Dénombrement

1. Application

Définition 1. — *Une application f est la donnée d'un ensemble de départ E (source), d'un ensemble d'arrivée F (but) et d'une règle qui assigne à tout élément x de E un et un seul élément de F, noté $f(x)$ (image de x par f).*

On veillera à distinguer les objets mathématiques f et $f(x)$ qui ont des natures différentes.

Exemple 2. — L'application « élévation au carré » est définie par :

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

Si A est une partie d'un ensemble E, l'indicatrice de A est l'application notée $\mathbf{1}_A$ définie par :

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

2. Injection, surjection, bijection

2.1. Définitions des trois notions

Définition 3. — *Soit $f\colon E \longrightarrow F$ une application.*

1. *L'application f est dite injective si :*

$$\forall\,(x_1,x_2)\in E^2 \quad f(x_1)=f(x_2)\Longrightarrow x_1=x_2$$

   i.e. si tout élément de F possède au plus un antécédent par f dans E.

2. *L'application f est dite surjective si :*

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

   i.e. si tout élément de F possède au moins un antécédent par f dans E.

3. *L'application f est bijective si et seulement si elle est injective et surjective, i.e. si :*

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

   i.e. si tout élément de F possède un et un seul antécédent par f dans E.

Étudier l'injectivité, la surjectivité, la bijectivité d'une application $f\colon E \longrightarrow F$ revient à étudier, pour tout $y\in F$, l'équation :

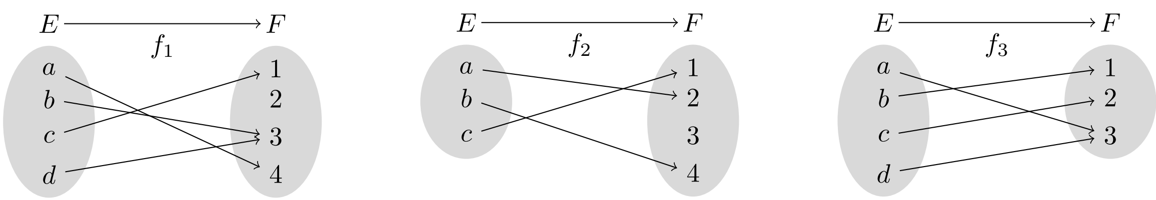
$$(\mathcal{E}_y) \qquad f(x)=y$$

d'inconnue $x\in E$.

1. L'application f est injective si et seulement si, pour tout $y\in F$, l'équation $(\mathcal{E}_y)$ possède au plus une solution.
2. L'application f est surjective si et seulement si, pour tout $y\in F$, l'équation $(\mathcal{E}_y)$ possède au moins une solution.
3. L'application f est bijective si et seulement si, pour tout $y\in F$, l'équation $(\mathcal{E}_y)$ possède une et une seule solution.

Exercice 4. — Soit $f\colon E \longrightarrow F$ une application. Écrire formellement l'assertion « l'application f n'est pas injective ».

Exercice 5. — Les applications suivantes sont-elles injectives ? surjectives ?



Les ensembles de départ et d'arrivée d'une application jouent un rôle majeur dans l'étude de son injectivité et de sa surjectivité. En effet, considérons les applications :

$$f_1 \left|\begin{array}{ccc}\mathbf{R} & \longrightarrow & \mathbf{R}\\ x & \longmapsto & x^2\end{array}\right. \qquad f_2 \left|\begin{array}{ccc}\mathbf{R}_+ & \longrightarrow & \mathbf{R}\\ x & \longmapsto & x^2\end{array}\right. \qquad f_3 \left|\begin{array}{ccc}\mathbf{R} & \longrightarrow & \mathbf{R}_+\\ x & \longmapsto & x^2\end{array}\right.$$

L'application f_1 n'est ni injective ni surjective, l'application f_2 est injective et l'application f_3 est surjective.

2.2. L'application réciproque d'une application bijective

Définition 6. — *Soit $f\colon E \longrightarrow F$ une application bijective. L'application f^{-1} définie par :*

$$f^{-1} \left|\begin{array}{ccc} F & \longrightarrow & E\\ y & \longmapsto & \text{l'unique antécédent de } y \text{ par } f \text{ dans } E\end{array}\right.$$

est appelée application réciproque de f.

Proposition 7. — *Soit $f\colon E \longrightarrow F$ une application bijective.*

1. *$f \circ f^{-1} = \mathrm{id}_F$*
2. *$f^{-1} \circ f = \mathrm{id}_E$*
3. *L'application f^{-1} est bijective.*
4. *$\left(f^{-1}\right)^{-1} = f$.*

Démonstration.

1. Soit $y \in F$. Comme $f^{-1}(y)$ est l'antécédent de y par f dans E :
$$f \circ f^{-1}(y) = f\left(f^{-1}(y)\right) = y = \mathrm{id}_F(y)$$
2. Soit $x \in E$. Comme x est l'antécédent de $f(x)$ par f dans E :
$$f^{-1} \circ f(x) = f^{-1}(f(x)) = x = \mathrm{id}_E(x)$$
3. Soient y_1 et y_2 deux éléments de F tels que $f^{-1}(y_1) = f^{-1}(y_2)$. En appliquant f à chacun des membres de l'identité précédente, il vient :
$$f\left(f^{-1}(y_1)\right) = f\left(f^{-1}(y_2)\right)$$
ce qui, avec la propriété $f \circ f^{-1} = \mathrm{id}_F$, livre $y_1 = y_2$.
L'injectivité de l'application f^{-1} est donc établie. Passons à la démonstration de sa surjectivité.
Soit $x \in E$. Grâce à la propriété $f^{-1} \circ f = \mathrm{id}_E$, nous savons :
$$f^{-1}(f(x)) = x$$
L'élément $f(x)$ est donc un antécédent de x par f^{-1} dans F.
4. En composant chacun des membres de l'identité :
$$f^{-1} \circ f = \mathrm{id}_E$$
par $\left(f^{-1}\right)^{-1}$ à gauche, nous obtenons :
$$f = \left(f^{-1}\right)^{-1}$$

□

2.3. Une étude d'injectivité et de surjectivité dans le cadre des nombres complexes

Exercice 8. — Soit l'application f définie par :

$$f \left| \begin{array}{ccc} \mathbf{C} & \longrightarrow & \mathbf{C} \\ z & \longmapsto & z^2 \end{array} \right.$$

1. Démontrer que l'application f est surjective.
2. L'application f est-elle injective ?
3. Étudier les antécédents éventuels de $z = -1 + i$ par f dans $\mathbf{C}$.
4. Étudier les antécédents éventuels de $z = 2 - 3i$ par f dans $\mathbf{C}$.

2.4. Une étude d'injectivité et de surjectivité d'une fonction réelle de la variable réelle

Exercice 9. — Soit l'application f définie par :

$$f \left| \begin{array}{ccc} \mathbf{R}_+ & \longrightarrow & [1, +\infty[\\ x & \longmapsto & \mathrm{ch}(x) \end{array} \right.$$

1. Justifier que l'application f est bien définie.
2. Énoncer le théorème de la bijection (corollaire du théorème des valeurs intermédiaires).
3. Démontrer que l'application f est bijective.
4. Un repère du plan étant fixé, tracer la courbe représentative $\mathcal{C}_f$ de l'application f, puis celle, notée $\mathcal{C}_{f^{-1}}$, de l'application f^{-1}.
5. Quel est le sens de variation de l'application f^{-1} sur $[1, +\infty[$?
6. Rappeler le résultat du cours sur la dérivabilité et la dérivée d'une application réciproque.
7. Déterminer le domaine de dérivabilité de la fonction f^{-1}, ainsi que sa fonction dérivée.
8. Expliciter, pour tout réel $y \geqslant 1$, le nombre $f^{-1}(y)$ à l'aide de fonctions usuelles.
9. Étudier la branche infinie de la courbe $\mathcal{C}_{f^{-1}}$.
10. Calculer $\displaystyle\int_2^5 \frac{1}{\sqrt{x^2-1}}\, \mathrm{d}x$.

2.5. Deux études d'injectivité et de surjectivité en algèbre linéaire

Exercice 10. — Soient a un nombre réel fixé et f l'application définie par :

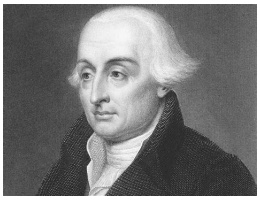
$$f \left| \begin{array}{ccc} \mathbf{R}^3 & \longrightarrow & \mathbf{R}^3 \\ (x,y,z) & \longmapsto & (x+y+2\,z, x+a\,y+z, 2\,x+y+z) \end{array} \right.$$

1. Étudier l'injectivité et la surjectivité de l'application f.
2. Expliciter l'application f^{-1}, lorsque l'application f est bijective.

Exercice 11. — Soient n un entier naturel , $a_0, a_1, \ldots, a_n$ des nombres réels et f l'application définie par :

$$f \left| \begin{array}{ccc} \mathbf{R}_n[X] & \longrightarrow & \mathbf{R}^{n+1} \\ P & \longmapsto & (P(a_0), P(a_1), \ldots, P(a_n)) \end{array} \right.$$

1. Étudier l'injectivité et la surjectivité de l'application f.
2. Expliciter l'application f^{-1}, lorsque l'application f est bijective.



Joseph-Louis Lagrange (1736-1813)

2.6. Une étude d'injectivité et de surjectivité dans le cadre des EDL

Exercice 12. — Soit l'application φ définie par :

$$\varphi \left| \begin{array}{ccc} \mathcal{C}^\infty(\mathbf{R},\mathbf{R}) & \longrightarrow & \mathcal{C}^\infty(\mathbf{R},\mathbf{R}) \\ f & \longmapsto & f' + 2\,f \end{array} \right.$$

1. Démontrer que l'application φ n'est pas injective.
2. Démontrer que l'application φ est surjective.

2.7. Stabilité de l'injectivité (resp. surjectivité, bijectivité) par composition

Proposition 13. — *Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ deux applications.*

1. *Si les applications f et g sont injectives, alors l'application $g \circ f$ est injective.*
2. *Si les applications f et g sont surjectives, alors l'application $g \circ f$ est surjective.*
3. *Si les applications f et g sont bijectives, alors l'application $g \circ f$ est bijective.*

Démonstration.

1. Supposons les applications f et g injectives et démontrons que l'application :

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

est injective. Pour cela, considérons deux éléments x_1, x_2 de E tels que $g \circ f(x_1) = g \circ f(x_2)$, i.e. tels que :

$$g(f(x_1)) = g(f(x_2))$$

Comme l'application g est injective, il vient :

$$f(x_1) = f(x_2)$$

L'injectivité de l'application f livre alors $x_1 = x_2$.

2. Supposons que les applications f et g sont surjectives et démontrons que l'application $g \circ f : E \longrightarrow G$ est surjective. Considérons un élément z de G. Comme l'application g est surjective, il existe $y \in F$ tel que :

$$z = g(y) \tag{1}$$

La surjectivité de l'application f assure l'existence d'un élément x de E tel que :

$$y = f(x) \tag{2}$$

D'après (1) et (2), $g \circ f(x) = z$.

3. Conséquence de 1 et 2.

□

Proposition 14. — *Soient $f\colon E \longrightarrow F$ et $g\colon F \longrightarrow G$ des applications bijectives. Alors :*

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

Démonstration. Nous prenons appui sur l'associativité du produit de composition.

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

En composant chacun des membres de l'identité :

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

par $(g \circ f)^{-1}$ à gauche, nous obtenons :

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

□

2.8. Injectivité et inversibilité à gauche, surjectivité et inversibilité à droite

Proposition 15. — *Soit $f\colon E \longrightarrow F$ une application.*

1. *L'application f est injective si et seulement s'il existe une application $g\colon F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$ (f est inversible à gauche).*
2. *L'application f est surjective si et seulement s'il existe une application $g\colon F \longrightarrow E$ telle que $f \circ g = \mathrm{id}_F$ (f est inversible à droite).*

Démonstration.

1 $\Longleftarrow$. Supposons qu'il existe une application $g\colon F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$. Considérons deux éléments x_1, x_2 de E tels que $f(x_1) = f(x_2)$. En appliquant g à chacun des membre de l'identité précédente, il vient $x_1 = x_2$.

1 $\Longrightarrow$. Supposons l'application f injective. Nous fixons un élément x_0 de l'ensemble E supposé non vide et considérons l'application g définie par :

$$g \left| \begin{array}{ccc} F & \longrightarrow & E \\ y & \longmapsto & \begin{cases} \text{l'unique antécédent de } y \text{ par } f \text{ dans } E & \text{si } y \in f(E) \\ x_0 & \text{sinon} \end{cases} \end{array} \right.$$

Soit $x \in E$. Comme $f(x) \in f(E)$ et x est l'unique antécédent de $f(x)$ par f dans E, nous savons que :

$$g(f(x)) = x = \mathrm{id}_E(x)$$

2 $\Longleftarrow$. Supposons qu'il existe une application $g\colon F \longrightarrow E$ telle que $f \circ g = \mathrm{id}_F$. Soit $y \in F$. Comme :

$$f(g(y)) = \mathrm{id}_F(y) = y$$

il existe un élément x de E ($x = g(y)$ convient) tel que $f(x) = y$.

2 $\Longrightarrow$. Supposons l'application f surjective. Considérons un élément $y \in G$ et choisissons un antécédent de y par f dans E, que nous notons $g(y)$. Ici, nous pouvons avoir une infinité de choix à réaliser, donc l'axiome du choix est appliqué. Nous pouvons alors considérer l'application :

$$g \left| \begin{array}{ccc} F & \longrightarrow & E \\ y & \longmapsto & \text{l'antécédent } g(y) \text{ de } y \text{ par } f \text{ dans } E \text{ préalablement choisi} \end{array} \right.$$

Soit $y \in F$. Comme $g(y)$ est un antécédent de y par f dans E :

$$f(g(y)) = y = \mathrm{id}_F(y)$$

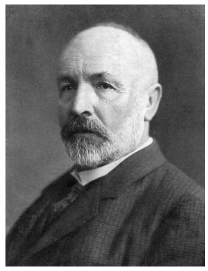
□

Exercice 16. — Soit $f\colon E \longrightarrow F$ une application injective. D'après la proposition précédente, il existe une application $g\colon F \longrightarrow E$ telle que $g \circ f = \mathrm{id}_E$. Que dire de l'application g ?

2.9. Digression : avoir le même « nombre d'éléments »

Définition 17. — *Deux ensembles E et F sont équipotents s'il existe une bijection de E vers F, ou de manière équivalente s'il existe une bijection de F vers E.*

Remarque 18. — Si deux ensembles E et F sont équipotents, alors leurs éléments sont en correspondance « un pour un », au moyen d'une bijection de E vers F. Il est donc naturel de penser que les deux ensembles E et F ont le même « nombre d'éléments », quand bien même cette notion de « nombre d'éléments » n'est pas (encore) fondée. Cette idée est due à Georg Cantor.



Georg Cantor (1845-1918)

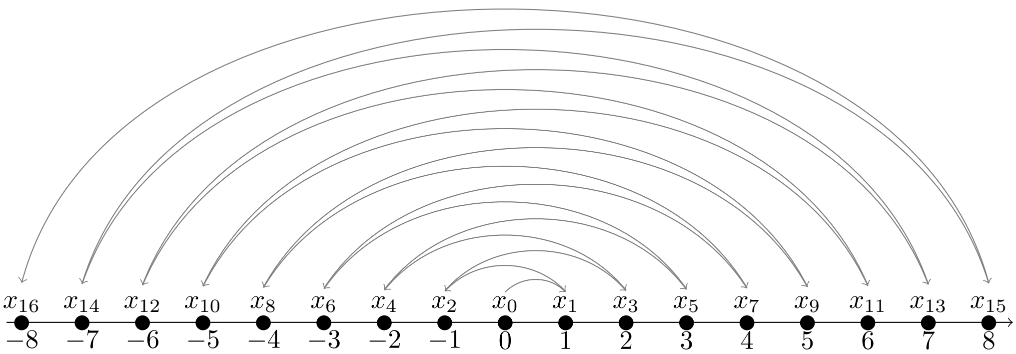
2.10. Les ensembles $\mathbf{N}$, $\mathbf{Z}$ et $\mathbf{N}^2$ sont équipotents

Exercice 19. — Démontrer que les ensembles $\mathbf{N}$ et $\mathbf{N}^*$ sont équipotents.

Proposition 20. — *Les ensembles $\mathbf{N}$ et $\mathbf{Z}$ sont équipotents.*

Éléments de démonstration.

1. Numérotation des éléments de $\mathbf{Z}$.
   On numérote les éléments de $\mathbf{Z}$ en commençant par affecter le numéro 0 à $0 \in \mathbf{Z}$, puis 1 à $1 \in \mathbf{Z}$, puis 2 à $-1 \in \mathbf{Z}$, puis 3 à $2 \in \mathbf{Z}$, puis 4 à $-2 \in \mathbf{Z}$,... en poursuivant indéfiniment ce jeu de « ping-pong ».



2. Construction de deux applications $f\colon \mathbf{N} \longrightarrow \mathbf{Z}$ et $g\colon \mathbf{Z} \longrightarrow \mathbf{N}$ à partir de la numérotation précédente.
   On remarque que l'entier relatif portant le numéro n est $-n/2$ si n est pair et $(n+1)/2$ si n est impair. On observe également qu'un élément de $n \in \mathbf{Z}$ est numéroté $-2n$ si $n<0$ et $2n-1$ si $n \geqslant 0$. C'est ainsi qu'apparaissent les applications :
   $$f \left| \begin{array}{rcl} \mathbf{N} & \longrightarrow & \mathbf{Z} \\ n & \longmapsto & \begin{cases} -n/2 & \text{si } n \text{ est pair} \\ (n+1)/2 & \text{si } n \text{ est impair} \end{cases} \end{array} \right. \qquad \text{et} \qquad g \left| \begin{array}{rcl} \mathbf{Z} & \longrightarrow & \mathbf{N} \\ n & \longmapsto & \begin{cases} -2n & \text{si } n \leqslant 0 \\ 2n-1 & \text{si } n > 0 \end{cases} \end{array} \right.$$
   qui sont bien définies.
3. Les applications f et g sont inverses l'une de l'autre.
   On vérifie que :
   - pour tout $n \in \mathbf{Z}$, $f(g(n)) = n$, en raisonnant par disjonction de cas suivant le signe de n ;
   - pour tout $n \in \mathbf{N}$, $g(f(n)) = n$ en raisonnant par disjonction de cas suivant la parité de n.

   Comme $f \circ g = \mathrm{id}_{\mathbf{Z}}$ et $g \circ f = \mathrm{id}_{\mathbf{N}}$ l'application f est bijective (il en est de même de g).

□

Lemme 21. — *Soit $x = (x_p)_{p \in \mathbf{N}}$ une suite strictement croissante d'entiers naturels. Alors :*

$$\forall\, p \in \mathbf{N} \quad x_p \geqslant p$$

Démonstration. On démontre, en raisonnant par récurrence, que, pour tout $p \in \mathbf{N}$:

$$\mathcal{P}(p) \ : \ x_p \geqslant p$$

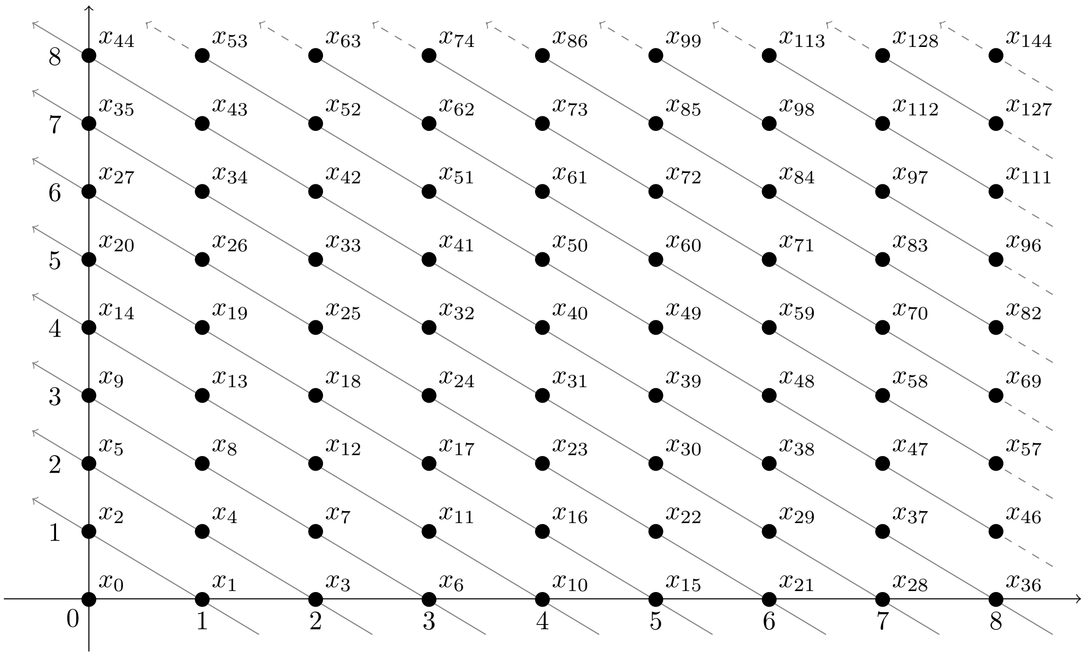
1. Initialisation à $p = 0$.
   Comme $x_0 \in N$, $x_0 \geqslant 0$. L'assertion $\mathcal{P}(0)$ est donc vraie.
2. Hérédité.
   Soit $p \in \mathbf{N}$ tel que l'assertion $\mathcal{P}(p)$ est vraie. Avec l'hypothèse de stricte croissance de la suite x, nous en déduisons que :
   $$x_{p+1} > x_p \geqslant p$$
   d'où $x_{p+1} > p$. Comme x_{p+1} et p sont de plus entiers, nous en déduisons $x_{p+1} \geqslant p + 1$.

□

Proposition 22. — *Les ensembles* $\mathbf{N}$ *et* $\mathbf{Z}^2$ *sont équipotents.*

Démonstration.

1. Principe de la numérotation.
   On numérote $(0, 0)$ à 0, puis on serpente de manière diagonale à travers le réseau dessiné par $\mathbf{N}^2$ dans le plan. Après avoir numéroté tous les éléments d'une diagonale, on reprend la numérotation sur la diagonale suivante, en partant du bas pour remonter.



2. Construction d'une application $f \colon \mathbf{Z}^2 \longrightarrow \mathbf{N}$ à partir de la numérotation précédente.
   On commence par observer que, pour tout $k \in \mathbf{N}$, $k+1$ points du réseau dessiné par $\mathbf{N}^2$ figurent sur la diagonale d'équation $y = -x + k$.
   Soit $(a, b) \in \mathbf{N}^2 \backslash \{(0, 0)\}$. Ce point appartient à la droite d'équation $y = -x+a+b$. Sur les diagonales précédentes :
   $$\sum_{k=0}^{a+b-1} (k+1) = \sum_{k=0}^{a+b} k$$
   points du réseau dessiné par $\mathbf{N}^2$ se sont déjà vus attribuer un numéro. Il faut encore en numéroter $b + 1$ sur la diagonale d'équation $y = -x + a + b$ pour atteindre (a, b). Ainsi le point (a, b) sera le $\left(b + 1 + \sum_{k=0}^{a+b} k\right)$-ième point du réseau dessiné par $\mathbf{N}^2$ recevant un numéro. Comme la numérotation débute à 0, il recevra le numéro $b + \sum_{k=0}^{a+b} k$.
   C'est ainsi qu'apparaît l'application :
   $$f \left| \begin{array}{ccc} \mathbf{Z}^2 & \longrightarrow & \mathbf{N} \\ (a, b) & \longmapsto & b + \displaystyle\sum_{k=0}^{a+b} k = b + \frac{(a+b)(a+b+1)}{2}. \end{array} \right.$$

3. Une suite d'entiers auxiliaire.
La suite :
$$\left(S_p = \sum_{k=0}^{p} k = \frac{p(p+1)}{2} \right)_{p \in \mathbf{N}}$$
est une suite strictement croissante d'entiers naturels. D'après le lemme précédent :
$$\forall\, p \in \mathbf{N} \quad S_p \geqslant p \tag{3}$$

4. Surjectivité de l'application f.
Soit $n \in \mathbf{N}$. D'après (3) :
$$A := \{p \in \mathbf{N} \ : \ S_p \leqslant n\} \subset [\![0, n]\!]$$
est fini. Comme A est de plus non vide ($0 \in A$), l'entier naturel :
$$p_0 := \max(A)$$
est bien défini. D'après la définition de p_0 :
$$S_{p_0} \leqslant n \leqslant S_{p_0+1} - 1 = S_{p_0} + p_0 \tag{4}$$
Nous définissons deux entiers relatifs a et b par :
$$b = n - S_{p_0} \qquad \text{et} \qquad a = p_0 - b = S_{p_0} + p_0 - n$$
D'après (4), $a \geqslant 0$ et $b \geqslant 0$, donc a et b sont des entiers naturels. Nous vérifions enfin que :
$$f(a, b) = S_{a+b} + b = S_{p_0} + n - S_{p_0} = n$$

5. Injectivité de l'application f.
Soient $(a_1, b_1) \in \mathbf{Z}^2$ et $(a_2, b_2) \in \mathbf{Z}^2$ tels que :
$$b_1 + S_{a_1+b_1} = f(a_1, b_1) = f(a_2, b_2) = b_2 + S_{a_2+b_2}. \tag{5}$$
Quitte à échanger les rôles de (a_1, b_1) et (a_2, b_2), nous pouvons supposer que $a_1 + b_1 \leqslant a_2 + b_2$. Alors :
$$S_{a_1+b_1} \leqslant S_{a_2+b_2} \leqslant S_{a_2+b_2} + b_2 = S_{a_1+b_1} + b_1 < S_{a_1+b_1+1}$$
Comme la suite $(S_p)_{p \in \mathbf{N}}$ est strictement croissante, de $S_{a_1+b_1} \leqslant S_{a_2+b_2} < S_{a_1+b_1+1}$, nous déduisons :
$$a_1 + b_1 = a_2 + b_2$$
Avec l'hypothèse (5), il vient $b_1 = b_2$. Les couples (a_1, b_1) et (a_2, b_2) sont donc égaux.

□

2.11. Théorème de Cantor

Théorème 23. — *Il n'existe aucune surjection entre un ensemble E et son ensemble de parties $\mathcal{P}(E)$.*

Démonstration. Soit E un ensemble. Supposons qu'il existe une application $f \colon E \longrightarrow \mathcal{P}(E)$ surjective et considérons la partie A de E définie par :
$$A = \{x \in E \ : \ x \notin f(x)\}$$
Comme f est surjective, il existe un élément a de E tel que $A = f(a)$.

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

Dans tous les cas, nous aboutissons à une contradiction. □

Remarque 24. — Les ensembles $\mathbf{N}$ et $\mathcal{P}(\mathbf{N})$ ne sont donc pas équipotents. Nous en déduirons, plus tard, que les ensembles $\mathbf{N}$ et $\mathbf{R}$ ne sont pas équipotents.

3. Ensembles finis

3.1. Définitions d'un ensemble fini et du cardinal d'un tel

Théorème 25. — *Soient n et m deux entiers naturels non nuls.*

1. *S'il existe une application injective $f\colon [\![1,n]\!] \longrightarrow [\![1,m]\!]$, alors $n \leqslant m$.*
2. *S'il existe une application surjective $f\colon [\![1,n]\!] \longrightarrow [\![1,m]\!]$, alors $n \geqslant m$.*
3. *S'il existe une application bijective $f\colon [\![1,n]\!] \longrightarrow [\![1,m]\!]$, alors $n = m$.*

Démonstration.

1. On démontre par récurrence que, pour tout $n \in \mathbf{N}^*$:
$$\mathcal{P}(n) \quad : \quad « \ \forall m \in \mathbf{N}^*,\ (\exists\, f\colon [\![1,n]\!] \longrightarrow [\![1,m]\!] \text{ injective}) \Longrightarrow n \leqslant m \ »$$
est vrai.
   (a) Initialisation à $n = 1$. Clair.
   (b) Hérédité. Soit $n \in \mathbf{N}^*$ tel que $\mathcal{P}(n)$ est vraie. Soient $m \in \mathbf{N}^*$ et $f\colon [\![1,n+1]\!] \longrightarrow [\![1,m]\!]$ injective.
      - L'entier naturel non nul m n'est pas égal à 1. En effet, si $m = 1$ alors $f(1) = f(n+1) = 1$, ce qui, comme $1 \neq n+1$, contredit l'injectivité de f. Ainsi $m - 1 \geqslant 1$.
      - Supposons que $f(n+1) = m$. Alors l'application :
$$\overline{f} \left| \begin{array}{ccc} [\![1,n]\!] & \longrightarrow & [\![1,m-1]\!] \\ x & \longmapsto & f(x) \end{array} \right.$$
est bien définie et est injective, comme restriction et corestriction de l'application injective f. D'après $\mathcal{P}(n)$, $n \leqslant m-1$ et donc $n+1 \leqslant m$.
      - Supposons que $f(n+1) \neq m$. Considérons la transposition $\tau_{f(n+1),m}\colon [\![1,m]\!] \longrightarrow [\![1,m]\!]$ qui envoie $f(n+1)$ sur m, m sur $f(n+1)$ et qui fixe tous les autres éléments de $[\![1,m]\!]$. On observe que l'application $g := \tau_{f(n+1),m} \circ f\colon [\![1,n+1]\!] \longrightarrow [\![1,m]\!]$ est injective (composée d'applications injectives) et vérifie $g(n+1) = m$. On est alors ramené au cas précédent, d'où $n+1 \leqslant m$.
2. S'il existe une surjection de $[\![1,n]\!]$ vers $[\![1,m]\!]$, alors il existe une injection de $[\![1,m]\!]$ dans $[\![1,n]\!]$. Le résultat se déduit donc de 1.
3. Conséquence de 1 et 2.

□

Définition 26. — *Un ensemble E est fini s'il vérifie l'une des deux conditions suivantes.*

1. *$E = \varnothing$*
2. *Il existe $n \in \mathbf{N}^*$ et une bijection $f\colon [\![1,n]\!] \longrightarrow E$.*

Définition 27. — *Soit E un ensemble fini. Le cardinal de E est le nombre entier noté $|E|$ ou $\mathrm{Card}(E)$ ou $\#E$ défini par :*
$$|E| := \begin{cases} 0 & \textit{si } E = \varnothing \\ n & \textit{s'il existe un entier } n \in \mathbf{N}^* \textit{ et une bijection } f\colon [\![1,n]\!] \longrightarrow E. \end{cases}$$

Remarque 28. — D'après le théorème 25, le cardinal d'un ensemble fini non vide est bien défini.

Exemple 29. — Si $n \in \mathbf{N}^*$, alors $[\![1,n]\!]$ est fini et $|[\![1,n]\!]| = 1$. En effet, l'application $\mathrm{id}_{[\![1,n]\!]}\colon [\![1,n]\!] \longrightarrow [\![1,n]\!]$ est bijective.

Exemple 30. — Si E est un singleton alors E est fini et $|E| = 1$. En effet, si a désigne l'unique élément de E alors l'application :
$$\left| \begin{array}{ccc} [\![1,1]\!] = \{1\} & \longrightarrow & E \\ 1 & \longmapsto & a \end{array} \right.$$
est bijective.

Proposition 31. — *Soit E un ensemble fini non vide et $\varphi\colon E \longrightarrow F$ une application bijective de E vers un autre ensemble F. Alors F est fini et $|F| = |E|$.*

Démonstration. Comme E est un ensemble fini non vide, il existe un entier $n \in \mathbf{N}^*$ et une application bijective $f\colon [\![1,n]\!] \longrightarrow E$. L'application $\varphi \circ f\colon [\![1,n]\!] \longrightarrow F$ est bijective (composée d'applications bijectives). Ainsi F est fini et $|F| = n = |E|$. □

Exercice 32. — Soient a et b des entiers relatifs tels que $a \leqslant b$. Démontrer que l'ensemble $[\![a,b]\!]$ est fini que :

$$\operatorname{card}\left([\![a,b]\!]\right) = b - a + 1.$$

3.2. Parties d'un ensemble fini

Théorème 33. — *Soient $n \in \mathbf{N}^*$ et A une partie de $[\![1,n]\!]$.*

1. *Si $A \neq [\![1,n]\!]$ alors l'ensemble A est fini et $|A| < n$.*
2. *Toutes les parties de $[\![1,n]\!]$ sont finies et leurs cardinaux sont inférieurs ou égaux à n.*
3. *Si $|A| = n$, alors $A = [\![1,n]\!]$.*

Démonstration.

1. On démontre par récurrence sur l'entier $n \in \mathbf{N}^*$ que le prédicat :

$$\mathcal{P}(n) \quad : \text{ « } \forall A \in \mathcal{P}([\![1,n]\!]) \quad A \subsetneq [\![1,n]\!] \implies A \text{ est finie et } |A| < n \text{ »}$$

   est vrai.

   (a) Initialisation à $n = 1$. L'ensemble vide est la seule partie de $[\![1,1]\!] = \{1\}$ distincte de $\{1\}$. Comme $\varnothing$ est fini de cardinal $0 < 1$, l'assertion $\mathcal{P}(1)$ établie.

   (b) Hérédité. Soit $n \in \mathbf{N}^*$ tel que $\mathcal{P}(n)$ est vraie. Ceci implique que toute partie X de $[\![1,n]\!]$ est finie de cardinal $|X| \leqslant n$. En effet, si $X \neq [\![1,n]\!]$ il s'agit d'une conséquence de $\mathcal{P}(n)$. Sinon $X = [\![1,n]\!]$ et le résultat découle de l'exemple 29.
   Soit A une partie de $[\![1,n+1]\!]$ dictincte de $[\![1,n+1]\!]$.

   - Si $A = \varnothing$ alors A est fini et $|A| = 0 < n+1$.
   - Supposons désormais que A est non vide.
     — Si $n+1 \notin A$, alors A est une partie de $[\![1,n]\!]$. Donc A est fini et $|A| \leqslant n < n+1$.
     — Supposons à présent que $n+1 \in A$. Comme $A \neq [\![1,n+1]\!]$, il existe $a \in [\![1,n]\!]$ tel que $a \notin A$. Introduisons la partie :

$$B := (A \setminus \{n+1\}) \sqcup \{a\}$$

     de $[\![1,n]\!]$. Ainsi B est finie et $|B| \leqslant n$. Les applications :

$$f \left| \begin{array}{ccc} B & \longrightarrow & A \\ x & \longmapsto & \begin{cases} x & \text{si } x \neq a \\ n+1 & \text{si } x = a \end{cases} \end{array} \right. \qquad \text{et} \qquad g \left| \begin{array}{ccc} A & \longrightarrow & B \\ y & \longmapsto & \begin{cases} y & \text{si } y \neq n+1 \\ a & \text{si } y = n+1 \end{cases} \end{array} \right.$$

     sont bien définies. On vérifie $f \circ g = \mathrm{id}_A$ et $g \circ f = \mathrm{id}_B$. L'application f est donc bijective. D'après la proposition 31, A est fini et $|A| = |B| \leqslant n < n+1$.

2. Si $A \neq [\![1,n]\!]$ alors, d'après 1, A est fini et $|A| < n$. Si $A = [\![1,n]\!]$ alors, d'après l'exemple 29, A est fini et $|A| = n$.
3. Conséquence de la disjonction de cas opérée pour la démonstration de 2.

□

Corollaire 34. — *Soit E une ensemble fini de cardinal $n \in \mathbf{N}^*$. Soit A une partie de E.*

1. *Si $A \neq E$ alors l'ensemble A est fini et $|A| < n$.*
2. *Toutes les parties de E sont finies et leurs cardinaux sont inférieurs ou égaux à n.*
3. *Si $|A| = n$, alors $A = E$.*

Démonstration.

0. Par hypothèse, il existe une bijection $f\colon E \longrightarrow [\![1,n]\!]$. Si A est une partie de E, alors l'application :
$$f_{|A}^{|f(A)} \left| \begin{array}{ccc} A & \longrightarrow & f(A) \\ a & \longmapsto & f(a) \end{array} \right.$$
est une bijection de A vers la partie :
$$f(A) := \{f(a) \ : \ a \in A\}$$
de $[\![1,n]\!]$. De plus $A = E$ si et seulement si $f(A) = [\![1,n]\!]$.
1. Supposons que $A \neq E$. Alors $f(A) \neq [\![1,n]\!]$. D'après le théorème 33, l'ensemble $f(A)$ est fini et $|f(A)| < n$. D'après la proposition 31, l'ensemble A est fini et $|A| < n$ (A et $f(A)$ sont équipotents *via* $f_{|A}^{|f(A)}$).
2. Si $A \neq E$ alors, d'après 1, A est fini et $|A| < n$. Si $A = E$ alors A est fini et $|A| = n$ (E est équipotent à $[\![1,n]\!]$).
3. Conséquence de la disjonction de cas opérée pour la démonstration de 2.

□

3.3. Réunion disjointe d'ensembles finis

Théorème 35. — *Soient A et B deux parties finies disjointes d'un ensemble fini E. L'ensemble $A \sqcup B$ est fini et :*
$$|A \sqcup B| = |A| + |B|$$

Démonstration. Si $A = \varnothing$, alors $A \sqcup B = B$ et l'assertion est claire puisque $|A| = 0$. Par symétrie des rôles joués par A et B, l'assertion est vraie dans le cas où $B = \varnothing$.
Supposons désormais que A et B sont non vides. Comme A et B sont finies et non vides, il existe $(a,b) \in \mathbf{N}^* \times \mathbf{N}^*$ et deux applications bijectives : $f\colon [\![1,a]\!] \longrightarrow A$ et $g\colon [\![1,b]\!] \longrightarrow B$. L'application :
$$h \left| \begin{array}{ccc} [\![1,a+b]\!] & \longrightarrow & A \sqcup B \\ n & \longmapsto & \begin{cases} f(n) & \text{si } n \leqslant a \\ g(n-a) & \text{si } n \geqslant a+1 \end{cases} \end{array} \right.$$
est bien définie.

- Soit $(n_1, n_2) \in [\![1,a+b]\!]^2$ tel que $h(n_1) = h(n_2) \in A \sqcup B$.
  - Supposons $h(n_1) = h(n_2) \in A$. Alors comme $A \cap B = \varnothing$, $n_1 \leqslant a$ et $n_2 \leqslant a$ et donc $h(n_1) = f(n_1)$ et $h(n_2) = f(n_2)$. Comme f est injective, $n_1 = n_2$.
  - Supposons $h(n_1) = h(n_2) \in B$ Alors comme $A \cap B = \varnothing$, $n_1 \geqslant a+1$ et $n_2 \geqslant a+1$ et donc $h(n_1) = g(n_1 - a)$ et $h(n_2) = g(n_2 - a)$. Comme g est injective, $n_1 - a = n_2 - a$ et donc $n_1 = n_2$.

  L'application h est injective.
- Soit $y \in A \sqcup B$.
  - Si $y \in A$, alors $f^{-1}(y) \in [\![1,a]\!]$ et donc $h\left(f^{-1}(y)\right) = f\left(f^{-1}(y)\right) = y$.
  - Si $y \in B$, alors $g^{-1}(y) \in [\![1,b]\!]$ et donc $a + g^{-1}(y) \in [\![a+1, a+b]\!]$. Ainsi $h\left(a + g^{-1}(y)\right) = g\left(g^{-1}(y)\right) = y$.

  L'application h est surjective.

Comme l'application h est bijective, la proposition 31 livre la finitude de l'ensemble $A \sqcup B$ et $|A \cup B| = a+b = |A|+|B|$.

□

Corollaire 36. — *Soient un entier $p \geqslant 2$ et $A_1, A_2, \dots, A_p$ des parties deux à deux disjointes d'un ensemble fini E. L'ensemble $\bigsqcup_{k=1}^{p} A_k$ est fini et :*
$$\left| \bigsqcup_{k=1}^{p} A_k \right| = \sum_{k=1}^{p} |A_k|$$

Éléments de démonstration. On démontre le résultat par récurrence sur l'entier $p \geqslant 2$.

- L'initialisation découle du théorème 35.
- Pour établir l'hérédité, on remarque que si $A_1, \dots, A_p, A_{p+1}$ sont des parties deux à deux disjointes de A alors :
$$\bigsqcup_{k=1}^{p+1} A_k = \left(\bigsqcup_{k=1}^{p} A_k \right) \ \sqcup \ A_{p+1}$$

□

Exercice 37. — Soit A et B deux parties d'un ensemble fini E. Justifier que :
$$|A| + |B| > |E| \quad \Longrightarrow \quad A \cap B \neq \emptyset. \qquad \text{[principe des tiroirs]}$$

3.4. Réunion d'ensembles finis

Proposition 38. — *réunion de deux ensembles finis Soient A et B deux parties finies d'un ensemble fini E. L'ensemble $A \cup B$ est fini et :*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Démonstration. L'ensemble $A \cup B$ est fini, comme partie de l'ensemble fini E (corollaire 34). On décompose les ensembles A, B et $A \cup B$ en réunions disjointes comme suit.

i. $A = (A \cap B) \sqcup (A \setminus A \cap B)$
ii. $B = (A \cap B) \sqcup (B \setminus A \cap B)$
iii. $A \cup B = (A \setminus A \cap B) \sqcup (A \cap B) \sqcup (B \setminus A \cap B)$

D'après le corollaire 36 :

$$|A| \underset{\text{(i)}}{=} |A \cap B| + |A \setminus A \cap B| \qquad |B| \underset{\text{(ii)}}{=} |A \cap B| + |B \setminus A \cap B| \qquad |A \cup B| \underset{\text{(iii)}}{=} |A \setminus A \cap B| + |A \cap B| + |B \setminus A \cap B| \ .$$

En combinant ces trois identités, on obtient celle de la proposition. □

Exercice 39. — Soient $p \geqslant 2$ et $A_1, A_2, \ldots, A_p$ des parties finies d'un ensemble fini E. Démontrer que :

$$\left| \bigcup_{k=1}^{p} A_k \right| = \sum_{k=1}^{p} (-1)^{p+1} \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$$

Il s'agit de la formule du crible aussi, appelée formule de Poincaré.

Henri Poincaré (1854-1912)

3.5. Théorème de Lagrange sur les sous-groupes d'un groupe fini

Exercice 40. — Soit $(G, *)$ un groupe fini et H un sous-groupe de G. Pour tout $g \in G$, on pose

$$g * H := \{g * h \ : \ h \in H\}$$

1. Justifier que la relation $\sim$ sur G définie par

$$\forall (g_1, g_2) \in G \quad g_1 \sim g_2 :\Longleftrightarrow g_1 * H = g_2 * H$$

   est une relation d'équivalence.
2. Soit $g \in G$. Déterminer la classe d'équivalence $\overline{g}$ de g pour la relation $\sim$ définie par

$$\overline{g} := \{g' \in G \ : \ g' \sim g\} \subset G$$

3. Soit $(g_1, g_2) \in G^2$. Démontrer que les ensembles $g_1 * H$ et $g_2 * H$ sont équipotents.
4. Soit $G/\sim$ l'ensemble des classes d'équivalences de $\sim$ défini par :

$$G/\sim := \ \{\overline{g} \ : \ g \in G\}$$

   Justifier que $G/\sim$ est un ensemble fini.
5. En déduire que $|H|$ divise $|G|$ (théorème de Lagrange).
6. Que dire des sous-groupes d'un groupe fini de cardinal un nombre premier ?

3.6. Produit cartésien d'ensembles finis

Proposition 41. — *Soient E_1, E_2 deux ensembles finis non vides. L'ensemble $E_1 \times E_2$ est fini et*

$$|E_1 \times E_2| = |E_1| \times |E_2|$$

Éléments de démonstration. Posons $n_1 := |E_1| \in \mathbf{N}^*$ et $n_2 := |E_2| \in \mathbf{N}^*$.
Par hypothèse, il existe des bijections $f_1 \colon [\![0, n_1 - 1]\!] \longrightarrow E_1$ et $f_2 \colon [\![0, n_2 - 1]\!] \longrightarrow E_2$.
Pour tout $x \in [\![0, n_1 n_2 - 1]\!]$, il existe un unique couple $(q(x), r(x)) \in [\![0, n_2 - 1]\!] \times [\![0, n_1 - 1]\!]$ tel que :

$$x = q(x)\, n_1 + r(x) \qquad \text{[division euclidienne de } x \text{ par } n_1]$$

L'application :

$$f \left| \begin{array}{ccc} [\![0, n_1 n_2 - 1]\!] & \longrightarrow & E_1 \times E_2 \\ x & \longmapsto & (f_1(r(x)), f_2((q(x))) \end{array} \right.$$

est bien définie. On vérifie qu'elle est bijective. □

Proposition 42. — *cardinal du produit cartésien de p ensembles finis Soient $p \in \mathbf{N}_{\geqslant 2}$ et $E_1, \ldots, E_p$ des ensembles finis non vides. L'ensemble $\prod_{i=1}^{p} E_i$ est fini et :*

$$\left| \prod_{i=1}^{p} E_i \right| = \prod_{i=1}^{p} |E_i| \, .$$

Éléments de démonstration. On démontre le résultat par récurrence sur l'entier $p \geqslant 2$.

- L'initialisation découle de la proposition 41.
- Pour établir l'hérédité, on remarque que si $E_1, \ldots, E_p, E_{p+1}$ sont des ensembles finis non vides, alors l'application :

$$\left| \begin{array}{ccc} \prod_{i=1}^{p+1} E_i & \longrightarrow & \left(\prod_{i=1}^{p} E_i \right) \times E_{p+1} \\ (x_1, \ldots, x_p, x_{p+1}) & \longmapsto & ((x_1, \ldots, x_p), x_{p+1}) \end{array} \right.$$

□

3.7. Ensemble des applications entre deux ensembles finis

Proposition 43. — *Soient E et F des ensembles finis non vides. Alors l'ensemble F^E des applications de E vers F est fini et :*

$$\left| F^E \right| = |F|^{|E|} \, .$$

Éléments de démonstration. Par hypothèse, il existe $n \in \mathbf{N}^*$ et une bijection $\varphi \colon [\![1, n]\!] \longrightarrow E$.

1. L'application :

$$\left| \begin{array}{ccc} F^{[\![1,n]\!]} & \longrightarrow & F^n \\ f & \longmapsto & (f(1), \ldots, f(n)) \end{array} \right.$$

   est bijective. D'après les propositions 31 et 36, l'ensemble $F^{[\![1,n]\!]}$ est fini et $\left| F^{[\![1,n]\!]} \right| = |F^n| = |F|^n = |F|^{|E|}$.
2. On vérifie que l'application :

$$\left| \begin{array}{ccc} F^E & \longrightarrow & F^{[\![1,n]\!]} \\ f & \longmapsto & f \circ \varphi \end{array} \right.$$

   est bijective. On conclut alors avec la proposition 31 et le point 1.

□

3.8. Critère de bijectivité pour une application entre deux ensembles finis

Théorème 44. — *Soient E, F deux ensemble finis non vides. et une application $f\colon E \longrightarrow F$. Si $|E| = |F|$ alors les trois assertions suivantes sont équivalentes.*

(a) f est bijective.

(b) f est injective.

(c) f est surjective.

Démonstration.

1 (a) $\Longrightarrow$ (b) et (c). Clair.

2 (b) $\Longrightarrow$ (a). Supposons l'application f injective. Alors l'application :

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

est bijective. D'après la proposition 31, $|f(E)| = |E| = |F|$. La partie $f(E)$ de F est finie, de même cardinal que F. D'après le corollaire 34, $f(E) = F$, i.e. f est surjective.

3 (c) $\Longrightarrow$ (a). Supposons l'application f surjective. Alors, il existe une application $g\colon F \longrightarrow E$ telle que $f \circ g = \mathrm{id}_F$. L'application g est injective et, d'après le point précédent, elle est bijective. De $f \circ g = \mathrm{id}_F$, on déduit alors que $f = g^{-1}$ est bijective.

$\square$

3.9. Ensemble des applications injectives entre deux ensembles finis et p-listes sans répétition

Notation. — Si E et F sont des ensembles non vides, alors on pose :

$$\mathrm{Inj}(E, F) := \left\{ f \in F^E \ : \ f \text{ est injective} \right\}.$$

Théorème 45. — *Soient E et F des ensembles finis non vides, de cardinaux respectifs n et m. L'ensemble* $\mathrm{Inj}(E, F)$ *est fini et :*

$$|\mathrm{Inj}(E, F)| = \begin{cases} 0 & \text{si } n > m \\ \dfrac{m!}{(m-n)!} & \text{si } n \leqslant m \end{cases}$$

Démonstration.

1. Comme $\mathrm{Inj}(E, F) \subset F^E$, les propositions 34 et 45 livrent la finitude de l'ensemble $\mathrm{Inj}(E, F)$.
2. Supposons qu'il existe une application $f\colon E \longrightarrow F$ injective. Alors l'application :

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

est bijective. D'après les propositions 31 et 34 :

$$n = |E| = |f(E)| \leqslant |F| = m$$

Ainsi, si $n > m$ alors $\mathrm{Inj}(E, F) = \varnothing$ et $|\mathrm{Inj}(E, F)| = 0$.

3. Nous démontrons que, pour tout $n \in \mathbf{N}^*$, le prédicat noté $\mathcal{P}(n)$:

« pour tout ensemble fini E de cardinal n, pour tout ensemble fini F de cardinal $m \geqslant n$, $|\mathrm{Inj}(E, F)| = \dfrac{m!}{(m-n)!}$ »

est vrai.

- Initialisation à $n = 1$. Soit E un ensemble fini de cardinal 1 et F un ensemble fini de cardinal $m \geqslant 1$. Comme E est un singleton, $\mathrm{Inj}(E, F) = F^E$, d'où :

$$|\mathrm{Inj}(E, F)| = \left|F^E\right| = |F|^{|E|} = m = \frac{m!}{(m-1)!}$$

- Soit $n \in \mathbf{N}^*$ tel que $\mathcal{P}(n)$ est vrai. Soit E un ensemble fini de cardinal $n+1$ et F un ensemble fini de cardinal $m \geqslant n+1$. Fixons un élement x_0 de E. L'application :

$$\left| \begin{array}{ccc} \operatorname{Inj}(E,F) & \longrightarrow & \displaystyle\bigsqcup_{y \in F} \operatorname{Inj}(E \setminus \{x_0\}, F \setminus \{y\}) \\ f & \longmapsto & f_{|\, E\setminus\{x_0\}}^{|\, F\setminus\{f(x_0)\}} \end{array} \right.$$

est bien définie et bijective. Nous en déduisons que :

$$|\operatorname{Inj}(E,F)| = \sum_{y \in F} |\operatorname{Inj}(E \setminus \{x_0\}, F \setminus \{y\})|$$

Grâce à $\mathcal{P}(n)$, cette identité se réécrit :

$$|\operatorname{Inj}(E,F)| = \sum_{y \in F} \frac{(m-1)!}{(m-1-n))!} = m \times \frac{(m-1)!}{(m-(n+1))!} = \frac{m!}{(m-(n+1))!}$$

□

Définition 46. — *Soient E un ensemble non vide et $p \in \mathbf{N}^*$. Une p-liste sans répétition d'éléments de E, aussi appelé un arrangement de p éléments de E, est un p-uplet $(x_1, \ldots, x_p)$ d'éléments de E tels que $x_1, \ldots, x_p$ sont deux à deux distincts.*

Une p-liste sans répétition d'éléments de E est ordonnée.

Notation. — Si E un ensemble non vide et $p \in \mathbf{N}^*$, l'ensemble des p-listes sans répétition d'éléments de E est noté $\mathcal{A}_p(E)$, i.e. :

$$\mathcal{A}_p(E) := \{(x_1, \ldots, x_p) \in E^p \ : \ x_1, \ldots, x_p \text{ sont deux à deux distincts}\}$$

Corollaire 47. — *Soient E un ensemble fini de cardinal $n \in \mathbf{N}^*$ et $p \leqslant n$. L'ensemble $\mathcal{A}_p(E)$ est fini et :*

$$|\mathcal{A}_p(E)| = \underbrace{n}_{\substack{\text{nombre de} \\ \text{choix du 1}^{\text{er}}}} \times \underbrace{n}_{\substack{\text{nombre de} \\ \text{choix du 2}^{\text{ème}}}} \times \ldots \times \underbrace{(n-p+1)}_{\substack{\text{nombre de} \\ \text{choix du p}^{\text{ème}}}} = \frac{n!}{(n-p)!}$$

Démonstration. Comme l'application :

$$\left| \begin{array}{ccc} \operatorname{Inj}([\![1,p]\!], E) & \longrightarrow & \mathcal{A}_p(E) \\ f & \longmapsto & (f(1), \ldots, f(p)) \end{array} \right.$$

est bijective, le résultat est conséquence du théorème 45. □

3.10. Permutations d'un ensemble fini

Définition 48. — *Soit E un ensemble non vide. Une permutation de E est une application $f\colon E \longrightarrow E$ qui est bijective.*

Notation. — Si E est un ensemble non vide, alors l'ensemble des permutations de E est noté $\mathfrak{S}(E)$, i.e. :

$$\mathfrak{S}(E) := \left\{ f \in E^E \ : \ f \text{ est bijective} \right\}$$

Proposition 49. — *Soit E un ensemble fini non vide. L'ensemble $\mathfrak{S}(E)$ est fini et :*

$$|\mathfrak{S}(E)| = |E|\,!$$

Démonstration. D'après le théorème 44, $\mathfrak{S}(E) = \operatorname{Inj}(E,E)$. Le résultat découle alors du théorème 45. □

3.11. Ensemble des parties à p-élements d'un ensemble fini ou p-combinaisons

Définition 50. — *Soient E un ensemble et $p \in \mathbf{N}^*$. Une p-combinaison de E est une partie de E à p éléments.*

Une p-combinaison de E n'est pas ordonnée.

Notation. — Si E un ensemble et $p \in \mathbf{N}^*$, l'ensemble des p-combinaisons de E est noté $\mathcal{P}_k(E)$, i.e. :

$$\mathcal{P}_k(E) := \{A \in \mathcal{P}(E) \ : \ |A| = p\}$$

où $\mathcal{P}(E)$ désigne l'ensemble des parties de E.

Remarque 51. — Si E est un ensemble fini, alors :

$$\mathcal{P}(E) = \bigsqcup_{p=0}^{|E|} \mathcal{P}_p(E).$$

Proposition 52. — *Soit E un ensemble fini de cardinal n. Pour tout $p \in [\![0, n]\!]$, l'ensemble $\mathcal{P}_p(E)$ est fini et :*

$$|\mathcal{P}_p(E)| = \binom{n}{p}.$$

Démonstration.

1. D'après le théorème 34, pour tout $p > n$, $\mathcal{P}_p(E) = \emptyset$, donc :
$$|\mathcal{P}_p(E)| = 0 = \binom{n}{p}$$
2. On démontre par récurrence sur l'entier $n \in \mathbf{N}$ que le prédicat
$$\mathcal{P}(n) \ : \ \text{« Pour tout ensemble } E \text{ de cardinal } n, \text{ pour tout } p \in [\![0, n]\!], \text{ l'ensemble } \mathcal{P}_p(E) \text{ est fini et } |\mathcal{P}_p(E)| = \binom{n}{p}. \text{ »}$$
est vrai.
   - Initialisation à $n = 0$. Comme $\mathcal{P}(\varnothing) = \{\varnothing\}$, pour tout $p \in \mathbf{N}$:
$$\mathcal{P}_p(\varnothing) = \begin{cases} \{\varnothing\} & \text{si } p = 0 \\ \varnothing & \text{si } p \geqslant 1 \end{cases}$$
donc $|\mathcal{P}_p(\varnothing)| = \binom{0}{p}$.
   - Hérédité. Soit $n \in \mathbf{N}$ tel que l'assertion $\mathcal{P}(n)$ est vraie. Soit E un ensemble de cardinal $n + 1$.
     — L'ensemble E possède une unique partie à 0 élément, l'ensemble vide. Ainsi $\mathcal{P}_0(E) = \{\varnothing\}$ est fini, de cardinal $1 = \binom{n+1}{0}$.
     — L'ensemble E est de cardinal $n + 1 \geqslant 1$, donc non vide. Soient x_0 un élement de E fixé et $p \in [\![1, n]\!]$.
       (i) Si on pose :
$$\mathcal{P}_p^{x_0}(E) := \{A \in \mathcal{P}_p(E) \ : \ x_0 \in A\} \quad \text{et} \quad \mathcal{P}_p^{\overline{x_0}}(E) := \{A \in \mathcal{P}_p(E) \ : \ x_0 \notin A\}$$
alors l'ensemble $\mathcal{P}_p(E)$ se décompose en $\mathcal{P}_p(E) = \mathcal{P}_p^{x_0}(E) \ \sqcup \ \mathcal{P}_p^{\overline{x_0}}(E)$.
       (ii) Les applications :
$$f \left| \begin{array}{ccc} \mathcal{P}_p^{x_0}(E) & \longrightarrow & \mathcal{P}_{p-1}(E \setminus \{x_0\}) \\ A & \longmapsto & A \setminus \{x_0\} \end{array} \right. \qquad \text{et} \qquad g \left| \begin{array}{ccc} \mathcal{P}_{p-1}(E \setminus \{x_0\}) & \longrightarrow & \mathcal{P}_p^{x_0}(E) \\ B & \longmapsto & B \sqcup \{x_0\} \end{array} \right.$$
sont bien définies et vérifient $f \circ g = \mathrm{id}_{\mathcal{P}_{p-1}(E \setminus \{x_0\})}$ et $g \circ f = \mathrm{id}_{\mathcal{P}_p^{x_0}(E)}$. L'application g est donc bijective. Comme $E \setminus \{x_0\}$ est fini de cardinal n et $0 \leqslant p - 1 \leqslant n$, l'hypothèse de récurrence livre la finitude de l'ensemble $\mathcal{P}_{p-1}(E \setminus \{x_0\})$ et $|\mathcal{P}_{p-1}(E \setminus \{x_0\})| = \binom{n}{p-1}$. D'après la proposition 31, l'ensemble $\mathcal{P}_p^{x_0}(E)$ est fini de cardinal $\left|\mathcal{P}_p^{x_0}(E)\right| = \binom{n}{p-1}$.

(iii) On observe que $\mathcal{P}_p^{\overline{x_0}}(E) = \mathcal{P}_p(E \setminus \{x_0\})$. Comme $E \setminus \{x_0\}$ est fini de cardinal n et $0 \leqslant k \leqslant n$, l'hypothèse de récurrence livre la finitude de l'ensemble $\mathcal{P}_p(E \setminus \{x_0\}) = \mathcal{P}_p^{\overline{x_0}}(E)$ et $\left|\mathcal{P}_p^{\overline{x_0}}(E)\right| = \binom{n}{p}$.

De (i), (ii) et (iii), on déduit que l'ensemble $\mathcal{P}_p(E)$ est fini et que :

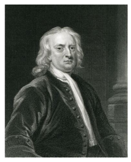
$$|\mathcal{P}_p(E)| = \binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}$$

□

3.12. Formule du binôme de Newton : approche combinatoire

Proposition 53. — *Soient A un anneau commutatif, a_1, a_2 deux éléments de A qui commutent ($a_1 \times a_2 = a_2 \times a_1$) et $n \in \mathbf{N}^*$. Alors :*

$$(a_1 + a_2)^n = \sum_{p=0}^{n} \binom{n}{p} a_1^p \, a_2^{n-p}$$



Isaac Newton (1642-1727)

Démonstration. Tout d'abord, nous écrivons la puissance n-ième $(a_1 + a_2)^n$ sous forme d'un produit :

$$(a_1 + a_2)^n = \underbrace{(a_1 + a_2)\,(a_1 + a_2)\,\ldots\,(a_1 + a_2)}_{n \text{ facteurs}} = \left(\sum_{i_1 \in \{1,2\}} a_{i_1}\right)\left(\sum_{i_2 \in \{1,2\}} a_{i_2}\right)\ldots\left(\sum_{i_n \in \{1,2\}} a_{i_n}\right)$$

En développant, il vient :

$$(a_1 + a_2)^n = \sum_{(i_1, \ldots, i_n) \in \{1,2\}^n} a_{i_1}\, a_{i_2}\, \ldots\, a_{i_n} \tag{6}$$

En regroupant ensemble les n-uplets d'éléments de $\{1,2\}$ suivant le nombre de composantes égales à 1, nous obtenons la décomposition ensembliste :

$$\{1,2\}^n = \bigsqcup_{p=0}^{n} \underbrace{\{(i_1, \ldots, i_n) \in \{1,2\}^n \;:\; |\{j \in [\![1,n]\!] \;:\; i_j = 1\}| = p\}}_{I_p}$$

L'identité (6) et l'identité $a_1 \times a_2 = a_2 \times a_1$ livrent alors :

$$(a_1 + a_2)^n = \sum_{p=0}^{n} \sum_{(i_1, \ldots, i_n) \in I_p} a_{i_1}\, a_{i_2}\, \ldots\, a_{i_n} = \sum_{p=0}^{n} \sum_{(i_1, \ldots, i_n) \in I_p} a_1^p\, a_2^{n-p} = \sum_{p=0}^{n} |I_p|\; a_1^p\, a_2^{n-p}$$

Soit $p \in [\![0,n]\!]$. Comme l'application :

$$\left|\begin{array}{ccc} I_p & \longrightarrow & \mathcal{P}_p([\![1,n]\!]) \\ (i_1, \ldots, i_n) & \longmapsto & \{j \in [\![1,n]\!] \;:\; i_j = 1\} \end{array}\right.$$

est bien définie et bijective, les propositions 31 et 52 livrent $|I_p| = \binom{n}{p}$. □

3.13. Ensemble des parties d'un ensemble fini

Proposition 54. — *Soit E un ensemble fini. Alors $\mathcal{P}(E)$ est fini et :*

$$|\mathcal{P}(E)| = 2^{|E|}$$

Démonstration. Posons $n := |E|$. On rappelle que $\mathcal{P}(E) = \bigsqcup_{p=0}^{n} \mathcal{P}_p(E)$. Avec la proposition 52, on en déduit que $\mathcal{P}(E)$ est fini et :

$$|\mathcal{P}(E)| = \sum_{p=0}^{n} \binom{n}{p} = \sum_{p=0}^{n} \binom{n}{p} \times 1^p \times 1^{n-p} = (1+1)^n = 2^n\,.$$

□

4. Une synthèse des résultats sur les ensembles finis

(1) Définition d'un ensemble fini. — Un ensemble E est fini si E est vide ou s'il existe un entier $n \in \mathbf{N}^*$ et une bijection $f\colon [\![1,n]\!] \longrightarrow E$.

(2) Pierre angulaire pour définir le cardinal d'un ensemble fini. — Si $(n,m) \in \mathbf{N}^*$ et s'il existe une application $f\colon [\![1,n]\!] \longrightarrow [\![1,m]\!]$ bijective, alors $n = m$.

(3) Définition du cardinal d'un ensemble fini. — Soit E est un ensemble fini non vide. L'unique nombre $n \in \mathbf{N}^*$ tel qu'il existe une bijection $f\colon [\![1,n]\!] \longrightarrow E$ est appelé cardinal de n et est noté $|E|$. Le cardinal de l'ensemble vide est 0.

(4) Des parties d'un ensemble fini. — Soient E un ensemble fini et A une partie de E.
- (a) L'ensemble A est fini et $|A| \leqslant |E|$.
- (b) Si $|A| = |E|$, alors $A = E$.

(5) Union disjointe de parties d'un ensemble fini. — Soient E un ensemble fini et $A_1, \ldots, A_p$ des parties de E deux à deux disjointes. Alors :

$$\left| \bigsqcup_{i=1}^{p} A_i \right| = \sum_{i=1}^{p} |A_i| \, .$$

(6) Union de deux parties d'un ensemble fini. — Soient E un ensemble fini et A_1, A_2 deux parties de E. Alors :

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \, .$$

(7) Produit cartésien d'ensembles finis. — Soient $E_1, \ldots, E_p$ des ensembles finis. Alors $\prod_{i=1}^{p} E_i$ est fini et :

$$\left| \prod_{i=1}^{p} E_i \right| = \prod_{i=1}^{p} |E_i| \, .$$

(8) Ensemble des applications entre deux ensembles finis. — Soient E et F des ensembles finis. Alors F^E est fini et :

$$\left| F^E \right| = |F|^{|E|} \, .$$

(9) Critère de bijectivité. — Soient E, F des ensembles finis de même cardinal et $f\colon E \longrightarrow F$ une application. Les trois assertions suivantes sont équivalentes.
- (a) L'application f est injective.
- (b) L'application f est surjective.
- (c) L'application f est bijective.

(10) p-listes sans répétition d'éléments d'un ensemble fini. — Soient E un ensemble fini de cardinal $n \in \mathbf{N}^*$ et $p \in [\![1,n]\!]$.
- (a) Une p-liste sans répétition d'éléments de E (ou un arrangement de p éléments de E) est un p-uplet d'éléments de E deux à deux distincts.
- (b) L'ensemble des p-listes sans répétition d'éléments de E est noté $\mathcal{A}_p(E)$.
- (c) L'ensemble $\mathcal{A}_p(E)$ est fini, de cardinal $\dfrac{n!}{(n-p)!}$.

(11) Permutations d'un ensemble fini. — Soit E un ensemble fini.
- (a) Une permutation de E est une bijection de E dans E.
- (b) L'ensemble des permutations de E est noté $\mathfrak{S}(E)$.
- (c) L'ensemble $\mathfrak{S}(E)$ est fini, de cardinal $|\mathfrak{S}(E)| = |E|!$.

(12) p-combinaisons d'un ensemble fini. — Soient E un ensemble fini de cardinal $n \in \mathbf{N}^*$ et $p \in [\![0,n]\!]$.
- (a) Une p-combinaison d'éléments de E est une partie de E à p éléments.
- (b) L'ensemble des p-combinaisons d'éléments de E est noté $\mathcal{P}_p(E)$.
- (c) L'ensemble $\mathcal{P}_p(E)$ est fini, de cardinal $\dbinom{n}{p}$.

(13) Ensemble des parties d'un ensemble fini. — Soit E un ensemble fini. L'ensemble $\mathcal{P}(E)$ des parties de E est fini et :

$$|\mathcal{P}(E)| = 2^{|E|}.$$