

Dénombrement

- 1. Application 1
- 2. Injection, surjection, bijection 2
 - 2.1. Définitions des trois notions 2
 - 2.2. L'application réciproque d'une application bijective 3
 - 2.3. Une étude d'injectivité et de surjectivité dans le cadre des nombres complexes 3
 - 2.4. Une étude d'injectivité et de surjectivité d'une fonction réelle de la variable réelle 4
 - 2.5. Deux études d'injectivité et de surjectivité en algèbre linéaire 4
 - 2.6. Une étude d'injectivité et de surjectivité dans le cadre des EDL 5
 - 2.7. Stabilité de l'injectivité (resp. surjectivité, bijectivité) par composition 5
 - 2.8. Injectivité et inversibilité à gauche, surjectivité et inversibilité à droite 5
 - 2.9. Digression : avoir le même « nombre d'éléments » 6
 - 2.10. Les ensembles \mathbb{N} , \mathbb{Z} et \mathbb{N}^2 sont équipotents 6
 - 2.11. Théorème de Cantor 9
- 3. Ensembles finis 9
 - 3.1. Définitions d'un ensemble fini et du cardinal d'un tel 9
 - 3.2. Parties d'un ensemble fini 10
 - 3.3. Réunion disjointe d'ensembles finis 11
 - 3.4. Réunion d'ensembles finis 12
 - 3.5. Théorème de Lagrange sur les sous-groupes d'un groupe fini 13
 - 3.6. Produit cartésien d'ensembles finis 13
 - 3.7. Ensemble des applications entre deux ensembles finis 14
 - 3.8. Critère de bijectivité pour une application entre deux ensembles finis 14
 - 3.9. Ensemble des applications injectives entre deux ensembles finis et p -listes sans répétition 15
 - 3.10. Permutations d'un ensemble fini 16
 - 3.11. Ensemble des parties à p -éléments d'un ensemble fini ou p -combinaisons 16
 - 3.12. Formule du binôme de Newton : approche combinatoire 17
 - 3.13. Ensemble des parties d'un ensemble fini 18
- 4. Une synthèse des résultats sur les ensembles finis 18

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 unique 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.

Remarque 2. — On peut également définir une application comme un triplet (E, F, Γ) où E, F sont des ensembles et Γ est une partie de $E \times F$ telle que :

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

À partir d'un tel triplet, on définit l'application f , au sens de la définition 1, de source E et de but F par :

$$f \left| \begin{array}{l} E \longrightarrow \\ x \longmapsto \end{array} \right. \begin{array}{l} F \\ \text{l'unique élément } y \text{ de } F \text{ tel que } (x, y) \in \Gamma. \end{array}$$

L'ensemble Γ est alors appelé graphe de l'application f .

Exemple 3. — Si A est une partie d'un ensemble E , alors l'indicatrice de A est l'application notée $\mathbf{1}_A$ et définie par :

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

2. Injection, surjection, bijection

2.1. Définitions des trois notions

Définition 4. — Soit $f : E \longrightarrow F$ une application.

1. L'application f est dite injective si :

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

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 $f : E \longrightarrow F$ revient à étudier, pour tout $y \in F$, l'équation :

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

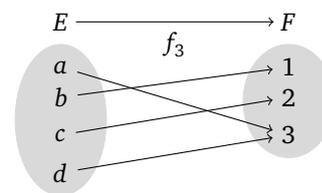
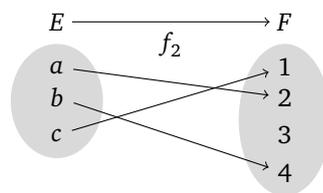
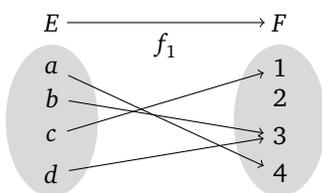
d'inconnue $x \in E$.



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

Exercice 6. — 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 :



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

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

Exercice 7. — Soit f l'application définie par :

$$f \left| \begin{array}{l} \mathbf{R} \longrightarrow \mathbf{R} \\ x \longmapsto 2x^2 - 3x + 5 \end{array} \right.$$

1. Justifier que l'application f n'est ni injective, ni surjective.
2. Déterminer deux intervalles ouverts I, J de \mathbf{R} tels que la restriction-corestriction de f :

$$f|_I \left| \begin{array}{l} I \longrightarrow J \\ x \longmapsto f(x) \end{array} \right.$$

est bijective.

2.2. L'application réciproque d'une application bijective

Définition 8. — Soit $f : E \longrightarrow F$ une application bijective. L'application f^{-1} définie par :

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

est appelée application réciproque de f .

Proposition 9. — Soit $f : E \longrightarrow F$ une application bijective.

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

Démonstration.

1. Soit $y \in F$. Comme $f^{-1}(y)$ est l'antécédent de y par f dans E :

$$f \circ f^{-1}(y) = f(f^{-1}(y)) = y = \text{id}_F(y).$$

2. Soit $x \in E$. Comme x est l'antécédent de $f(x)$ par f dans E :

$$f^{-1} \circ f(x) = f^{-1}(f(x)) = x = \text{id}_E(x).$$

3. (a) *Injectivité de l'application f^{-1} .*

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 :

$$f(f^{-1}(y_1)) = f(f^{-1}(y_2))$$

ce qui, avec la propriété $f \circ f^{-1} = \text{id}_F$, livre $y_1 = y_2$.

- (b) *Surjectivité de l'application f^{-1} .*

Soit $x \in E$. Grâce à la propriété $f^{-1} \circ f = \text{id}_E$, 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 :

$$f^{-1} \circ f = \text{id}_E$$

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

$$f = (f^{-1})^{-1}.$$

□

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

Exercice 10. — Soit l'application f définie par :

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

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} .

Considérons un nombre complexe non nul z .

1. Les deux racines complexes de z sont données par $\sqrt{|z|} e^{i \frac{\arg(z)}{2}}$ et $-\sqrt{|z|} e^{i \frac{\arg(z)}{2}}$.
2. D'après 1, si l'on connaît une forme exponentielle explicite de z , on est en mesure de calculer les deux racines carrées complexes de z . Dans le cas contraire, on introduit l'équation :

$$(\mathcal{E}) \quad (a + ib)^2 = z$$



d'inconnue $(a, b) \in \mathbf{R}^2$, que l'on résout par analyse et synthèse. On notera que l'équation (\mathcal{E}) est équivalente au système algébrique :

$$\begin{cases} a^2 - b^2 = \operatorname{Re}(z) & \text{(équation des parties réelles)} \\ 2ab = \operatorname{Im}(z) & \text{(équation des parties imaginaires)} \\ a^2 + b^2 = |z| & \text{(équation des modules)} \end{cases}$$

plus aisé à résoudre.

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

Exercice 11. — Soit l'application f définie par :

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

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 $y \geq 1$, 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 $\int_2^5 \frac{1}{\sqrt{x^2-1}} dx$.

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

Exercice 12. — Soient a un nombre réel fixé et f l'application définie par :

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

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

Exercice 13. — Soient n un entier naturel, a_0, a_1, \dots, a_n des nombres réels et f l'application définie par :

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

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 14. — Soit l'application φ définie par :

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

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 15. — 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 :

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

est injective. Pour cela, considérons deux éléments x_1, x_2 de E tels que :

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

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 16. — Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ des applications bijectives. Alors :

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

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

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

En composant chacun des membres de l'identité :

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

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 17. — Soit $f : E \longrightarrow F$ une application.

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

Démonstration.

1. (a) *Sens réciproque* \Leftarrow .

Supposons qu'il existe une application $g : F \longrightarrow E$ telle que $g \circ f = \text{id}_E$. Considérons deux éléments x_1, x_2 de E tels que :

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

En appliquant g à chacun des membres de l'identité précédente, il vient $x_1 = x_2$.

- (b) *Sens direct* \Rightarrow .

Supposons l'application f injective. Fixons un élément x_0 de l'ensemble E supposé non vide et considérons l'application g définie par :

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

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 :

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

2. (a) *Sens réciproque* \Leftarrow .

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

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

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

- (b) *Sens direct* \Rightarrow .

Supposons l'application f surjective. Considérons un élément $y \in F$ 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 :

$$g \begin{cases} F \longrightarrow E \\ y \longmapsto \text{l'antécédent } g(y) \text{ de } y \text{ par } f \text{ dans } E \text{ préalablement choisi} \end{cases}$$

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

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

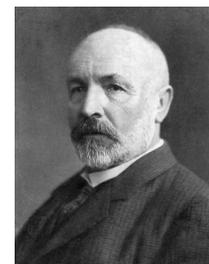
□

Exercice 18. — Soit $f : E \longrightarrow F$ une application injective. D'après la proposition précédente, il existe une application $g : F \longrightarrow E$ telle que $g \circ f = \text{id}_E$. Que dire de l'application g ?

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

Définition 19. — 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 20. — 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 », bien que cette notion de « nombre d'éléments » ne soit pas (encore) fondée. Cette idée est due à Georg Cantor.



Georg Cantor (1845-1918)

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

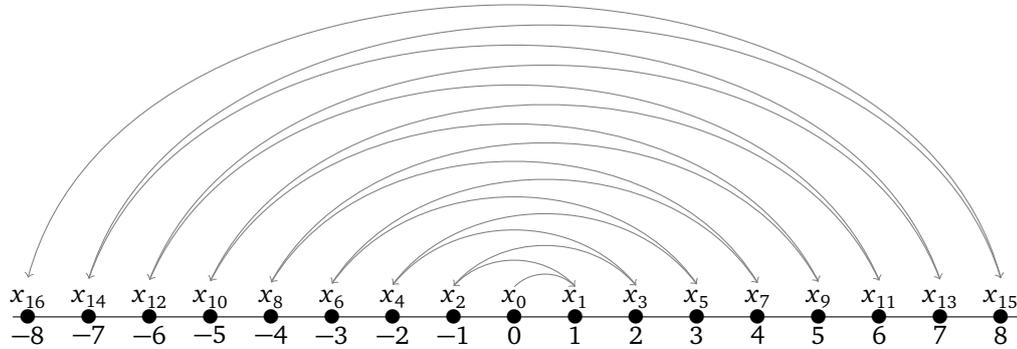
Exercice 21. — Démontrer que les ensembles \mathbb{N} et \mathbb{N}^* sont équipotents.

Proposition 22. — Les ensembles \mathbf{N} et \mathbf{Z} sont équipotents.

Éléments de démonstration.

(a) 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 ».



(b) Construction de deux applications $f : \mathbf{N} \longrightarrow \mathbf{Z}$ et $g : \mathbf{Z} \longrightarrow \mathbf{N}$ 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 $n \geq 0$. C'est ainsi qu'apparaissent les applications :

$$f \left| \begin{array}{l} \mathbf{N} \longrightarrow \\ n \longmapsto \end{array} \right. \left\{ \begin{array}{l} -n/2 \text{ si } n \text{ est pair} \\ (n+1)/2 \text{ si } n \text{ est impair} \end{array} \right. \quad \text{et} \quad g \left| \begin{array}{l} \mathbf{Z} \longrightarrow \\ n \longmapsto \end{array} \right. \left\{ \begin{array}{l} -2n \text{ si } n \leq 0 \\ 2n - 1 \text{ si } n > 0 \end{array} \right.$$

qui sont bien définies.

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

□

Lemme 23. — Soit $x = (x_p)_{p \in \mathbf{N}}$ une suite strictement croissante d'entiers naturels. Alors :

$$\forall p \in \mathbf{N} \quad x_p \geq p .$$

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

$$\mathcal{P}(p) : x_p \geq p .$$

(a) Initialisation à $p = 0$.

Comme $x_0 \in \mathbf{N}$, $x_0 \geq 0$. L'assertion $\mathcal{P}(0)$ est donc vraie.

(b) 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 :

$$x_{p+1} > x_p \geq p$$

d'où $x_{p+1} > p$. Comme x_{p+1} et p sont de plus entiers, nous en déduisons $x_{p+1} \geq p + 1$.

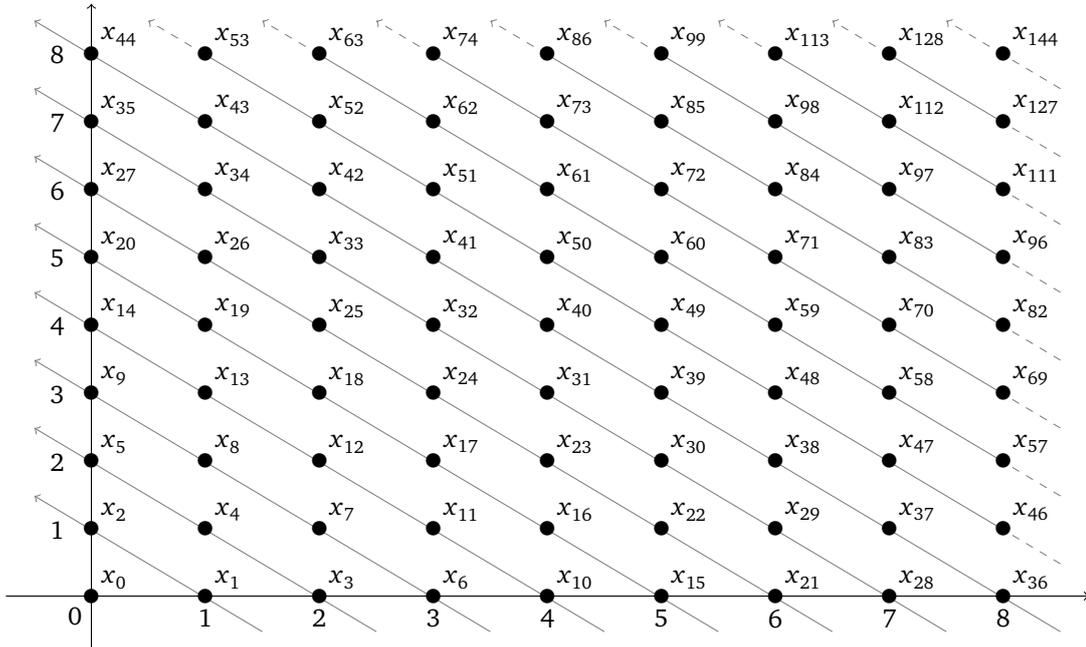
□

Proposition 24. — Les ensembles \mathbf{N} et \mathbf{Z}^2 sont équipotents.

Démonstration.

(a) *Principe de la numérotation.*

On numérote $(0, 0)$ à 0, puis on serpente de manière diagonale à travers le réseau dessiné par \mathbb{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.



(b) *Construction d'une application $f : \mathbb{Z}^2 \longrightarrow \mathbb{N}$ à partir de la numérotation précédente.*

On commence par observer que, pour tout $k \in \mathbb{N}$, $k+1$ points du réseau dessiné par \mathbb{N}^2 figurent sur la diagonale d'équation $y = -x + k$.

Soit $(a, b) \in \mathbb{N}^2 \setminus \{(0, 0)\}$. 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 \mathbb{N}^2 se sont déjà vus attribuer un numéro. Il faut encore en numéroté $b+1$ 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 \mathbb{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 :

$$f \left| \begin{array}{l} \mathbb{Z}^2 \longrightarrow \mathbb{N} \\ (a, b) \longmapsto b + \sum_{k=0}^{a+b} k = b + \frac{(a+b)(a+b+1)}{2} \end{array} \right.$$

(c) *Une suite d'entiers auxiliaire.*

La suite :

$$\left(S_p = \sum_{k=0}^p k = \frac{p(p+1)}{2} \right)_{p \in \mathbb{N}}$$

est une suite strictement croissante d'entiers naturels. D'après le lemme précédent :

$$\forall p \in \mathbb{N} \quad S_p \geq p. \tag{3}$$

(d) *Surjectivité de l'application f .*

Soit $n \in \mathbb{N}$. D'après (3) :

$$A := \{p \in \mathbb{N} : S_p \leq n\} \subset \llbracket 0, n \rrbracket$$

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 :

$$S_{p_0} \leq n \leq S_{p_0+1} - 1 = S_{p_0} + p_0. \quad (4)$$

Nous définissons deux entiers relatifs a et b par :

$$b = n - S_{p_0} \quad \text{et} \quad a = p_0 - b = S_{p_0} + p_0 - n.$$

D'après (4), $a \geq 0$ et $b \geq 0$, donc a et b sont des entiers naturels. Nous vérifions enfin que :

$$f(a, b) = S_{a+b} + b = S_{p_0} + n - S_{p_0} = n.$$

(e) *Injectivité de l'application f .*

Soient $(a_1, b_1) \in \mathbb{Z}^2$ et $(a_2, b_2) \in \mathbb{Z}^2$ tels que :

$$b_1 + S_{a_1+b_1} = f(a_1, b_1) = f(a_2, b_2) = b_2 + S_{a_2+b_2}. \quad (5)$$

Quitte à échanger les rôles de (a_1, b_1) et (a_2, b_2) , nous pouvons supposer que $a_1 + b_1 \leq a_2 + b_2$. Alors :

$$S_{a_1+b_1} \leq S_{a_2+b_2} \leq S_{a_2+b_2} + b_2 = S_{a_1+b_1} + b_1 < S_{a_1+b_1+1}.$$

Comme la suite $(S_p)_{p \in \mathbb{N}}$ est strictement croissante, de $S_{a_1+b_1} \leq S_{a_2+b_2} < S_{a_1+b_1+1}$, 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 25. — *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 $f : E \longrightarrow \mathcal{P}(E)$ 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 26. — Les ensembles \mathbb{N} et $\mathcal{P}(\mathbb{N})$ ne sont donc pas équipotents. Nous en déduirons, plus tard, que les ensembles \mathbb{N} et \mathbb{R} ne sont pas équipotents.

3. Ensembles finis

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

Théorème 27. — *Soient n et m deux entiers naturels non nuls.*

1. *S'il existe une application injective $f : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, m \rrbracket$, alors $n \leq m$.*
2. *S'il existe une application surjective $f : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, m \rrbracket$, alors $n \geq m$.*
3. *S'il existe une application bijective $f : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, m \rrbracket$, alors $n = m$.*

Démonstration.

1. On démontre par récurrence que, pour tout $n \in \mathbb{N}^*$:

$$\mathcal{P}(n) : \ll \forall m \in \mathbb{N}^* \quad (\exists f : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, m \rrbracket \text{ injective}) \implies n \leq m \gg$$

est vrai.

(a) *Initialisation* à $n = 1$.

Clair.

(b) *Hérédité*.

Soit $n \in \mathbb{N}^*$ tel que $\mathcal{P}(n)$ est vraie. Soient $m \in \mathbb{N}^*$ et $f : \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, m \rrbracket$ injective. Nous souhaitons établir que $n+1 \leq m$.

- 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 $m - 1 \geq 1$.
- Supposons que $f(n+1) = m$. Alors l'application :

$$\bar{f} \left| \begin{array}{l} \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, m-1 \rrbracket \\ x \longmapsto f(x) \end{array} \right.$$

est bien définie et est injective, comme restriction et corestriction de l'application injective f . D'après $\mathcal{P}(n)$, $n \leq m-1$ et donc $n+1 \leq m$.

- Supposons que $f(n+1) \neq m$. Considérons la transposition $\tau_{f(n+1),m} : \llbracket 1, m \rrbracket \longrightarrow \llbracket 1, m \rrbracket$ qui envoie $f(n+1)$ sur m , m sur $f(n+1)$ et qui fixe tous les autres éléments de $\llbracket 1, m \rrbracket$. On observe que l'application $g := \tau_{f(n+1),m} \circ f : \llbracket 1, n+1 \rrbracket \longrightarrow \llbracket 1, m \rrbracket$ est injective (composée d'applications injectives) et vérifie $g(n+1) = m$. On est alors ramené au cas précédent, d'où $n+1 \leq m$.

2. S'il existe une surjection de $\llbracket 1, n \rrbracket$ vers $\llbracket 1, m \rrbracket$, alors il existe une injection de $\llbracket 1, m \rrbracket$ dans $\llbracket 1, n \rrbracket$. Le résultat se déduit donc de 1.

3. Conséquence de 1 et 2.

□

Définition 28. — Un ensemble E est fini s'il vérifie l'une des deux conditions suivantes.

1. $E = \emptyset$
2. Il existe $n \in \mathbb{N}^*$ et une bijection $f : \llbracket 1, n \rrbracket \longrightarrow E$.

Définition 29. — Soit E un ensemble fini. Le cardinal de E est le nombre entier noté $|E|$ ou $\text{Card}(E)$ ou $\#E$ défini par :

$$|E| := \begin{cases} 0 & \text{si } E = \emptyset \\ n & \text{s'il existe un entier } n \in \mathbb{N}^* \text{ et une bijection } f : \llbracket 1, n \rrbracket \longrightarrow E. \end{cases}$$

Remarque 30. — D'après le théorème 27, le cardinal d'un ensemble fini non vide est bien défini.

Exemple 31. — Si $n \in \mathbb{N}^*$, alors $\llbracket 1, n \rrbracket$ est fini et $|\llbracket 1, n \rrbracket| = n$. En effet, l'application $\text{id}_{\llbracket 1, n \rrbracket} : \llbracket 1, n \rrbracket \longrightarrow \llbracket 1, n \rrbracket$ est bijective.

Exemple 32. — 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 :

$$\left| \begin{array}{l} \llbracket 1, 1 \rrbracket = \{1\} \longrightarrow E \\ 1 \longmapsto a \end{array} \right.$$

est bijective.

Proposition 33. — Soit E un ensemble fini non vide et $\varphi : E \longrightarrow F$ 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 $n \in \mathbb{N}^*$ et une application bijective $f : \llbracket 1, n \rrbracket \longrightarrow E$. L'application $\varphi \circ f : \llbracket 1, n \rrbracket \longrightarrow F$ est bijective (composée d'applications bijectives). Ainsi F est fini et $|F| = n = |E|$. □

Exercice 34. — Soient a et b des entiers relatifs tels que $a \leq b$. Démontrer que l'ensemble $\llbracket a, b \rrbracket$ est fini que :

$$\text{card}(\llbracket a, b \rrbracket) = b - a + 1.$$

3.2. Parties d'un ensemble fini

Théorème 35. — Soient $n \in \mathbb{N}^*$ et A une partie de $\llbracket 1, n \rrbracket$.

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

Démonstration.

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

$$\mathcal{P}(n) : \ll \forall A \in \mathcal{P}(\llbracket 1, n \rrbracket) \quad A \subsetneq \llbracket 1, n \rrbracket \implies (A \text{ est fini et } |A| < n) \gg$$

est vrai.

- (a) *Initialisation à $n = 1$.*

L'ensemble vide est la seule partie de $\llbracket 1, 1 \rrbracket = \{1\}$ distincte de $\{1\}$. Comme \emptyset est fini de cardinal $0 < 1$, l'assertion $\mathcal{P}(1)$ est établie.

- (b) *Hérédité.*

Soit $n \in \mathbb{N}^*$ tel que $\mathcal{P}(n)$ est vraie. Ceci implique que toute partie X de $\llbracket 1, n \rrbracket$ est finie de cardinal $|X| \leq n$. En effet, si $X \neq \llbracket 1, n \rrbracket$ il s'agit d'une conséquence de $\mathcal{P}(n)$. Sinon $X = \llbracket 1, n \rrbracket$ et le résultat découle de l'exemple 31.

Soit A une partie de $\llbracket 1, n+1 \rrbracket$ distincte de $\llbracket 1, n+1 \rrbracket$.

- Si $A = \emptyset$ 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 $\llbracket 1, n \rrbracket$. Donc A est fini et $|A| \leq n < n+1$.
 - Supposons à présent que $n+1 \in A$. Comme $A \neq \llbracket 1, n+1 \rrbracket$, il existe $a \in \llbracket 1, n \rrbracket$ tel que $a \notin A$. Introduisons la partie :

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

de $\llbracket 1, n \rrbracket$. Ainsi B est finie et $|B| \leq n$. Les applications :

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

sont bien définies. On vérifie que $f \circ g = \text{id}_A$ et $g \circ f = \text{id}_B$. L'application f est donc bijective. D'après la proposition 33, A est fini et $|A| = |B| \leq n < n+1$.

2. Si $A \neq \llbracket 1, n \rrbracket$ alors, d'après 1, A est fini et $|A| < n$. Si $A = \llbracket 1, n \rrbracket$ alors, d'après l'exemple 31, A est fini et $|A| = n$.
3. Conséquence de la disjonction de cas opérée pour la démonstration de 2.

□

Corollaire 36. — Soit E une ensemble fini de cardinal $n \in \mathbb{N}^*$. 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 $f : E \longrightarrow \llbracket 1, n \rrbracket$. Si A est une partie de E , alors l'application :

$$f|_A \left| \begin{array}{l} A \longrightarrow f(A) \\ a \longmapsto f(a) \end{array} \right.$$

est une bijection de A vers la partie :

$$f(A) := \{f(a) : a \in A\}$$

de $\llbracket 1, n \rrbracket$. De plus $A = E$ si et seulement si $f(A) = \llbracket 1, n \rrbracket$.

1. Supposons que $A \neq E$. Alors $f(A) \neq \llbracket 1, n \rrbracket$. D'après le théorème 35, l'ensemble $f(A)$ est fini et $|f(A)| < n$. D'après la proposition 33, l'ensemble A est fini et $|A| < n$ (A et $f(A)$ sont équipotents via $f|_A$).
2. Si $A = E$ alors, d'après 1, A est fini et $|A| < n$. Si $A = E$ alors A est fini et $|A| = n$ (E est équipotent à $\llbracket 1, n \rrbracket$).
3. Conséquence de la disjonction de cas opérée pour la démonstration de 2.

□

3.3. Réunion disjointe d'ensembles finis

Théorème 37. — 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 $A = \emptyset$, 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 $B = \emptyset$.

Supposons désormais que A et B sont non vides. Comme A et B sont finies et non vides, il existe $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ et deux applications bijectives : $f : \llbracket 1, a \rrbracket \longrightarrow A$ et $g : \llbracket 1, b \rrbracket \longrightarrow B$. L'application :

$$h \left| \begin{array}{l} \llbracket 1, a+b \rrbracket \longrightarrow A \sqcup B \\ n \longmapsto \begin{cases} f(n) & \text{si } n \leq a \\ g(n-a) & \text{si } n \geq a+1 \end{cases} \end{array} \right.$$

est bien définie.

- Soit $(n_1, n_2) \in \llbracket 1, a+b \rrbracket^2$ tel que $h(n_1) = h(n_2) \in A \sqcup B$.
 - Supposons $h(n_1) = h(n_2) \in A$. Alors comme $A \cap B = \emptyset$, $n_1 \leq a$ et $n_2 \leq a$ 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 $A \cap B = \emptyset$, $n_1 \geq a+1$ et $n_2 \geq a+1$ 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 $f^{-1}(y) \in \llbracket 1, a \rrbracket$ et donc $h(f^{-1}(y)) = f(f^{-1}(y)) = y$.
 - Si $y \in B$, alors $g^{-1}(y) \in \llbracket 1, b \rrbracket$ et donc $a + g^{-1}(y) \in \llbracket a+1, a+b \rrbracket$. Ainsi $h(a + g^{-1}(y)) = g(g^{-1}(y)) = y$.

L'application h est surjective.

Comme l'application h est bijective, la proposition 33 livre la finitude de l'ensemble $A \sqcup B$ et $|A \sqcup B| = a + b = |A| + |B|$. □

Corollaire 38. — Soient un entier $p \geq 2$ 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 $p \geq 2$.

(a) *Initialisation.*

Elle découle du théorème 37.

(b) *Hérédité.*

Pour l'établir, 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 39. — Soit A et B deux parties d'un ensemble fini E . Justifier que :

$$|A| + |B| > |E| \implies A \cap B \neq \emptyset . \quad [\text{principe des tiroirs}] .$$

3.4. Réunion d'ensembles finis

Proposition 40. — *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 36). 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 38 :

$$|A| \stackrel{(i)}{=} |A \cap B| + |A \setminus A \cap B| \quad |B| \stackrel{(ii)}{=} |A \cap B| + |B \setminus A \cap B| \quad |A \cup B| \stackrel{(iii)}{=} |A \setminus A \cap B| + |A \cap B| + |B \setminus A \cap B| .$$

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

Exercice 41. — Soient $p \geq 2$ et A_1, A_2, \dots, A_p des parties finies d'un ensemble fini E . Démontrer que :

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



Henri Poincaré (1854-1912)

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

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

Exercice 42. — 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

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

est une relation d'équivalence.

2. Soit $g \in G$. Nous notons \bar{g} la classe d'équivalence de g pour la relation \sim , définie par :

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

Démontrer que $\bar{g} = g * H$.

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 :

$$G / \sim := \{\bar{g} : g \in G\} .$$

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 43. — 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 $f_1 : \llbracket 0, n_1 - 1 \rrbracket \longrightarrow E_1$ et $f_2 : \llbracket 0, n_2 - 1 \rrbracket \longrightarrow E_2$.

Pour tout $x \in \llbracket 0, n_1 n_2 - 1 \rrbracket$, il existe un unique couple $(q(x), r(x)) \in \llbracket 0, n_2 - 1 \rrbracket \times \llbracket 0, n_1 - 1 \rrbracket$ tel que :

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

L'application :

$$f \left| \begin{array}{l} \llbracket 0, n_1 n_2 - 1 \rrbracket \longrightarrow E_1 \times E_2 \\ x \longmapsto (f_1(r(x)), f_2(q(x))) \end{array} \right.$$

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

Proposition 44. — cardinal du produit cartésien de p ensembles finis Soient $p \in \mathbf{N}_{\geq 2}$ et E_1, \dots, 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 $p \geq 2$.

- L'initialisation découle de la proposition 43.
- Pour établir l'hérédité, on remarque que si E_1, \dots, E_p, E_{p+1} sont des ensembles, alors l'application :

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

est bijective.

□

3.7. Ensemble des applications entre deux ensembles finis

Proposition 45. — Soient E et F des ensembles finis non vides. Alors l'ensemble F^E des applications de E vers F est fini et :

$$|F^E| = |F|^{|E|}.$$

Éléments de démonstration. Par hypothèse, il existe $n \in \mathbf{N}^*$ et une bijection $\varphi : \llbracket 1, n \rrbracket \longrightarrow E$.

1. L'application :

$$\left| \begin{array}{l} F^{\llbracket 1, n \rrbracket} \quad \longrightarrow \quad F^n \\ f \quad \longmapsto \quad (f(1), \dots, f(n)) \end{array} \right.$$

est bijective. D'après les propositions 33 et 38, l'ensemble $F^{\llbracket 1, n \rrbracket}$ est fini et $|F^{\llbracket 1, n \rrbracket}| = |F^n| = |F|^n = |F|^{|E|}$.

2. On vérifie que l'application :

$$\left| \begin{array}{l} F^E \quad \longrightarrow \quad F^{\llbracket 1, n \rrbracket} \\ f \quad \longmapsto \quad f \circ \varphi \end{array} \right.$$

est bijective. On conclut alors avec la proposition 33 et le point 1.

□

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

Théorème 46. — Soient E, F deux ensemble finis non vides. et une application $f : E \longrightarrow F$. 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) \implies (b) et (c). Clair.
2. (b) \implies (a). Supposons l'application f injective. Alors l'application :

$$f|_{f(E)} \left| \begin{array}{l} E \quad \longrightarrow \quad f(E) \\ x \quad \longmapsto \quad f(x) \end{array} \right.$$

est bijective. D'après la proposition 33, $|f(E)| = |E| = |F|$. La partie $f(E)$ de F est finie, de même cardinal que F . D'après le corollaire 36, $f(E) = F$, i.e. f est surjective.

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

□

Corollaire 49. — Soient E un ensemble fini de cardinal $n \in \mathbb{N}^*$ et $p \leq n$. L'ensemble $\mathcal{A}_p(E)$ est fini et :

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

Démonstration. Comme l'application :

$$\left| \begin{array}{ccc} \text{Inj}(\llbracket 1, p \rrbracket, E) & \longrightarrow & \mathcal{A}_p(E) \\ f & \longmapsto & (f(1), \dots, f(p)) \end{array} \right.$$

est bijective, le résultat est conséquence du théorème 47. □

3.10. Permutations d'un ensemble fini

Définition 50. — Soit E un ensemble non vide. Une permutation de E est une application $f : E \longrightarrow E$ 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. :

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

Proposition 51. — Soit E un ensemble fini non vide. L'ensemble $\mathfrak{S}(E)$ est fini et :

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

Démonstration. D'après le théorème 46, $\mathfrak{S}(E) = \text{Inj}(E, E)$. Le résultat découle alors du théorème 47. □

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

Définition 52. — Soient E un ensemble et $p \in \mathbb{N}^*$. 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 $p \in \mathbb{N}^*$, l'ensemble des p -combinaisons de E est noté $\mathcal{P}_p(E)$, i.e. :

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

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

Remarque 53. — Si E est un ensemble fini, alors :

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

Proposition 54. — Soit E un ensemble fini de cardinal n . Pour tout $p \in \llbracket 0, n \rrbracket$, l'ensemble $\mathcal{P}_p(E)$ est fini et :

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

Démonstration.

1. D'après le théorème 36, 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 $n \in \mathbb{N}$ que le prédicat :

$\mathcal{P}(n)$: « Pour tout ensemble E de cardinal n , pour tout $p \in \llbracket 0, n \rrbracket$, l'ensemble $\mathcal{P}_p(E)$ est fini et $|\mathcal{P}_p(E)| = \binom{n}{p}$. »

est vrai.

(a) *Initialisation à $n = 0$.*

Comme $\mathcal{P}(\emptyset) = \{\emptyset\}$, pour tout $p \in \mathbb{N}$:

$$\mathcal{P}_p(\emptyset) = \begin{cases} \{\emptyset\} & \text{si } p = 0 \\ \emptyset & \text{si } p \geq 1 \end{cases}$$

donc $|\mathcal{P}_p(\emptyset)| = \binom{0}{p}$.

(b) *Hérédité.*

Soit $n \in \mathbb{N}$ 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 $\mathcal{P}_0(E) = \{\emptyset\}$ est fini, de cardinal $1 = \binom{n+1}{0}$.

— L'ensemble E est de cardinal $n + 1 \geq 1$, donc non vide. Soient x_0 un élément de E fixé et $p \in \llbracket 1, n \rrbracket$.

(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 :

$$f \left| \begin{array}{ccc} \mathcal{P}_p^{x_0}(E) & \longrightarrow & \mathcal{P}_{p-1}(E \setminus \{x_0\}) \\ A & \longmapsto & A \setminus \{x_0\} \end{array} \right. \quad \text{et} \quad g \left| \begin{array}{ccc} \mathcal{P}_{p-1}(E \setminus \{x_0\}) & \longrightarrow & \mathcal{P}_p^{x_0}(E) \\ B & \longmapsto & B \sqcup \{x_0\} \end{array} \right.$$

sont bien définies et vérifient $f \circ g = \text{id}_{\mathcal{P}_{p-1}(E \setminus \{x_0\})}$ et $g \circ f = \text{id}_{\mathcal{P}_p^{x_0}(E)}$. L'application g est donc bijective. Comme $E \setminus \{x_0\}$ est fini de cardinal n et $0 \leq p - 1 \leq n$, 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 33, l'ensemble $\mathcal{P}_p^{x_0}(E)$ est

fini de cardinal $|\mathcal{P}_p^{x_0}(E)| = \binom{n}{p-1}$.

(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 $0 \leq k \leq n$, 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 $|\mathcal{P}_p^{\overline{x_0}}(E)| = \binom{n}{p}$.

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 55. — 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 $n \in \mathbb{N}^*$. 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 :

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

En développant, il vient :

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

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

$$\{1, 2\}^n = \bigsqcup_{p=0}^n \underbrace{\{(i_1, \dots, i_n) \in \{1, 2\}^n : |\{j \in \llbracket 1, n \rrbracket : i_j = 1\}| = p\}}_{I_p}.$$

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

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

Soit $p \in \llbracket 0, n \rrbracket$. Comme l'application :

$$\begin{cases} I_p & \longrightarrow \mathcal{P}_p(\llbracket 1, n \rrbracket) \\ (i_1, \dots, i_n) & \longmapsto \{j \in \llbracket 1, n \rrbracket : i_j = 1\} \end{cases}$$

est bien définie et bijective, les propositions 33 et 54 livrent $|I_p| = \binom{n}{p}$. □

3.13. Ensemble des parties d'un ensemble fini

Proposition 56. — 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 54, 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 $n \in \mathbb{N}^*$ et une bijection $f : \llbracket 1, n \rrbracket \longrightarrow E$.

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

(3) Définition du cardinal d'un ensemble fini. — Soit E est un ensemble fini non vide. L'unique nombre $n \in \mathbb{N}^*$ tel qu'il existe une bijection $f : \llbracket 1, n \rrbracket \longrightarrow E$ est appelé cardinal de E 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 $|A| \leq |E|$.

(b) Si $|A| = |E|$, alors $A = E$.

(5) **Union disjointe de parties d'un ensemble fini.** — Soient E un ensemble fini et A_1, \dots, 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, \dots, 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 :

$$|F^E| = |F|^{|E|} .$$

(9) **Critère de bijectivité.** — Soient E, F des ensembles finis de même cardinal et $f : E \longrightarrow F$ 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 $p \in \llbracket 1, n \rrbracket$.

- (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 $\frac{n!}{(n-p)!}$.

(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 $p \in \llbracket 0, n \rrbracket$.

- (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 $\binom{n}{p}$.

(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 :

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