Chapitre 2

Applications et relations binaires

2.1 Introduction historique

> *[...] la faculté de l'esprit de rapporter des choses à des choses, de faire correspondre une chose à une chose, ou de représenter une chose par une chose, faculté sans laquelle aucune pensée n'est possible.*
>
> Richard Dedekind - *Was sind und was sollen die Zahlen ?*, Vieweg, 1888, préface

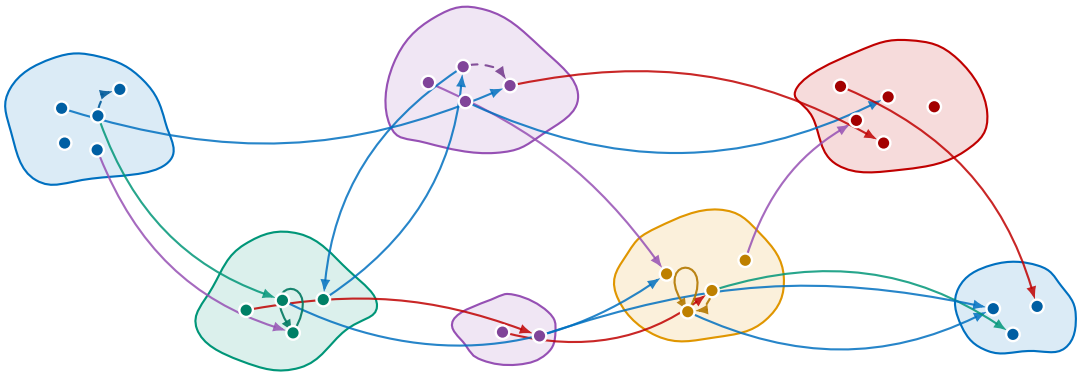
Le chapitre 1 a fixé le langage des ensembles ; celui-ci introduit la manière de les mettre en relation. Une application fait correspondre à chaque élément d'un ensemble un élément d'un autre, une relation compare les éléments d'un même ensemble : c'est, comme le dit Dedekind, l'opération la plus élémentaire de la pensée mathématique.

2.1.1 De la formule à la correspondance

Pour **Leonhard Euler**, en 1748, une fonction est une *expression analytique*, une formule construite à partir d'une variable. En 1837, **Peter Gustav Lejeune Dirichlet** propose d'appeler fonction *toute* correspondance qui associe à chaque valeur de la variable une valeur déterminée, qu'une formule la décrive ou non. En 1888, **Richard Dedekind** fait de l'*Abbildung* (application) un objet de base, défini entre ensembles quelconques, et nomme *ähnlich* celles qui envoient deux éléments distincts sur deux images distinctes : ce sont nos injections. Les mots *injection*, *surjection* et *bijection* viennent du groupe **Bourbaki**, au milieu du XX^{e} siècle.

2.1.2 Comparer, classer, ordonner

En 1801, **Carl Friedrich Gauss** ouvre ses *Disquisitiones arithmeticae* par la congruence et la notation $a \equiv b$, exemple fondateur de relation d'équivalence. En 1891, **Georg Cantor** démontre par son argument diagonal qu'aucun ensemble n'est en bijection avec l'ensemble de ses parties (section 2.5). Enfin, **Felix Hausdorff** étudie en 1914 les ensembles ordonnés où deux éléments ne sont pas toujours comparables, comme les parties d'un ensemble pour l'inclusion.



2.2 Applications

2.2.1 Définition et graphe

Définition : Soit E et F deux ensembles. Une **application** de E dans F est un triplet $f = (E, F, \Gamma)$, où Γ est une partie de $E \times F$ vérifiant

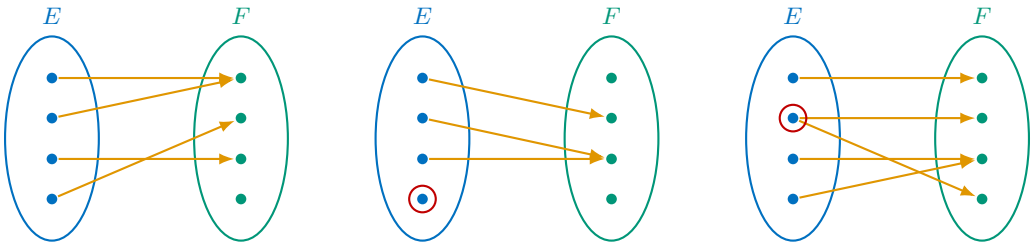
$$(*) \qquad \forall x \in E,\ \exists! y \in F,\ (x, y) \in \Gamma.$$

L'ensemble E est l'**ensemble de départ** de f, l'ensemble F son **ensemble d'arrivée**, et la partie Γ, notée aussi Γ_f, son **graphe**. Pour $x \in E$, l'unique élément y de F tel que $(x, y) \in \Gamma$ est noté $f(x)$ et appelé l'**image** de x par f ; on dit que x est *un* **antécédent** de y. On écrit

$$f : \left| \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right. \qquad \text{et l'on a} \qquad \Gamma_f = \{(x, f(x)) \mid x \in E\}.$$

L'ensemble des applications de E dans F est noté $\mathcal{F}(E, F)$ ou F^E.

Cette définition donne un sens précis à l'idée que f « associe » à tout élément x de E l'élément $f(x)$ de F : la règle d'association n'est rien d'autre que le graphe lui-même. Aucune formule n'est exigée, ce qui est exactement la conception de Dirichlet évoquée dans l'introduction. La condition $(*)$ contient deux exigences, l'*existence* et l'*unicité* de l'image, et chacune peut être mise en défaut, comme le montre la figure suivante, où chaque flèche représente un couple de Γ.



(a) (b) (c)

Seul le diagramme (a) représente une application : de chaque point de E part exactement une flèche, ce qui est la condition $(*)$. Dans le diagramme (b), un élément de E, entouré, n'a pas d'image : l'existence est en défaut. Dans le diagramme (c), un élément en a deux : c'est l'unicité. En revanche, rien n'est exigé à l'arrivée : dans le diagramme (a), un point de F reçoit deux flèches et un autre n'en reçoit aucune.

Deux triplets sont égaux lorsque leurs composantes le sont. La définition entraîne donc la caractérisation suivante de l'égalité de deux applications, qu'une présentation intuitive devrait poser comme une convention.

Égalité de deux applications : Deux applications $f = (E, F, \Gamma_f)$ et $g = (E', F', \Gamma_g)$ sont égales si et seulement si $E = E'$, $F = F'$ et $f(x) = g(x)$ pour tout $x \in E$.

∘ Démonstration : Par définition, $f = g$ signifie $E = E'$, $F = F'$ et $\Gamma_f = \Gamma_g$. Il suffit donc de montrer que, lorsque $E = E'$ et $F = F'$, l'égalité des graphes équivaut à l'égalité des images.

Images égales ⇒ graphes égaux. Si $f(x) = g(x)$ pour tout $x \in E$, alors

$$\Gamma_f = \{(x, f(x)) \mid x \in E\} = \{(x, g(x)) \mid x \in E\} = \Gamma_g.$$

Graphes égaux ⇒ images égales. Supposons $\Gamma_f = \Gamma_g$ et soit $x \in E$. Le couple $(x, f(x))$ appartient à Γ_f, donc à Γ_g ; par l'unicité dans $(*)$ appliquée à g, on obtient $f(x) = g(x)$. □

Exemples :

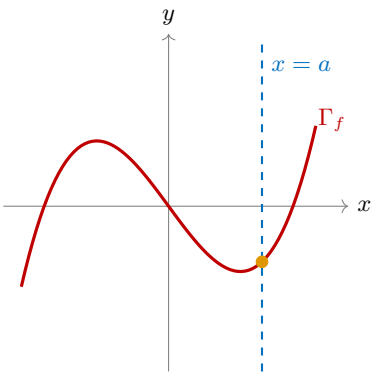
- Pour tout ensemble E, l'**identité** de E est l'application $\mathrm{id}_E : x \mapsto x$ de E dans E ; son graphe est la *diagonale* $\{(x, x) \mid x \in E\}$ de $E \times E$. Pour $c \in F$, l'application $x \mapsto c$ de E dans F, de graphe $E \times \{c\}$, est dite **constante**. L'application $\mathbb{R} \to \mathbb{R}$, $x \mapsto \lfloor x \rfloor$, qui à un réel associe l'unique entier k tel que $k \leqslant x < k + 1$, vérifie la condition $(*)$ grâce à la partition de $\mathbb{R}$ par les intervalles $[k, k+1[$ vue au chapitre 1 : l'existence de k vient de ce que ces intervalles recouvrent $\mathbb{R}$, son unicité de ce qu'ils sont disjoints.
- La partie $\Gamma = \{(x, y) \in \mathbb{R}_+ \times \mathbb{R} \mid y^2 = x\}$, qui est une parabole couchée, n'est pas le graphe d'une application de $\mathbb{R}_+$ dans $\mathbb{R}$: pour $x = 4$, les couples $(4, 2)$ et $(4, -2)$ appartiennent tous deux à Γ, et l'unicité est en défaut, comme dans le diagramme (c). La partie

$\{(x,y) \in \mathbb{R}_+ \times \mathbb{R}_+ \mid y^2 = x\}$, obtenue en ne gardant que la moitié supérieure, vérifie au contraire $(*)$: c'est le graphe de la racine carrée. De même, $\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x\}$ ne définit pas une application de $\mathbb{R}$ dans $\mathbb{R}$, car pour $x = -1$ aucun y ne convient : c'est l'existence qui fait défaut, comme dans le diagramme (b).

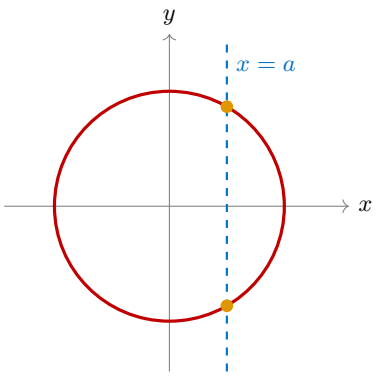
Remarques :

- L'ensemble d'arrivée fait partie des données, et cette exigence n'est pas une formalité. Les triplets $(\mathbb{R}, \mathbb{R}, \Gamma)$ et $(\mathbb{R}, \mathbb{R}_+, \Gamma)$, où $\Gamma = \{(x, x^2) \mid x \in \mathbb{R}\}$, ont le même graphe mais sont deux applications *différentes*. On verra à la section 2.5 que la seconde est surjective et la première non : la surjectivité est une propriété du triplet, et non de la « formule » x^2. L'ensemble de départ, lui, se retrouve à partir du graphe, comme ensemble des premières composantes des couples de Γ ; on le fait néanmoins figurer dans le triplet par symétrie et par commodité.
- Cette définition ramène la notion d'application à celles de couple et de partie d'un produit cartésien, et c'est la même idée qui servira à définir les relations binaires à la section 2.6. Elle ne fonde pas pour autant tout sur la seule notion d'ensemble, puisque les couples ont été introduits au chapitre 1 de façon intuitive, par la seule règle $(x,y) = (x',y') \Leftrightarrow (x = x' \text{ et } y = y')$. On peut aller jusqu'au bout en posant, avec Kuratowski (1921), $(x,y) = \big\{\{x\}, \{x,y\}\big\}$, ensemble dont on vérifie qu'il satisfait cette règle, puis $(a,b,c) = \big((a,b),c\big)$; cette construction, qui relève de la théorie des ensembles, est hors programme.
- Nous ne distinguerons pas les mots « fonction » et « application ». Certains ouvrages appellent *fonction* un triplet dont le graphe vérifie seulement l'unicité dans $(*)$, l'existence n'étant requise que sur une partie de E, appelée *domaine de définition* : c'est l'origine de l'habitude, prise au lycée, de chercher l'ensemble de définition d'une fonction donnée par une formule. Dans ce cours, une application est toujours définie en tout point de son ensemble de départ.

Lorsque E et F sont des parties de $\mathbb{R}$, le graphe de f est la courbe représentative de f dans le plan $\mathbb{R}^2$, et la condition $(*)$ a une traduction géométrique simple.



graphe d'une application



une partie qui n'est pas un graphe

Une partie du plan est le graphe d'une application définie sur une partie E de $\mathbb{R}$ si et seulement si chaque droite verticale d'abscisse $a \in E$ la rencontre en exactement un point. À gauche, la courbe d'équation $y = \frac{x^3-3x}{2,2}$ vérifie ce critère ; à droite, le cercle de rayon 1,6 centré à l'origine est coupé deux fois par la droite d'abscisse 0,8, en $y = \pm 1{,}6\frac{\sqrt{3}}{2} \approx \pm 1{,}39$.

2.2.2 Familles, suites et fonctions indicatrices

Définition : Soit I et E deux ensembles. Une **famille d'éléments de E indexée par I** est une application x de I dans E, que l'on note $(x_i)_{i \in I}$ en écrivant x_i au lieu de $x(i)$. Lorsque $I = \mathbb{N}$, on parle de **suite** d'éléments de E.

Remarque : Une famille n'est pas un ensemble. La famille $(1,1,2)$, indexée par $[\![1\,,3]\!]$, a trois termes, dont deux égaux, alors que l'ensemble $\{1,1,2\} = \{1,2\}$ n'a que deux éléments ; et la famille $(2,1)$ diffère de $(1,2)$, alors que $\{2,1\} = \{1,2\}$. Une famille retient l'ordre et les répétitions, comme un n-uplet du chapitre 1 : un n-uplet de E^n n'est rien d'autre qu'une famille indexée par $[\![1\,,n]\!]$. Les familles de parties $(A_i)_{i \in I}$ du chapitre 1 entrent aussi dans ce cadre.

Définition : Soit A une partie d'un ensemble E. La **fonction indicatrice** de A est l'application

$$\mathbf{1}_A : \left| \begin{array}{ccc} E & \longrightarrow & \{0,1\} \\ x & \longmapsto & \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} \end{array} \right.$$

Proposition 1 : Soit A et B deux parties d'un ensemble E. Alors :

(i) $A = B \iff \mathbf{1}_A = \mathbf{1}_B$;

(ii) $\mathbf{1}_{A\cap B} = \mathbf{1}_A\,\mathbf{1}_B$, $\quad \mathbf{1}_{\overline{A}} = 1 - \mathbf{1}_A$, $\quad \mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A\,\mathbf{1}_B$.

∘ Démonstration : **(i)** Si $A = B$, les deux fonctions ont les mêmes valeurs en tout point. Réciproquement, si $\mathbf{1}_A = \mathbf{1}_B$, alors pour tout $x \in E$:

$$x \in A \iff \mathbf{1}_A(x) = 1 \iff \mathbf{1}_B(x) = 1 \iff x \in B.$$

(ii) Soit $x \in E$. Le produit $\mathbf{1}_A(x)\,\mathbf{1}_B(x)$ vaut 1 si les deux facteurs valent 1, c'est-à-dire si $x \in A \cap B$, et 0 sinon. De même, $1 - \mathbf{1}_A(x)$ vaut 1 exactement lorsque $x \notin A$. Enfin, par une loi de De Morgan, $\overline{A \cup B} = \overline{A} \cap \overline{B}$, donc

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

□

Remarque : La propriété (i) transforme une égalité d'ensembles en une égalité de fonctions à valeurs dans $\{0,1\}$, sur lesquelles on peut *calculer*. Par exemple, la différence symétrique $A \,\Delta\, B$ a pour indicatrice $\mathbf{1}_A + \mathbf{1}_B - 2\,\mathbf{1}_A\,\mathbf{1}_B = (\mathbf{1}_A - \mathbf{1}_B)^2$; on peut ainsi démontrer l'associativité de Δ par un simple développement. Ces formules prépareront aussi le dénombrement d'une réunion au chapitre 21, où l'on sommera des indicatrices.

2.2.3 Restriction et prolongement

Définition : Soit $f : E \to F$ une application et A une partie de E. La **restriction** de f à A est l'application

$$f_{|A} : \left| \begin{array}{ccc} A & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$$

Si $E \subset E'$, on appelle **prolongement** de f à E' toute application $g : E' \to F$ telle que $g_{|E} = f$.

Exemple : La fonction $x \mapsto \frac{\sin x}{x}$, définie sur $\mathbb{R}^*$, admet une infinité de prolongements à $\mathbb{R}$, un pour chaque valeur choisie en 0. Le choix de la valeur 1 est privilégié, car $\frac{\sin x}{x}$ tend vers 1 lorsque x tend vers 0, comme on l'a vu en Terminale : c'est le seul prolongement continu, au sens du chapitre 8.

Remarque : On peut aussi modifier l'ensemble d'arrivée. Si $f(x)$ appartient à une partie F' de F pour tout $x \in E$, l'application $E \to F'$, $x \mapsto f(x)$, est une *autre* application que f, puisque l'ensemble d'arrivée fait partie des données ; on l'appelle l'application **induite** par f. On retrouve la situation de la fonction carré, vue de $\mathbb{R}$ dans $\mathbb{R}$ ou de $\mathbb{R}$ dans $\mathbb{R}_+$, rencontrée à la section 2.2.1.

2.3 Image directe et image réciproque

Définition : Soit $f : E \to F$ une application.

- Pour toute partie A de E, l'**image directe** de A par f est la partie de F

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

  L'ensemble $f(E)$ est l'**image** de f, notée aussi $\operatorname{Im} f$.
- Pour toute partie B de F, l'**image réciproque** de B par f est la partie de E

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

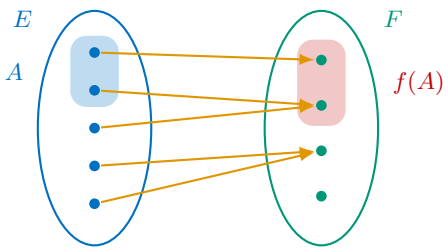


image directe $f(A)$

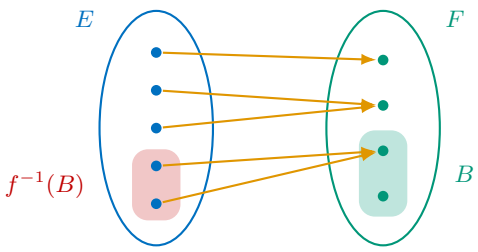


image réciproque $f^{-1}(B)$

Les deux panneaux représentent la même application d'un ensemble à cinq éléments dans un ensemble à quatre éléments. À gauche, $f(A)$ est formé des extrémités des flèches issues de A. À droite, $f^{-1}(B)$ est formé des origines des flèches qui aboutissent dans B ; le point le plus bas de B, qui ne reçoit aucune flèche, n'apporte rien à $f^{-1}(B)$.

Exemple : Soit

$$f : \left| \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^2 \end{array} \right.$$

Alors $f([-1\,,2]) = [0\,,4]$, et non $[1\,,4]$: l'image d'un intervalle n'est pas l'intervalle des images des extrémités. On a aussi

$$f^{-1}([1\,,4]) = [-2\,,-1] \cup [1\,,2], \qquad f^{-1}(\{0\}) = \{0\}, \qquad f^{-1}([-3\,,-1]) = \varnothing,$$

ce qui montre qu'une image réciproque peut être vide.

Remarque : L'erreur la plus répandue est de croire que la notation $f^{-1}(B)$ suppose l'existence d'une « application réciproque » f^{-1}. Il n'en est rien : l'image réciproque d'une partie est définie pour *toute* application, comme l'exemple de la fonction carré le montre. La notation sera justifiée à la section 2.5.3, où l'on verra que, lorsque f est bijective, les deux lectures possibles de $f^{-1}(B)$ désignent le même ensemble. Par prudence, on évitera d'écrire $f^{-1}(y)$ pour un élément y, et l'on écrira $f^{-1}(\{y\})$, ensemble des antécédents de y.

Proposition 2 : Soit $f : E \to F$ une application, A et A' deux parties de E, B et B' deux parties de F.

(i) *Image directe :* $f(A \cup A') = f(A) \cup f(A')$ et $f(A \cap A') \subset f(A) \cap f(A')$.

(ii) *Image réciproque :* $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$, $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$, $f^{-1}(F \setminus B) = E \setminus f^{-1}(B)$.

(iii) $A \subset f^{-1}\big(f(A)\big)$ et $f\big(f^{-1}(B)\big) \subset B$.

Ces propriétés s'étendent aux réunions et intersections d'une famille quelconque de parties.

∘ Démonstration : **(i)** Soit $y \in F$. Comme « il existe » se distribue sur « ou », on a

$$\begin{aligned} y \in f(A \cup A') &\iff \exists x \in A \cup A',\ y = f(x) \\ &\iff \big(\exists x \in A,\ y = f(x)\big) \ \text{ ou } \ \big(\exists x \in A',\ y = f(x)\big) \\ &\iff y \in f(A) \cup f(A'). \end{aligned}$$

Pour l'intersection, si $y = f(x)$ avec $x \in A \cap A'$, alors $y \in f(A)$ et $y \in f(A')$, donc $y \in f(A) \cap f(A')$.

(ii) Soit $x \in E$. On a

$$\begin{aligned} x \in f^{-1}(B \cap B') &\iff f(x) \in B \cap B' \\ &\iff \big(f(x) \in B \ \text{ et } \ f(x) \in B'\big) \\ &\iff x \in f^{-1}(B) \cap f^{-1}(B'). \end{aligned}$$

Les deux autres égalités se démontrent de la même façon, en remplaçant « et » par « ou », puis par « non ».

(iii) Si $x \in A$, alors $f(x) \in f(A)$, donc $x \in f^{-1}(f(A))$. Si $y \in f(f^{-1}(B))$, il s'écrit $y = f(x)$ avec $x \in f^{-1}(B)$, c'est-à-dire $f(x) \in B$; donc $y \in B$. □

Remarques :

- Les inclusions de cette proposition peuvent être strictes, et c'est le piège principal de la section. Avec la fonction carré sur $\mathbb{R}$ et les parties $A = [-2\,,-1]$, $A' = [1\,,2]$, on obtient

$$f(A \cap A') = f(\varnothing) = \varnothing \qquad \text{alors que} \qquad f(A) \cap f(A') = [1\,,4],$$
$$f^{-1}\big(f([0\,,1])\big) = f^{-1}([0\,,1]) = [-1\,,1] \supsetneq [0\,,1],$$
$$f\big(f^{-1}([-1\,,4])\big) = f([-2\,,2]) = [0\,,4] \subsetneq [-1\,,4].$$

  On verra à la section 2.5 que ces défauts disparaissent exactement lorsque f est injective, pour les deux premiers, ou surjective, pour le dernier.

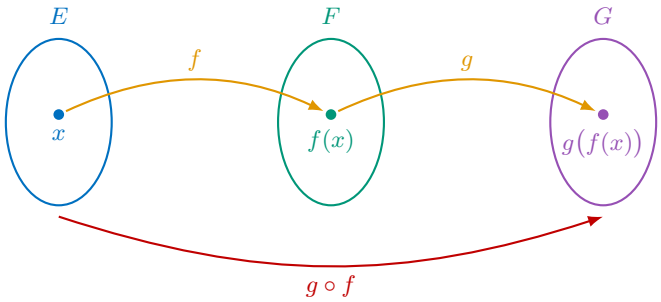
- L'image réciproque se comporte donc parfaitement avec toutes les opérations du dictionnaire logique / ensembles qui clôt le chapitre 1, ce qui n'est pas le cas de l'image directe. La raison est visible sur les démonstrations : $f^{-1}(B)$ se définit sans quantificateur, alors que $f(A)$ contient un « il existe », qui se distribue sur « ou » mais pas sur « et ». C'est le phénomène déjà rencontré à l'exercice 38 de la feuille du chapitre 1.

2.4 Composition

Définition : Soit $f : E \to F$ et $g : F \to G$ deux applications. La **composée** de f suivie de g est l'application

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

On lit « g rond f ». Plus généralement, $g \circ f$ est définie dès que $f(E)$ est contenu dans l'ensemble de départ de g.



On applique d'abord f, puis g : la notation $g \circ f$ se lit de droite à gauche, dans l'ordre inverse de celui où les applications agissent, parce que l'on écrit $g(f(x))$ avec la variable à droite.

Exemple : Soit $f, g : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = x + 1$ et $g(x) = x^2$. Alors $(g \circ f)(x) = (x+1)^2$ et $(f \circ g)(x) = x^2 + 1$. En $x = 1$, on obtient 4 et 2 : la composition n'est pas commutative, et $g \circ f \neq f \circ g$ en général. Il arrive même que $g \circ f$ soit définie sans que $f \circ g$ le soit, lorsque les ensembles ne s'y prêtent pas.

Proposition 3 : Soit $f : E \to F$, $g : F \to G$ et $h : G \to H$ trois applications. Alors

$$h \circ (g \circ f) = (h \circ g) \circ f \qquad \text{et} \qquad f \circ \mathrm{id}_E = \mathrm{id}_F \circ f = f.$$

∘ Démonstration : Les deux applications ont pour départ E et pour arrivée H, et pour tout $x \in E$, elles prennent toutes deux la valeur $h\big(g(f(x))\big)$. La seconde affirmation est immédiate. □

Remarque : Grâce à l'associativité, on écrit simplement $h \circ g \circ f$, sans parenthèses. Pour une application $f : E \to E$, on note $f^n = f \circ \cdots \circ f$ (n facteurs), avec la convention $f^0 = \mathrm{id}_E$. Il ne faut pas confondre cette *itérée* avec la puissance $x \mapsto f(x)^n$: pour $f = \sin$, la notation $\sin^2 x$ désigne traditionnellement $(\sin x)^2$, et non $\sin(\sin x)$. Le contexte doit toujours lever l'ambiguïté. La suite récurrente $u_{n+1} = f(u_n)$, étudiée au chapitre 7, vérifie $u_n = f^n(u_0)$.

2.5 Injections, surjections, bijections

2.5.1 Injections et surjections

Définition : Soit $f : E \to F$ une application.

- f est **injective** (ou est une **injection**) si deux éléments distincts ont des images distinctes :

$$\forall (x, x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'$$

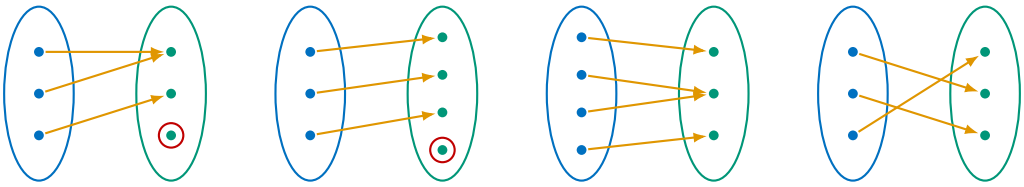
- f est **surjective** (ou est une **surjection**) si tout élément de F a au moins un antécédent :

$$\forall y \in F,\ \exists x \in E,\ y = f(x), \quad \text{c'est-à-dire} \quad f(E) = F.$$

- f est **bijective** (ou est une **bijection**) si elle est injective et surjective, c'est-à-dire si

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

Ces trois définitions se lisent toutes sur l'équation $f(x) = y$, d'inconnue $x \in E$, où y est un élément donné de F : l'application f est injective si, pour tout y, cette équation a *au plus* une solution ; surjective si elle en a *au moins* une ; bijective si elle en a *exactement* une.



Sur ces diagrammes, l'injectivité se lit à l'arrivée : aucun point de F ne reçoit deux flèches. La surjectivité se lit aussi à l'arrivée : chaque point de F reçoit au moins une flèche ; les points entourés n'en reçoivent aucune. Une bijection apparie exactement les points de E et ceux de F.

Exemples :

- L'application $\mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$, est injective, car $2n = 2n'$ entraîne $n = n'$, mais elle n'est pas surjective, puisque 1 n'a pas d'antécédent. L'application $\mathbb{N} \to \mathbb{N}$, $n \mapsto \lfloor n/2 \rfloor$, est surjective, puisque $m = \lfloor 2m/2 \rfloor$, mais elle n'est pas injective, puisque 0 et 1 ont la même image.
- La fonction carré n'est ni injective ni surjective de $\mathbb{R}$ dans $\mathbb{R}$, puisque $f(-1) = f(1)$ et que -1 n'a pas d'antécédent ; elle est surjective de $\mathbb{R}$ dans $\mathbb{R}_+$; et elle est bijective de $\mathbb{R}_+$ dans $\mathbb{R}_+$. La même « formule » définit donc des applications aux propriétés différentes : l'injectivité dépend de l'ensemble de départ, la surjectivité de l'ensemble d'arrivée.

♡ **Méthode : Pour démontrer que f est injective**, on fixe x et x' dans E tels que $f(x) = f(x')$, et l'on démontre que $x = x'$. **Pour démontrer qu'elle ne l'est pas**, on exhibe $x \neq x'$ tels que $f(x) = f(x')$.

Pour démontrer que f est surjective, on fixe $y \in F$ et l'on trouve un antécédent, souvent par analyse-synthèse : on résout $f(x) = y$, puis on vérifie que la solution trouvée appartient bien à E. **Pour démontrer qu'elle ne l'est pas**, on exhibe un $y \in F$ sans antécédent.

Pour démontrer que f est bijective, il suffit souvent de montrer que l'équation $f(x) = y$ a une unique solution dans E pour tout $y \in F$; l'expression de cette solution en fonction de y fournit alors l'application réciproque de la section 2.5.3.

Exemple : Soit

$$f : \left| \begin{array}{ccc} \mathbb{R} \setminus \{1\} & \longrightarrow & \mathbb{R} \setminus \{2\} \\ x & \longmapsto & \dfrac{2x+1}{x-1} \end{array} \right.$$

Elle est bien définie, car $f(x) = 2$ conduirait à $2x + 1 = 2x - 2$, ce qui est impossible. Soit $y \in \mathbb{R} \setminus \{2\}$. Pour $x \neq 1$, on a

$$f(x) = y \iff 2x + 1 = y(x - 1) \iff x(2 - y) = -y - 1 \iff x = \frac{y+1}{y-2},$$

puisque $y \neq 2$. Ce réel est bien différent de 1, car $y+1 = y-2$ est impossible. L'équation $f(x) = y$ a donc une unique solution dans $\mathbb{R} \setminus \{1\}$: f est bijective, et l'on vérifie par exemple que $f(0) = -1$ et que $\frac{-1+1}{-1-2} = 0$.

Proposition 4 : Soit I une partie de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction **strictement monotone**. Alors f est injective, et l'application induite $I \to f(I)$, $x \mapsto f(x)$, est bijective.

∘ Démonstration : Supposons f strictement croissante, l'autre cas étant analogue. Soit $x \neq x'$ dans I, par exemple $x < x'$. Alors $f(x) < f(x')$, donc $f(x) \neq f(x')$: c'est la contraposée de l'injectivité. L'application induite est injective pour la même raison, et surjective par définition de $f(I)$. □

Remarque : La réciproque est fausse : la fonction définie sur $\mathbb{R}$ par $f(x) = x$ pour $x \in \mathbb{Q}$ et $f(x) = -x$ sinon est injective sans être monotone sur aucun intervalle : comme la fonction de Dirichlet, qui vaut 1 sur $\mathbb{Q}$ et 0 ailleurs, elle change de comportement entre deux réels aussi proches que l'on veut. On verra au chapitre 8 qu'une fonction *continue* et injective sur un intervalle est, elle, nécessairement strictement monotone.

Proposition 5 : Soit $f : E \to F$ une application, A une partie de E et B une partie de F.

(i) Si f est injective, alors $f^{-1}(f(A)) = A$.

(ii) Si f est surjective, alors $f(f^{-1}(B)) = B$.

∘ Démonstration : **(i)** L'inclusion $A \subset f^{-1}(f(A))$ est toujours vraie (proposition 2). Soit $x \in f^{-1}(f(A))$: alors $f(x) \in f(A)$, donc $f(x) = f(a)$ pour un certain $a \in A$, et l'injectivité donne $x = a \in A$.

(ii) L'inclusion $f(f^{-1}(B)) \subset B$ est toujours vraie. Soit $y \in B$: par surjectivité, $y = f(x)$ pour un $x \in E$, qui vérifie $f(x) \in B$, c'est-à-dire $x \in f^{-1}(B)$; donc $y \in f(f^{-1}(B))$. □

2.5.2 Composition et injectivité

Proposition 6 : Soit $f : E \to F$ et $g : F \to G$ deux applications.

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

(ii) Si $g \circ f$ est injective, alors f est injective.

(iii) Si $g \circ f$ est surjective, alors g est surjective.

∘ Démonstration : **(i)** *Injections.* Supposons f et g injectives, et soit x, x' tels que $g(f(x)) = g(f(x'))$. L'injectivité de g donne $f(x) = f(x')$, puis celle de f donne $x = x'$.

Surjections. Supposons f et g surjectives, et soit $z \in G$. Il existe $y \in F$ tel que $z = g(y)$, puis $x \in E$ tel que $y = f(x)$, d'où $z = (g \circ f)(x)$.

Bijections. Ce cas réunit les deux précédents.

(ii) Si $f(x) = f(x')$, alors $g(f(x)) = g(f(x'))$, donc $x = x'$ par injectivité de $g \circ f$.

(iii) Soit $z \in G$. Il existe $x \in E$ tel que $z = g(f(x))$: l'élément $y = f(x)$ de F est un antécédent de z par g. □

Remarque : Les points (ii) et (iii) sont dissymétriques, et il faut les retenir dans le bon sens : si $g \circ f$ est injective, c'est l'application appliquée *en premier*, f, qui est injective ; si $g \circ f$ est surjective, c'est l'application appliquée *en dernier*, g, qui est surjective. L'autre application peut ne pas l'être : avec $f : \{0\} \to \{0,1\}$, $0 \mapsto 0$, et $g : \{0,1\} \to \{0\}$, l'application $g \circ f$ est l'identité de $\{0\}$, donc bijective, alors que g n'est pas injective et que f n'est pas surjective.

2.5.3 Bijections et application réciproque

Théorème 1 : Caractérisation des bijections :
Une application $f : E \to F$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que

$$g \circ f = \mathrm{id}_E \qquad \text{et} \qquad f \circ g = \mathrm{id}_F.$$

Une telle application g est alors unique ; on l'appelle l'**application réciproque** de f, et on la note f^{-1}. Elle associe à tout $y \in F$ l'unique antécédent de y par f :

$$\forall (x,y) \in E \times F, \quad y = f(x) \iff x = f^{-1}(y).$$

∘ Démonstration : *Si f est bijective, g existe.* Pour tout $y \in F$, notons $g(y)$ l'unique antécédent de y : cela définit une application $g : F \to E$ telle que $f(g(y)) = y$ pour tout y, c'est-à-dire $f \circ g = \mathrm{id}_F$. Pour $x \in E$, l'élément x est un antécédent de $f(x)$, et c'est le seul : donc $g(f(x)) = x$, et $g \circ f = \mathrm{id}_E$.

Si g existe, f est bijective. L'application $g \circ f = \mathrm{id}_E$ est injective, donc f est injective d'après la proposition 6 (ii) ; l'application $f \circ g = \mathrm{id}_F$ est surjective, donc f est surjective d'après la proposition 6 (iii).

Unicité de g. Si g et g' conviennent, alors, grâce à l'associativité,

$$g = g \circ \mathrm{id}_F = g \circ (f \circ g') = (g \circ f) \circ g' = \mathrm{id}_E \circ g' = g'.$$

Lien entre f et f^{-1}. Soit $(x,y) \in E \times F$. Si $y = f(x)$, alors $f^{-1}(y) = f^{-1}(f(x)) = x$; si $x = f^{-1}(y)$, alors $f(x) = f(f^{-1}(y)) = y$. □

Remarque : Les deux égalités sont indispensables. Soit

$$f : \left| \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n+1 \end{array} \right. \qquad \text{et} \qquad g : \left| \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \begin{cases} 0 & \text{si } n = 0 \\ n-1 & \text{si } n \geqslant 1 \end{cases} \end{array} \right.$$

Alors $g \circ f = \mathrm{id}_{\mathbb{N}}$, puisque $g(n+1) = n$; mais $f \circ g \neq \mathrm{id}_{\mathbb{N}}$, puisque $f(g(0)) = 1$. Et en effet f n'est pas bijective : 0 n'a pas d'antécédent. Une telle application g est seulement un *inverse à gauche* de f.

Proposition 7 : Soit $f : E \to F$ et $g : F \to G$ deux bijections.

(i) L'application f^{-1} est bijective, et $(f^{-1})^{-1} = f$.

(ii) L'application $g \circ f$ est bijective, et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(iii) Pour toute partie B de F, l'image réciproque de B par f est égale à l'image directe de B par f^{-1}.

∘ Démonstration : **(i)** Les égalités $f^{-1} \circ f = \mathrm{id}_E$ et $f \circ f^{-1} = \mathrm{id}_F$ montrent, par le théorème 1 appliqué à f^{-1}, que f^{-1} est bijective, de réciproque f.

(ii) Par associativité,

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

et de même $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_G$. On conclut par le théorème 1.

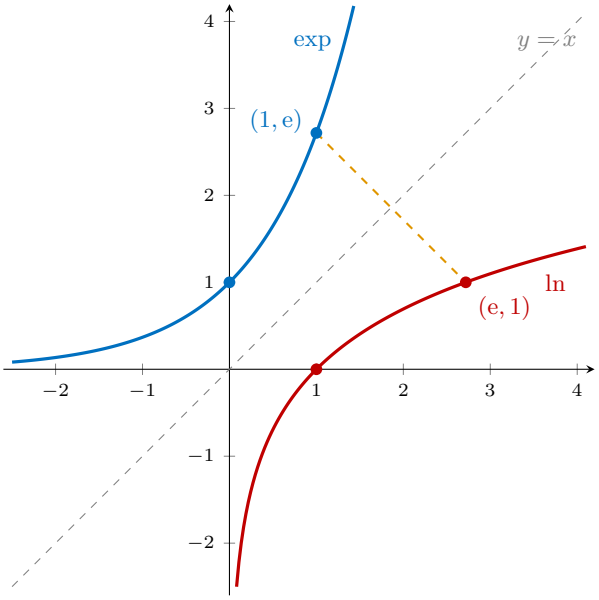
(iii) Soit $x \in E$. En posant $y = f(x)$ et en utilisant le théorème 1, on obtient

$$x \in f^{-1}(B) \iff f(x) \in B \iff \exists y \in B,\ x = f^{-1}(y),$$

ce qui est la définition de l'image directe de B par f^{-1}. □

Remarque : L'ordre de la formule (ii) s'impose dès qu'on y réfléchit : pour défaire « f puis g », on défait d'abord g, puis f, comme on retire ses chaussures avant ses chaussettes. Écrire $g^{-1} \circ f^{-1}$ est l'erreur la plus répandue, et elle n'a même pas de sens en général : f^{-1} arrive dans E, qui n'est pas l'ensemble de départ de g^{-1}. Le point (iii) justifie enfin la notation $f^{-1}(B)$: lorsque f est bijective, ses deux lectures désignent le même ensemble.

Lorsque E et F sont des parties de $\mathbb{R}$, la relation $y = f(x) \Leftrightarrow x = f^{-1}(y)$ signifie que le point (x, y) appartient au graphe de f si et seulement si le point (y, x) appartient au graphe de f^{-1}.



La fonction exponentielle est une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$, dont la réciproque est le logarithme népérien. Les deux courbes sont symétriques par rapport à la droite d'équation $y = x$: le point $(1, \mathrm{e})$ de la courbe de exp a pour symétrique le point $(\mathrm{e}, 1)$ de celle de ln, et le segment qui les joint, en pointillés orange, est perpendiculaire à cette droite.

Exemple : La bijection de l'exemple de la section 2.5.1 a pour réciproque

$$f^{-1} : \left| \begin{array}{ccc} \mathbb{R} \setminus \{2\} & \longrightarrow & \mathbb{R} \setminus \{1\} \\ y & \longmapsto & \dfrac{y+1}{y-2} \end{array} \right.$$

que l'analyse-synthèse a fournie directement. De même, la fonction $x \mapsto x^2$ induit une bijection de $\mathbb{R}_+$ sur $\mathbb{R}_+$, dont la réciproque est la racine carrée. D'autres réciproques, comme les fonctions arccos, arcsin et arctan, seront construites au chapitre 5 en restreignant les fonctions trigonométriques à des intervalles où elles sont strictement monotones, grâce à la proposition 4.

2.5.4 Ensembles finis et théorème de Cantor

L'expression « ensemble à n éléments » est employée depuis le chapitre 1 sans avoir été définie. Les bijections permettent de lui donner un sens précis : avoir n éléments, c'est pouvoir numéroter ses éléments de 1 à n, sans oubli ni répétition. Pour deux entiers m et n, on note $[\![m\,,n]\!] = \{k \in \mathbb{Z} \mid m \leqslant k \leqslant n\}$; cet ensemble est vide lorsque $n < m$, et en particulier $[\![1\,,0]\!] = \varnothing$.

Définition : Un ensemble E est **fini** s'il existe un entier naturel n et une bijection $\varphi : [\![1\,,n]\!] \to E$, que l'on appelle une **numérotation** de E. Un ensemble qui n'est pas fini est dit **infini**.

Pour $n = 0$, l'ensemble $[\![1\,,0]\!]$ est vide, et la seule application de $\varnothing$ dans E, de graphe vide, est bijective si et seulement si E est vide : l'ensemble vide est fini, numéroté par 0 entier. Pour qu'il soit légitime de parler du *nombre* d'éléments de E, il reste à montrer que deux numérotations de E utilisent le même entier n. Tout repose sur le lemme suivant.

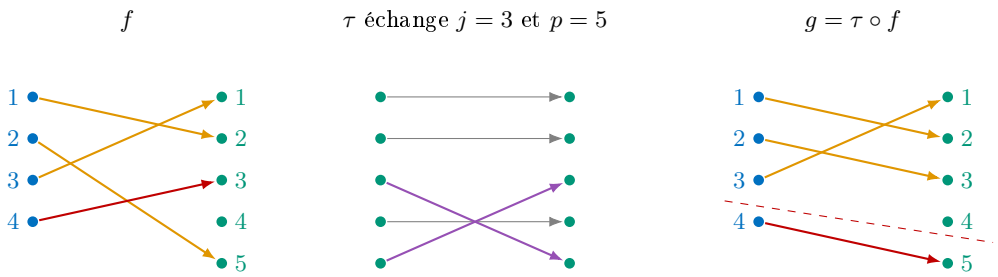
Lemme 1 : *(Principe des tiroirs.)* Soit n et p deux entiers naturels. S'il existe une injection de $[\![1\,,n]\!]$ dans $[\![1\,,p]\!]$, alors $n \leqslant p$.

∘ Démonstration : On démontre par récurrence sur n l'assertion $P(n)$: « pour tout $p \in \mathbb{N}$, s'il existe une injection de $[\![1\,,n]\!]$ dans $[\![1\,,p]\!]$, alors $n \leqslant p$ ».

Initialisation. L'assertion $P(0)$ est vraie, puisque $0 \leqslant p$ pour tout $p \in \mathbb{N}$.

Hérédité. Supposons $P(n)$ vraie, et soit $f : [\![1\,,n+1]\!] \to [\![1\,,p]\!]$ une injection. L'ensemble de départ n'est pas vide, donc $[\![1\,,p]\!]$ non plus, et $p \geqslant 1$. On commence par modifier f pour que $n+1$ soit envoyé sur p. Notons $j = f(n+1)$ et $\tau : [\![1\,,p]\!] \to [\![1\,,p]\!]$ l'application qui échange j et p et laisse fixes les autres entiers ; elle vérifie $\tau \circ \tau = \mathrm{id}$, donc elle est bijective, et c'est l'identité si $j = p$. L'application $g = \tau \circ f$ est injective, comme composée de deux injections, et $g(n+1) = \tau(j) = p$.

Pour $k \in [\![1\,,n]\!]$, on a $k \neq n+1$, donc $g(k) \neq g(n+1) = p$ par injectivité : la restriction de g à $[\![1\,,n]\!]$ est une injection de $[\![1\,,n]\!]$ dans $[\![1\,,p-1]\!]$. L'hypothèse de récurrence donne $n \leqslant p-1$, c'est-à-dire $n+1 \leqslant p$. □



La figure illustre l'hérédité pour $n+1 = 4$ et $p = 5$. À gauche, l'injection f envoie 4 sur $j = 3$, en rouge. Au centre, la bijection τ, en violet, échange 3 et 5. À droite, la composée $g = \tau \circ f$ est encore injective, envoie 4 sur 5, et les trois autres éléments, au-dessus du trait pointillé, sur $[\![1\,,4]\!]$: on s'est ramené au rang précédent.

Lemme 2 : Soit E un ensemble fini.

(i) Toutes les numérotations de E sont définies sur le même intervalle $[\![1\,,n]\!]$.

(ii) Si F est un ensemble en bijection avec E, alors F est fini, et ses numérotations sont définies sur ce même intervalle $[\![1\,,n]\!]$.

∘ Démonstration : Soit $\varphi : [\![1\,,n]\!] \to E$ et $\psi : [\![1\,,m]\!] \to E$ deux numérotations de E. L'application $\psi^{-1} \circ \varphi$ est une bijection de $[\![1\,,n]\!]$ sur $[\![1\,,m]\!]$, comme composée de deux bijections. Elle est en particulier injective, et le lemme 1 donne $n \leqslant m$. Sa réciproque $\varphi^{-1} \circ \psi$ donne de même $m \leqslant n$, d'où $n = m$.

Si $h : E \to F$ est une bijection et φ une numérotation de E, alors $h \circ \varphi : [\![1\,,n]\!] \to F$ est une bijection : c'est une numérotation de F, définie sur le même intervalle, et le point (i) s'applique à F. □

Définition : Soit E un ensemble fini. L'unique entier n tel qu'il existe une bijection de $[\![1\,,n]\!]$ sur E est appelé le **cardinal**, ou **nombre d'éléments**, de E, et noté $\mathrm{card}(E)$. D'après le lemme 2, deux ensembles en bijection ont le même cardinal.

Remarques :

- Le lemme 1 est le véritable contenu du lemme 2 : sans lui, rien n'empêcherait a priori qu'un ensemble puisse être numéroté à la fois de 1 à 5 et de 1 à 6. Ce qui semble évident ici l'est beaucoup moins pour les ensembles infinis, comme on le verra plus bas avec l'hôtel de Hilbert.
- Nous admettons les propriétés usuelles de $\mathbb{N}$: addition, ordre, raisonnement par récurrence et existence d'un plus petit élément dans toute partie non vide. Leur construction à partir de la seule théorie des ensembles est hors programme.

On établit maintenant deux règles de calcul sur les cardinaux, qui serviront dès le chapitre 3.

Lemme 3 : Soit E un ensemble fini et A une partie de E.

(i) La partie A est finie, et $\mathrm{card}(A) \leqslant \mathrm{card}(E)$, avec égalité si et seulement si $A = E$.

(ii) Si $a \in E$, alors $\mathrm{card}\big(E \setminus \{a\}\big) = \mathrm{card}(E) - 1$.

∘ Démonstration : On démontre les deux points ensemble, par récurrence sur $n = \text{card}(E)$. Pour $n = 0$, l'ensemble E est vide, sa seule partie est $\varnothing = E$, et le point (ii) ne dit rien. Supposons les deux points vrais pour les ensembles à n éléments, et soit E un ensemble à $n+1$ éléments, numéroté par $\varphi : [\![1\,, n+1]\!] \to E$.

Le point (ii). Pour $a = \varphi(n+1)$, la restriction de φ à $[\![1\,, n]\!]$ est une bijection de $[\![1\,, n]\!]$ sur $E \setminus \{a\}$, qui a donc n éléments. Pour un autre élément $a = \varphi(i)$, on se ramène à ce cas en remplaçant φ par $\varphi \circ \tau$, où τ échange i et $n+1$: c'est encore une numérotation de E, qui envoie $n+1$ sur a.

Le point (i). Soit $A \subset E$, $a = \varphi(n+1)$ et $E' = E \setminus \{a\}$, qui a n éléments. On distingue deux cas.

- Si $a \notin A$, alors $A \subset E'$. Par hypothèse de récurrence, A est finie et $\text{card}(A) \leqslant n < n+1$; en particulier $A \neq E$, puisque $a \in E$.
- Si $a \in A$, alors $A \setminus \{a\} \subset E'$ est finie, avec $m \leqslant n$ éléments, et l'égalité $m = n$ a lieu si et seulement si $A \setminus \{a\} = E'$. Une numérotation ψ de $A \setminus \{a\}$, prolongée par $\psi(m+1) = a$, numérote A : ainsi $\text{card}(A) = m+1 \leqslant n+1$, avec égalité si et seulement si $A \setminus \{a\} = E'$, c'est-à-dire $A = E$.

□

Lemme 4 : Soit A et B deux ensembles finis *disjoints*. Alors $A \cup B$ est fini et

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B).$$

∘ Démonstration : Soit $\varphi : [\![1\,, p]\!] \to A$ et $\psi : [\![1\,, q]\!] \to B$ deux numérotations. On numérote d'abord les éléments de A, puis ceux de B, en posant

$$\chi(k) = \varphi(k) \quad \text{si } 1 \leqslant k \leqslant p, \qquad \chi(k) = \psi(k-p) \quad \text{si } p+1 \leqslant k \leqslant p+q.$$

L'application $\chi : [\![1\,, p+q]\!] \to A \cup B$ est surjective, puisque chaque élément de A est atteint par φ et chaque élément de B par ψ. Elle est injective : deux indices du même bloc ont des images distinctes, par injectivité de φ ou de ψ, et deux indices de blocs différents ont l'un une image dans A, l'autre dans B, qui sont distinctes puisque $A \cap B = \varnothing$. □

Remarque : L'hypothèse de disjonction est indispensable : pour $A = \{1, 2\}$ et $B = \{2, 3\}$, on a $\text{card}(A \cup B) = 3 \neq 2 + 2$. Dans le cas général, on écrit $A \cup B$ comme réunion disjointe de A et de $B \setminus A$, ce qui conduit à la formule $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)$, que l'exercice 25 de la feuille établit.

Lorsque l'on découpe un ensemble selon les valeurs d'une application, le lemme 4 se généralise en une règle de comptage très souvent utilisée. Pour $f : E \to F$ et $y \in F$, la partie $f^{-1}(\{y\})$ des antécédents de y s'appelle la **fibre** de f au-dessus de y.

Lemme 5 : *(Lemme des bergers.)* Soit $f : E \to F$ une application, où F est un ensemble fini, et k un entier naturel. Si chaque fibre $f^{-1}(\{y\})$, pour $y \in F$, est finie à k éléments, alors E est fini et

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

∘ Démonstration : On raisonne par récurrence sur $p = \text{card}(F)$, l'entier k étant fixé. Si $p = 0$, l'ensemble F est vide ; comme tout élément de E aurait une image dans F, l'ensemble E est vide lui aussi, et $\text{card}(E) = 0 = k \times 0$.

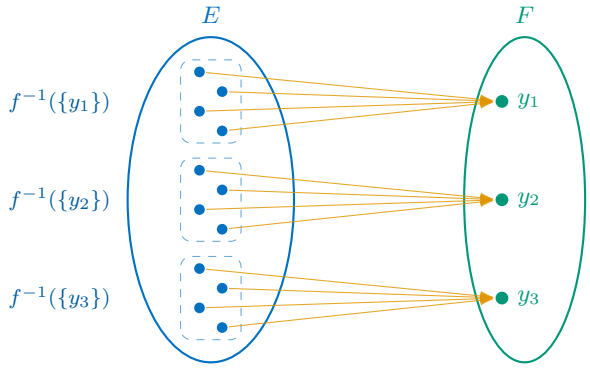
Supposons le résultat vrai pour les ensembles d'arrivée à p éléments, et soit F à $p+1$ éléments. On choisit $y \in F$ et l'on pose $F' = F \setminus \{y\}$, qui a p éléments d'après le lemme 3, et $E' = f^{-1}(F') = E \setminus f^{-1}(\{y\})$. L'application

$$f' : \left| \begin{array}{ccc} E' & \longrightarrow & F' \\ x & \longmapsto & f(x) \end{array} \right.$$

est bien définie, et ses fibres sont celles de f au-dessus des points de F', qui ont k éléments. Par hypothèse de récurrence, E' est fini et $\text{card}(E') = kp$. Enfin E est la réunion disjointe de E' et de la fibre $f^{-1}(\{y\})$, et le lemme 4 donne

$$\text{card}(E) = kp + k = k\,(p+1).$$

□



Ici F a trois éléments, et chaque fibre, entourée en pointillés, en a quatre : l'ensemble E en a donc $4 \times 3 = 12$. Le nom du lemme vient de l'image du berger qui compte ses moutons en comptant les pattes, puis en divisant par 4 : l'ensemble des pattes est découpé en fibres de quatre éléments au-dessus de l'ensemble des moutons.

Lemme 6 : *(Produit cartésien.)* Si E et F sont deux ensembles finis, alors $E \times F$ est fini et

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

∘ Démonstration : On applique le lemme 5 à la projection $\pi : E \times F \to F$, $(x, y) \mapsto y$. Pour $y \in F$, sa fibre est $E \times \{y\}$, qui est en bijection avec E par $x \mapsto (x, y)$: elle a $\text{card}(E)$ éléments, d'après le lemme 2. □

Remarques :

- Par récurrence sur r, on en déduit que $E_1 \times \cdots \times E_r$ a $\text{card}(E_1) \times \cdots \times \text{card}(E_r)$ éléments. Par exemple, le lancer de deux dés donne $6 \times 6 = 36$ résultats, et un code de carte bancaire à quatre chiffres peut prendre 10^4 valeurs. C'est le *principe multiplicatif*, que le chapitre 21 utilisera constamment.
- Le lemme des bergers permet aussi de dénombrer les applications : l'exercice 25 de la feuille montre ainsi qu'il y a n^p applications d'un ensemble à p éléments dans un ensemble à n éléments, en regroupant les applications selon l'image d'un point fixé. Le chapitre 3, qui introduit le symbole $\sum$, en donnera la forme générale, où les fibres n'ont pas toutes le même nombre d'éléments.

On peut maintenant démontrer le résultat principal de cette section, qui compare les cardinaux à l'aide des applications.

Théorème 2 : Applications entre ensembles finis :
Soit E et F deux ensembles finis, à n et p éléments, et $f : E \to F$ une application.

- Si f est injective, alors $n \leqslant p$. Si f est surjective, alors $n \geqslant p$.
- Si $n = p$, alors f injective $\iff$ f surjective $\iff$ f bijective.

∘ Démonstration : **Injections.** Si f est injective, elle induit une bijection de E sur son image $f(E)$. D'après le lemme 2, $f(E)$ a n éléments, et le lemme 3, appliqué à la partie $f(E)$ de F, donne $n \leqslant p$.

Surjections. Supposons f surjective, et fixons une numérotation φ de E. Pour $y \in F$, l'ensemble des entiers $k \in [\![1, n]\!]$ tels que $f(\varphi(k)) = y$ n'est pas vide ; on note k_y son plus petit élément, et l'on pose $g(y) = \varphi(k_y)$. On a construit ainsi une application $g : F \to E$ telle que $f \circ g = \text{id}_F$. Elle est injective, puisque $g(y) = g(y')$ entraîne $y = f(g(y)) = f(g(y')) = y'$. Le premier point, appliqué à g, donne $p \leqslant n$.

Cas $n = p$. Si f est injective, $f(E)$ est une partie de F ayant autant d'éléments que F : d'après le cas d'égalité du lemme 3, $f(E) = F$, et f est surjective. Si f est surjective, l'application g construite ci-dessus est une injection de F dans E, avec $p = n$: elle est donc surjective, d'après ce qui précède, donc bijective. L'égalité $f \circ g = \text{id}_F$ donne alors $f = f \circ g \circ g^{-1} = g^{-1}$, qui est bijective. Enfin, une bijection est injective et surjective. □

La contraposée du premier point est le **principe des tiroirs** sous sa forme usuelle : si $n > p$, aucune application de E dans F n'est injective, c'est-à-dire que si l'on range n objets dans $p < n$ tiroirs, deux objets au moins partagent un tiroir.

Exemple : Parmi 13 personnes, deux au moins sont nées le même mois, puisque l'application qui associe à chaque personne son mois de naissance va d'un ensemble à 13 éléments dans un ensemble à 12 éléments. L'exercice 43 de la feuille du chapitre 1 démontrait déjà ce principe, et en tirait que deux inscrits d'un réseau social ont toujours le même nombre d'amis.

Remarques :

- La construction de g, dans la démonstration du théorème 2, choisit pour chaque y le plus petit antécédent dans la numérotation de E. C'est ce qui permet de se passer de l'*axiome du choix*, indispensable en revanche pour construire un tel g lorsque E est infini et n'est pas numéroté.
- Le second point est faux pour les ensembles infinis, et c'est même ce qui les caractérise. L'application $\mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$, est injective sans être surjective, et l'application $\mathbb{N} \to \mathbb{N}^*$, $n \mapsto n+1$, est une bijection de $\mathbb{N}$ sur l'une de ses parties strictes. C'est le paradoxe de l'« hôtel de Hilbert » : un hôtel complet ayant une infinité de chambres numérotées peut accueillir un nouveau client, en demandant à chaque occupant de passer de la chambre n à la chambre $n+1$. On en déduit d'ailleurs que $\mathbb{N}$ est infini : s'il était fini, la bijection $n \mapsto n+1$ de $\mathbb{N}$ sur sa partie stricte $\mathbb{N}^*$ contredirait le cas d'égalité du lemme 3.

Définition : Deux ensembles E et F sont dits **équipotents** s'il existe une bijection de E sur F.

D'après le lemme 2, deux ensembles finis sont équipotents si et seulement s'ils ont le même nombre d'éléments : pour la réciproque, si φ et ψ numérotent E et F sur le même intervalle, $\psi \circ \varphi^{-1}$ est une bijection de E sur F. Pour les ensembles infinis, l'équipotence réserve des surprises : $\mathbb{N}$ est équipotent à l'ensemble $2\mathbb{N}$ des entiers pairs, par $n \mapsto 2n$, et même à $\mathbb{Z}$, par l'application qui envoie $2k$ sur k et $2k+1$ sur $-k-1$. Le théorème suivant montre pourtant que tous les ensembles infinis ne sont pas équipotents.

Théorème 3 : Cantor :
Pour tout ensemble E, il n'existe **aucune surjection** de E sur $\mathcal{P}(E)$. En particulier, E et $\mathcal{P}(E)$ ne sont jamais équipotents.

∘ Démonstration : Soit $f : E \to \mathcal{P}(E)$ une application quelconque. Pour chaque $x \in E$, l'image $f(x)$ est une partie de E, qui contient ou non l'élément x. Considérons la partie

$$D = \{x \in E \mid x \notin f(x)\}.$$

Supposons par l'absurde que D ait un antécédent $a \in E$, c'est-à-dire $D = f(a)$, et demandons-nous si a appartient à D.

- Si $a \in D$, alors par définition de D, $a \notin f(a) = D$.
- Si $a \notin D$, alors $a \notin f(a)$, donc $a \in D$ par définition de D.

Dans les deux cas, on aboutit à une contradiction. Ainsi D n'a pas d'antécédent, et f n'est pas surjective. □

Remarque : La partie D est construite pour différer de chaque $f(x)$ au moins en un point, l'élément x lui-même : c'est l'*argument diagonal*. Il est de même nature que le paradoxe de Russell du chapitre 1, où l'ensemble de tous les ensembles x tels que $x \notin x$ conduisait à la même contradiction ; l'exercice 48 de la feuille du chapitre 1 en traitait le cas $E = \mathbb{N}$. Avec $E = \mathbb{N}$, le théorème montre qu'il y a « strictement plus » de parties de $\mathbb{N}$ que d'entiers : on ne peut pas les numéroter. On montrera de même que $\mathbb{R}$ n'est pas équipotent à $\mathbb{N}$, comme Cantor l'avait établi dès 1874.

2.6 Relations binaires

Définition : Une **relation binaire** $\mathcal{R}$ sur un ensemble E est la donnée d'une partie G de $E \times E$, appelée son graphe. Pour $(x, y) \in E^2$, on note $x \mathcal{R} y$, et l'on dit que x est en relation avec y, lorsque $(x, y) \in G$. La relation $\mathcal{R}$ est dite :

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

Comme pour les applications à la section 2.2.1, une relation est donc entièrement décrite par une partie d'un produit cartésien, ici $E \times E$. Une application de E dans E en est un cas particulier : c'est une relation dans laquelle chaque x est en relation avec exactement un y, à savoir $f(x)$, ce qui est la condition $(*)$. Le tableau suivant examine quelques relations familières. Les relations $\equiv$ et $\mid$ seront définies précisément aux sections 2.7.3 et 2.8.1.

Relation	**Ensemble**	réflexive	symétrique	antisymétrique	transitive
$x = y$	quelconque	✓	✓	✓	✓
$x \leqslant y$	$\mathbb{R}$	✓	×	✓	✓
$x < y$	$\mathbb{R}$	×	×	✓	✓
$x \neq y$	$\mathbb{R}$	×	✓	×	×
$A \subset B$	$\mathcal{P}(E)$	✓	×	✓	✓
$a \mid b$	$\mathbb{N}$	✓	×	✓	✓
$a \mid b$	$\mathbb{Z}$	✓	×	×	✓
$a \equiv b\ [3]$	$\mathbb{Z}$	✓	✓	×	✓

Remarque : Antisymétrique ne veut pas dire « non symétrique ». La relation d'égalité est à la fois symétrique et antisymétrique, et la relation $x \neq y$ n'est ni l'une ni l'autre. L'antisymétrie de $<$ est d'ailleurs obtenue « à vide » : l'hypothèse $x < y$ et $y < x$ n'est jamais vraie, donc l'implication l'est toujours, comme on l'a vu au chapitre 1. Pour la ligne $\mid$ sur $\mathbb{Z}$, l'antisymétrie tombe parce que $2 \mid -2$ et $-2 \mid 2$ sans que $2 = -2$.

Deux familles de relations jouent un rôle central : celles qui sont réflexives, symétriques et transitives, qui servent à *identifier* des objets, et celles qui sont réflexives, antisymétriques et transitives, qui servent à les *comparer*.

2.7 Relations d'équivalence

2.7.1 Définition et exemples

Définition : Une **relation d'équivalence** sur un ensemble E est une relation binaire sur E qui est **réflexive**, **symétrique** et **transitive**. On la note souvent $\sim$.

Exemples :

- Soit $f : E \to F$ une application. La relation définie sur E par $x \sim x' \Leftrightarrow f(x) = f(x')$ est une relation d'équivalence, car l'égalité dans F est réflexive, symétrique et transitive. Deux éléments sont équivalents lorsqu'ils ont la même image. Par exemple, avec la fonction valeur absolue sur $\mathbb{R}$, on a $x \sim x' \Leftrightarrow x' = \pm x$. On verra qu'en un sens précis, toutes les relations d'équivalence sont de cette forme.
- Sur l'ensemble des droites du plan, la relation « est parallèle à » est une relation d'équivalence, à condition de considérer qu'une droite est parallèle à elle-même. En revanche, la relation « est perpendiculaire à » n'est ni réflexive ni transitive.

2.7.2 Classes d'équivalence

Définition : Soit $\sim$ une relation d'équivalence sur E et $x \in E$. La **classe d'équivalence** de x est la partie de E

$$\overline{x} = \{y \in E \mid x \sim y\}$$

Tout élément y de $\overline{x}$ est appelé un **représentant** de cette classe.

Remarque : La notation $\overline{x}$ ne mentionne pas la relation, qui doit être claire d'après le contexte ; lorsque plusieurs relations sont en jeu, on précise, par exemple en écrivant $\overline{x}^{\sim}$. La même barre désigne aussi le complémentaire d'une partie, comme au chapitre 1, et désignera le conjugué d'un nombre complexe : l'ambiguïté est rare, puisque $\overline{A}$ s'applique à une partie et $\overline{x}$ à un élément, mais il faut y prendre garde lorsque les éléments sont eux-mêmes des parties.

Théorème 4 : Les classes forment une partition :
Soit $\sim$ une relation d'équivalence sur un ensemble E. Pour tous x, y de E :

$$x \sim y \iff \overline{x} = \overline{y} \qquad \text{et} \qquad x \not\sim y \iff \overline{x} \cap \overline{y} = \varnothing.$$

Les classes d'équivalence distinctes forment donc une **partition** de E.

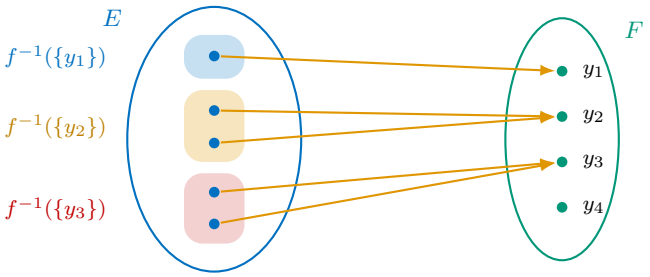
∘ Démonstration : *Première équivalence.* Supposons $x \sim y$. Si $z \in \overline{y}$, alors $y \sim z$, et par transitivité $x \sim z$, donc $z \in \overline{x}$: ainsi $\overline{y} \subset \overline{x}$. Par symétrie, $y \sim x$, et le même argument donne $\overline{x} \subset \overline{y}$. Réciproquement, si $\overline{x} = \overline{y}$, alors $y \in \overline{y}$ par réflexivité, donc $y \in \overline{x}$, c'est-à-dire $x \sim y$.

Seconde équivalence. Si $\overline{x} \cap \overline{y}$ contient un élément z, alors $x \sim z$ et $y \sim z$, donc $z \sim y$ par symétrie et $x \sim y$ par transitivité. Par contraposée, $x \not\sim y$ entraîne $\overline{x} \cap \overline{y} = \varnothing$; et inversement, si $x \sim y$, les classes sont égales et non vides, donc non disjointes.

Partition. Les classes vérifient les trois conditions de la définition du chapitre 1 :

- chaque classe est non vide, puisque $x \in \overline{x}$;
- leur réunion est E, puisque tout x appartient à sa classe ;
- deux classes distinctes sont disjointes, d'après la seconde équivalence.

□



Pour la relation « avoir la même image par f », avec l'application de la section 2.3, les classes sont les ensembles d'antécédents $f^{-1}(\{y\})$, pour $y \in f(E)$: elles découpent E en trois morceaux disjoints, colorés différemment. Le point y_4, sans antécédent, ne fournit aucune classe, puisqu'une classe n'est jamais vide.

Proposition 8 : Réciproquement, soit $(A_i)_{i \in I}$ une partition de E. La relation « appartenir à la même partie », définie par $x \sim y \Leftrightarrow \exists i \in I,\ (x \in A_i \ \text{ et } \ y \in A_i)$, est une relation d'équivalence sur E, dont les classes sont exactement les parties A_i.

∘ Démonstration : Tout $x \in E$ appartient à une unique partie $A_{i(x)}$, puisque les A_i forment un recouvrement disjoint. La relation s'écrit donc

$$x \sim y \iff i(x) = i(y) :$$

c'est la relation « avoir la même image » pour l'application $x \mapsto i(x)$, qui est une relation d'équivalence d'après le premier exemple de la section 2.7.1. La classe de x est l'ensemble des y tels que $i(y) = i(x)$, soit $A_{i(x)}$; et chaque A_i, étant non vide, est la classe de n'importe lequel de ses éléments. □

Remarque : Se donner une relation d'équivalence sur E ou une partition de E revient donc au même, comme l'annonçait le chapitre 1. Cette démonstration explique aussi la remarque de la section 2.7.1 : toute relation d'équivalence est la relation « avoir la même image » pour l'application $x \mapsto \overline{x}$, de E dans $\mathcal{P}(E)$. L'ensemble des classes, appelé ensemble quotient, est hors programme en MPSI, mais l'idée sous-jacente, « identifier les éléments équivalents », sera constamment utilisée.

2.7.3 Congruences dans $\mathbb{Z}$ et dans $\mathbb{R}$

Définition :

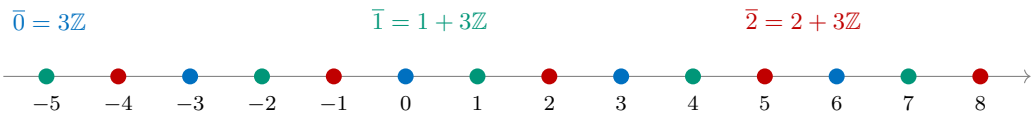
- Soit $n \in \mathbb{N}^*$. Deux entiers a et b sont **congrus modulo** n, et l'on note $a \equiv b\ [n]$, si n divise $b-a$, c'est-à-dire s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$.
- Soit $c > 0$. Deux réels x et y sont **congrus modulo** c, et l'on note $x \equiv y\ [c]$, s'il existe $k \in \mathbb{Z}$ tel que $y = x + kc$.

Proposition 9 : Les congruences modulo n sur $\mathbb{Z}$ et modulo c sur $\mathbb{R}$ sont des relations d'équivalence. La classe d'un entier a modulo n est $a + n\mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\}$, et il y a exactement n classes, celles de 0, 1, …, $n-1$.

∘ Démonstration : *Relation d'équivalence.* On traite le cas de $\mathbb{R}$, celui de $\mathbb{Z}$ étant identique.

- Réflexivité : $x = x + 0 \cdot c$.
- Symétrie : si $y = x + kc$, alors $x = y + (-k)c$.
- Transitivité : si $y = x + kc$ et $z = y + k'c$, alors $z = x + (k + k')c$.

Classes modulo n. Pour $\mathbb{Z}$, la classe de a est par définition $\{a+kn \mid k \in \mathbb{Z}\}$. D'après la division euclidienne, vue en mathématiques expertes, tout entier b s'écrit $b = qn + r$ avec $r \in [\![0\,, n-1]\!]$, donc $b \equiv r\ [n]$: toute classe contient un entier de $[\![0\,, n-1]\!]$. Deux entiers distincts $r < r'$ de $[\![0\,, n-1]\!]$ ne sont pas congrus, car $0 < r' - r < n$ n'est pas un multiple de n. Les classes de 0, …, $n-1$ sont donc distinctes, et ce sont les seules. □



Les entiers de -5 à 8 sont colorés selon leur classe modulo 3. Les trois couleurs se succèdent périodiquement : chaque entier appartient à une et une seule des trois classes, qui forment une partition de $\mathbb{Z}$, et deux entiers ont la même couleur exactement lorsque leur différence est un multiple de 3.

Exemple : Dans $\mathbb{R}$, la congruence modulo 2π est celle des angles : deux réels congrus modulo 2π repèrent le même point du cercle trigonométrique. Chaque classe contient un unique représentant dans $]-\pi\,, \pi]$, la *mesure principale*, et l'on retrouve les écritures de Terminale comme $\cos x = \cos y \iff x \equiv y\ [2\pi]$ ou $x \equiv -y\ [2\pi]$, qui seront reprises dans l'étude de la trigonométrie.

Proposition 10 : (*Compatibilité avec les opérations*) Soit $n \in \mathbb{N}^*$, et a, b, a', b' des entiers tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$. Alors

$$a + a' \equiv b + b'\ [n], \qquad aa' \equiv bb'\ [n], \qquad a^m \equiv b^m\ [n] \ \text{ pour tout } m \in \mathbb{N}.$$

Dans $\mathbb{R}$, si $x \equiv y\ [c]$ et $x' \equiv y'\ [c]$, alors $x + x' \equiv y + y'\ [c]$, et pour tout réel $\lambda > 0$, $\lambda x \equiv \lambda y\ [\lambda c]$.

∘ Démonstration : Écrivons $b = a + kn$ et $b' = a' + k'n$. Alors $b + b' = a + a' + (k + k')n$ et

$$bb' = aa' + (ak' + a'k + kk'n)\,n,$$

d'où les deux premières congruences ; la troisième s'en déduit par récurrence sur m, en multipliant par $a \equiv b$ à chaque étape.

Dans $\mathbb{R}$, si $y = x + kc$ et $y' = x' + k'c$, alors

$$y + y' = x + x' + (k + k')c \qquad \text{et} \qquad \lambda y = \lambda x + k\,(\lambda c).$$

□

Exemple : Déterminons le chiffre des unités de 7^{2026}, c'est-à-dire son reste modulo 10. On a $7^2 = 49 \equiv -1\ [10]$, donc $7^4 \equiv 1\ [10]$. Comme $2026 = 4 \times 506 + 2$, on obtient

$$7^{2026} = (7^4)^{506} \times 7^2 \equiv 1^{506} \times 49 \equiv 9\ [10] :$$

le nombre 7^{2026}, qui a 1 713 chiffres, se termine par un 9.

Remarque : Dans $\mathbb{R}$, une congruence ne se multiplie pas par un réel quelconque sans changer le module, et ne se divise pas. L'erreur la plus répandue est la suivante : de $3x \equiv \frac{\pi}{2}\ [2\pi]$, on tire $x \equiv \frac{\pi}{6}\ [\frac{2\pi}{3}]$, et *non* $x \equiv \frac{\pi}{6}\ [2\pi]$. En effet, pour $k \in \mathbb{Z}$,

$$3x = \frac{\pi}{2} + 2k\pi \iff x = \frac{\pi}{6} + \frac{2k\pi}{3},$$

et l'on obtient dans $[0\,, 2\pi[$ trois solutions, $\frac{\pi}{6}$, $\frac{5\pi}{6}$ et $\frac{3\pi}{2}$, et non une seule. On évite l'erreur en revenant toujours à l'écriture avec l'entier k.

2.8 Relations d'ordre

2.8.1 Ordres totaux et partiels

Définition : Une **relation d'ordre** sur un ensemble E est une relation binaire sur E qui est **réflexive**, **antisymétrique** et **transitive**. On la note souvent $\preccurlyeq$, et l'on dit que $(E, \preccurlyeq)$ est un **ensemble ordonné**. Deux éléments x et y sont **comparables** si $x \preccurlyeq y$ ou $y \preccurlyeq x$. L'ordre est dit **total** si deux éléments quelconques de E sont toujours comparables, et **partiel** sinon.

Exemples :

- L'ordre usuel $\leqslant$ est un ordre total sur $\mathbb{R}$, donc aussi sur $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$. L'inclusion est un ordre sur $\mathcal{P}(E)$, partiel dès que E a au moins deux éléments $a \neq b$, puisque les parties $\{a\}$ et $\{b\}$ ne sont pas comparables.
- Sur $\mathbb{N}$, la relation de **divisibilité**, définie par $a \mid b \Leftrightarrow \exists k \in \mathbb{N},\ b = ka$, est un ordre partiel.
  - Elle est réflexive, car $a = 1 \cdot a$.
  - Elle est transitive : si $b = ka$ et $c = k'b$, alors $c = (k'k)\, a$.
  - Elle est antisymétrique : si $b = ka$ et $a = k'b$, alors $a = k'k\, a$. Si $a = 0$, alors $b = 0 = a$; sinon $k'k = 1$, donc $k = k' = 1$ et $a = b$.
  - Elle est partielle, car 2 et 3 ne se divisent pas l'un l'autre.

  On remarquera que, pour cet ordre, 0 est « plus grand » que tous les entiers, puisque $0 = 0 \times a$ pour tout a.
- Sur $\mathbb{R}^2$, l'**ordre lexicographique**, défini par

$$(x, y) \preccurlyeq (x', y') \iff \big(x < x' \ \text{ ou } \ (x = x' \ \text{ et } \ y \leqslant y')\big),$$

  est un ordre total : c'est l'ordre du dictionnaire, où l'on compare d'abord la première lettre, puis la deuxième en cas d'égalité. On vérifie par exemple que $(1, 5) \preccurlyeq (2, 0)$ et $(1, 0) \preccurlyeq (1, 5)$.

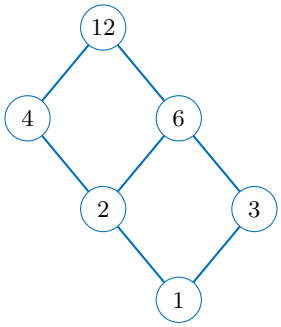
Remarque : À une relation d'ordre $\preccurlyeq$ on associe l'*ordre strict* $\prec$, défini par

$$x \prec y \iff (x \preccurlyeq y \ \text{ et } \ x \neq y).$$

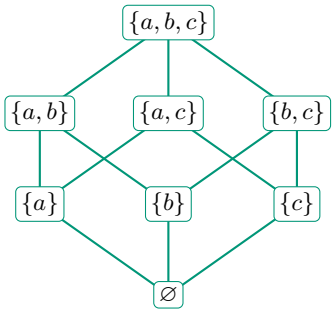
Ce n'est pas une relation d'ordre au sens précédent, puisqu'elle n'est pas réflexive, comme le montrait la ligne $<$ du tableau de la section 2.6. L'erreur la plus répandue est de croire que la négation de $x \preccurlyeq y$ est $y \prec x$: c'est vrai pour un ordre total, mais faux pour un ordre partiel, où la négation de $\{a\} \subset \{b\}$ n'entraîne pas $\{b\} \subsetneq \{a\}$.

2.8.2 Diagrammes de Hasse, plus grand élément, majorants

Un ensemble ordonné fini se représente par son **diagramme de Hasse** : on place les éléments de sorte que x soit plus bas que y lorsque $x \prec y$, et l'on relie x à y lorsque $x \prec y$ sans élément intermédiaire. Les autres comparaisons se lisent en suivant les segments vers le haut, par transitivité.



diviseurs de 12, ordonnés par |



parties de $\{a, b, c\}$, ordonnées par $\subset$

Dans le diagramme de gauche, on lit que $2 \mid 12$ en remontant de 2 à 4 puis à 12, et que 4 et 6 ne sont pas comparables : aucun chemin montant ne les relie. Dans celui de droite, les huit parties de $\{a, b, c\}$ forment un cube ; chaque segment ajoute un élément à la partie du dessous.

Définition : Soit $(E, \preccurlyeq)$ un ensemble ordonné et A une partie de E.

- Un élément $M \in E$ est un **majorant** de A si $\forall a \in A,\ a \preccurlyeq M$. On définit de même un **minorant**.
- Un élément M est le **plus grand élément** (ou **maximum**) de A si c'est un majorant de A *qui appartient à* A. On définit de même le **plus petit élément** (ou **minimum**).

Proposition 11 : Une partie A d'un ensemble ordonné possède au plus un plus grand élément. Lorsqu'il existe, on le note $\max A$.

∘ Démonstration : Si M et M' sont deux plus grands éléments de A, alors $M \preccurlyeq M'$ car M' majore A et $M \in A$, et de même $M' \preccurlyeq M$. Par antisymétrie, $M = M'$. □

Exemple : Dans $(\mathcal{P}(E), \subset)$, la partie $\{A, B\}$ a pour majorants les parties de E qui contiennent $A \cup B$, et pour plus grand élément B si $A \subset B$; si A et B ne sont pas comparables, elle n'a pas de plus grand élément, mais l'ensemble de ses majorants a un plus petit élément, $A \cup B$. De même, dans $(\mathbb{N}, |)$, les majorants de $\{4, 6\}$ sont les multiples communs de 4 et 6, c'est-à-dire les multiples de 12, et le plus petit d'entre eux est $12 = \text{ppcm}(4, 6)$, comme le chapitre 12 l'établira.

Remarque : Une partie peut n'avoir aucun plus grand élément, même lorsqu'elle est majorée : dans $(\mathbb{R}, \leqslant)$, l'intervalle $[0, 1[$ est majoré par 1, mais n'a pas de maximum, car tout $a \in [0, 1[$ est strictement inférieur à $\frac{a+1}{2}$, qui appartient aussi à $[0, 1[$. Le plus petit des majorants, s'il existe, s'appelle la *borne supérieure* ; c'est 1 dans cet exemple, et c'est $A \cup B$ et $\text{ppcm}(4, 6)$ dans les deux exemples précédents. L'existence de la borne supérieure de toute partie non vide et majorée de $\mathbb{R}$ sera l'axiome fondamental des nombres réels au chapitre 7.

2.9 Bilan

Les notions de ce chapitre se traduisent toutes par des assertions quantifiées, et les démonstrations consistent presque toujours à revenir à ces définitions. Le tableau suivant les rassemble.

Notion	Définition quantifiée	Lecture
f injective	$\forall (x, x') \in E^2,\ f(x) = f(x') \Rightarrow x = x'$	$f(x) = y$ a au plus une solution
f surjective	$\forall y \in F,\ \exists x \in E,\ y = f(x)$	$f(x) = y$ a au moins une solution
f bijective	$\forall y \in F,\ \exists! x \in E,\ y = f(x)$	existence de f^{-1}
$x \in f^{-1}(B)$	$f(x) \in B$	compatible avec $\cup$, $\cap$, complémentaire
$y \in f(A)$	$\exists x \in A,\ y = f(x)$	compatible avec $\cup$ seulement
équivalence	réflexive, symétrique, transitive	classes = partition
ordre	réflexive, antisymétrique, transitive	total ou partiel

Deux règles de composition méritent d'être retenues par cœur, car elles reviennent sans cesse : si $g \circ f$ est injective, alors f l'est, et si $g \circ f$ est surjective, alors g l'est ; et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Le chapitre 3, consacré au calcul algébrique, utilisera immédiatement les bijections pour justifier les changements d'indice dans les sommes.