alors prouvé dans le chapitre 3 que les principes de récurrence double et récurrence forte découlent directement du principe de récurrence simple.

Proposition 10.75 : *Toute partie non vide et majorée de* **N** *possède un plus grand élément.*

Démonstration. Soit A une partie non vide et majorée de **N**. Si $A = \{0\}$, il n'y a rien à dire.
Supposons donc que A contient des éléments non nuls.
Soit alors $B = \{n \in \mathbf{N},\ \forall a \in A,\ a \leqslant n\}$ l'ensemble des majorants entiers de A.
Alors B est non vide par hypothèse, et donc possède un plus petit élément b. Ce minimum est alors non nul, faut de quoi on aurait : $\forall n \in A,\ n \leqslant 0$, et donc $n = 0$: A serait réduit à $\{0\}$.
Montrons alors que $b \in A$, ce qui prouvera le résultat, car alors b sera un majorant de A, dans A.
Puisque $b - 1 \notin B$, et donc $b - 1$ n'est pas un majorant de A : il existe $a \in A$ tel que $a > b - 1 \Leftrightarrow a \geqslant b$.
Mais un tel a vérifie $a \leqslant b$. Donc $a = b$, et donc $b \in A$.
Ainsi, A possède un majorant qui est dans A, c'est le plus grand élément de A. □