Chapitre 1

Dénombrement

Compter des objets est certainement l'activité la plus élémentaire à la base des mathématiques. Pourtant, à y regarder de plus près, ce n'est pas si facile. Déjà pour un ensemble fini, la méthode qui consiste à regarder ses éléments l'un après l'autre et à les compter (donc à les numéroter) n'est applicable que pour de « petits » ensembles. Le plus souvent on s'en sort en faisant une représentation de l'ensemble à dénombrer à l'aide d'un autre ensemble plus familier. Cette représentation est ce que l'on appelle une bijection. Elle est d'ailleurs à la base du processus de comptage qui consiste simplement à mettre en bijection un ensemble avec un ensemble de nombres entiers. Cette notion de bijection permet d'étendre en un certain sens le dénombrement aux ensembles infinis.

Dans tout ce qui suit, la notation $[\![a, b]\!]$ pour $a, b \in \mathbb{N}$ désigne l'ensemble de tous les entiers compris au sens large entre a et b. On définit de même les intervalles d'entiers semi ouverts ou ouverts. L'écriture un peu abusive « $\forall i = 1, \dots, n$ » signifie « $\forall i \in [\![1, n]\!]$ ».

1.1 Rappels ensemblistes

1.1.1 Opérations ensemblistes

Soit Ω un ensemble. On dit que l'ensemble A est un *sous-ensemble* ou une *partie* de Ω (notation $A \subset \Omega$) si tout élément de A est aussi un élément de Ω ($\forall \omega \in A$, $\omega \in \Omega$). On appelle $\mathcal{P}(\Omega)$ l'ensemble des parties de Ω, ce que l'on peut noter [1]

$$\mathcal{P}(\Omega) = \{A\ ;\ A \subset \Omega\}.$$

Ainsi les écritures $A \subset \Omega$ et $A \in \mathcal{P}(\Omega)$ sont deux façons de dire la même chose [2].

1. Dans toutes les écritures d'ensembles entre accolades, nous utilisons le point virgule au sens de « tel que ».

2. Noter cependant la différence de statut de A : dans la première écriture, A est considéré comme un ensemble, dans la deuxième comme un élément d'un ensemble d'un type un peu particulier.

Si A et B sont deux parties du même ensemble Ω, on dit que A est *incluse* dans B (notation $A \subset B$) si tout élément de A est aussi élément de B ($\forall \omega \in A,\ \omega \in B$), autrement dit, si l'appartenance à A *implique* l'appartenance à B :

$$A \subset B \quad \text{signifie} \quad \forall \omega \in \Omega, \quad (\omega \in A) \Rightarrow (\omega \in B).$$

Soit I un ensemble quelconque d'indices (fini ou infini) et $(A_i)_{i \in I}$ une famille de parties de Ω. On définit son intersection $\bigcap_{i \in I} A_i$ et sa réunion, $\bigcup_{i \in I} A_i$ par :

$$\bigcap_{i \in I} A_i := \{\omega \in \Omega\ ;\ \forall i \in I,\ \omega \in A_i\} \qquad \text{et} \qquad \bigcup_{i \in I} A_i = \{\omega \in \Omega\ ;\ \exists i \in I,\ \omega \in A_i\}. \tag{1.1}$$

Autrement dit, $\bigcap_{i \in I} A_i$ est l'ensemble des éléments appartenant à la fois à *tous* les A_i et $\bigcup_{i \in I} A_i$ est l'ensemble des éléments appartenant à *au moins l'un* des A_i.

Remarque 1.1. La réunion et l'intersection d'une famille de parties de Ω sont définies de façon globale, elles s'obtiennent d'un coup, *sans passage à la limite* quand I est infini et sans qu'un ordre éventuel sur l'ensemble d'indices I n'ait d'importance.

Réunion et intersection sont très utiles pour la traduction automatique des quantificateurs. Si I est un ensemble quelconque d'indices, (π_i) une propriété dépendant de l'indice i et A_i l'ensemble des $\omega \in \Omega$ vérifiant (π_i),

$$\begin{aligned} \{\omega \in \Omega\ ;\ \forall i \in I,\ \omega \text{ vérifie } (\pi_i)\} &= \bigcap_{i \in I} A_i, \\ \{\omega \in \Omega\ ;\ \exists i = i(\omega) \in I,\ \omega \text{ vérifie } (\pi_i)\} &= \bigcup_{i \in I} A_i. \end{aligned}$$

Ainsi le quantificateur $\forall$ *peut se traduire par une intersection* et le quantificateur $\exists$ *par une réunion.* Pour une importante application de cette remarque, voir page 334.

L'intersection et l'union sont distributives l'une par rapport à l'autre, c'est à dire

$$B \cup \Big(\bigcap_{i \in I} A_i\Big) = \bigcap_{i \in I} (A_i \cup B), \qquad B \cap \Big(\bigcup_{i \in I} A_i\Big) = \bigcup_{i \in I} (A_i \cap B).$$

Le *complémentaire* de A (dans Ω) est l'ensemble $A^c := \{\omega \in \Omega\ ;\ \omega \notin A\}$. L'opération passage au complémentaire (qui est une bijection de $\mathcal{P}(\Omega)$ dans lui-même) vérifie $(A^c)^c = A$, $\Omega^c = \varnothing$, $\varnothing^c = \Omega$ et échange réunions et intersections grâce aux très utiles formules :

$$\Big(\bigcap_{i \in I} A_i\Big)^c = \bigcup_{i \in I} A_i^c \qquad \Big(\bigcup_{i \in I} A_i\Big)^c = \bigcap_{i \in I} A_i^c.$$

On définit le *produit cartésien* de deux ensembles E et F, noté $E \times F$, par :

$$E \times F := \{(x, y)\ ;\ x \in E, y \in F\}.$$

Attention, dans cette écriture (x, y) ne désigne en aucune façon un ensemble mais un couple d'éléments (l'ordre d'écriture a une importance). Pour éviter toute confusion, on utilise des accolades pour la description des ensembles et des parenthèses pour les couples d'éléments.

On définit de manière analogue le produit cartésien d'une suite finie d'ensembles $E_1, \dots, E_n$ par[3]

$$E_1 \times \cdots \times E_n := \big\{(x_1, \dots, x_n) \ ;\ \forall i \in [\![1, n]\!],\ x_i \in E_i\big\}.$$

L'ensemble $E^2 := E \times E = \{(x_1, x_2) \ ;\ x_1 \in E, x_2 \in E\}$ peut être utilisé pour représenter l'ensemble de toutes les applications de $\{1, 2\}$ dans E, le couple (x_1, x_2) correspondant à l'application $f : \{1, 2\} \to E$ définie par $f(1) = x_1$ et $f(2) = x_2$. Il pourrait de la même façon, représenter les applications d'un ensemble à deux éléments dans E (remplacer les chiffres 1 et 2 par n'importe quelle paire de symboles distincts : 0 et 1, a et b, etc.).

Plus généralement, pour $n \geqslant 2$, E^n est l'ensemble des n-uplets ou listes de longueur n d'éléments de E. Dans un n-uplet $(x_1, \dots, x_n)$, il peut y avoir des répétitions. On peut aussi utiliser E^n pour représenter toutes les applications de l'ensemble $[\![1, n]\!]$ (ou de n'importe quel ensemble à n éléments) dans E.

Soit I un ensemble quelconque, fini ou infini. Par analogie avec ce qui précède, l'ensemble de toutes les applications $f : I \to E$ sera noté E^I. Par exemple avec $E = \{0, 1\}$ et $I = \mathbb{N}$, on obtient l'ensemble $\{0, 1\}^{\mathbb{N}}$ de toutes les suites de chiffres binaires indexées par $\mathbb{N}$: $\{0, 1\}^{\mathbb{N}} = \{u = (u_i)_{i \in \mathbb{N}} \ ;\ u_i = 0 \text{ ou } 1\}$. Avec $E = \mathbb{R}$ et $I = [0, 1]$, on obtient l'ensemble $\mathbb{R}^{[0,1]}$ des fonctions définies sur l'intervalle $[0, 1]$ et à valeurs dans $\mathbb{R}$.

1.1.2 Bijections

Définition 1.2 (injection)**.** *Une application $f : E \to F$ est dite* injective *si deux éléments distincts de E ont toujours des images distinctes dans F :*

$$\forall x \in E, \forall x' \in E, \quad (x \neq x') \Rightarrow (f(x) \neq f(x')).$$

Une formulation équivalente est :

$$\forall x \in E, \forall x' \in E, \quad (f(x) = f(x')) \Rightarrow (x = x').$$

Une application injective $f : E \to F$ est appelée injection *de E* dans *F.*

Définition 1.3 (surjection)**.** *Une application $f : E \to F$ est dite* surjective *si tout élément de l'ensemble d'arrivée a au moins un antécédent par f :*

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

Une application surjective $f : E \to F$ est appelée surjection *de E* sur *F.*

3. Noter qu'ici le quantificateur « $\forall i$ » ne se traduit pas par une intersection. Ne confondez pas « $\forall i \in [\![1, n]\!],\ x \in E_i$ » qui traduit l'appartenance de x à $\bigcap_{i \in I} E_i$ avec « $\forall i \in [\![1, n]\!],\ x_i \in E_i$ ».

Définition 1.4 (bijection)**.** *Une application $f : E \to F$ est dite* bijective *si elle est à la fois injective et surjective, autrement dit si tout élément de l'ensemble d'arrivée F a un* unique *antécédent par f dans l'ensemble de départ E :*

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

Une application bijective $f : E \to F$ est appelée bijection *de E* sur *F.*

Remarque 1.5. Si $f : E \to F$ est une injection, en restreignant son ensemble d'arrivée à $f(E) := \{y \in F;\ \exists x \in E\ ;\ f(x) = y\}$ la nouvelle application $f : E \to f(E)$ est une bijection. En effet cette opération préserve clairement l'injectivité et rend f surjective.

Définition 1.6 (application réciproque)**.** *Soit $f : E \to F$ une bijection. Tout $y \in F$ admet un unique antécédent x par f dans E. En posant $f^{-1}(y) := x$, on définit une application $f^{-1} : F \to E$ appelée application réciproque de f ou inverse de f. Cette application f^{-1} est bijective.*

Justification. Pour vérifier l'injectivité de f^{-1}, soient y et y' deux éléments de F tels que $f^{-1}(y) = f^{-1}(y')$. Cela signifie qu'ils ont le même antécédent x par f, donc que $y = f(x)$ et $y' = f(x)$, d'où $y = y'$.

Pour la surjectivité, soit $x \in E$ quelconque. Posons $y = f(x)$. Alors x est antécédent de y par f, donc $f^{-1}(y) = x$ et ainsi y est antécédent de x par f^{-1}. Tout élément de E a donc un antécédent dans F par f^{-1}. Autrement dit, f^{-1} est surjective. □

Remarque 1.7. Ainsi l'existence d'une bijection $E \to F$ équivaut à celle d'une bijection $F \to E$. On dira que E « est en bijection avec » F s'il existe une bijection $E \to F$ (ou $F \to E$).

Proposition 1.8. *Soient $f : E \to F$ et $g : F \to G$ deux bijections. Alors $g \circ f$ est une bijection de E sur G. De plus $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Preuve. Rappelons que $(g \circ f)(x) := g(f(x))$ pour tout $x \in E$. Pour vérifier l'injectivité, soient x et x' dans E tels que $(g \circ f)(x) = (g \circ f)(x')$. Cette égalité réécrite $g(f(x)) = g(f(x'))$ implique par injectivité de g l'égalité $f(x) = f(x')$, laquelle implique $x = x'$ par injectivité de f. Pour la surjectivité de $g \circ f$, soit $z \in G$ quelconque. Par surjectivité de g, z a au moins un antécédent y dans F avec $g(y) = z$. À son tour $y \in F$ a un antécédent $x \in E$ par la surjection f. Finalement $y = f(x)$ et $z = g(y)$, d'où $z = g(f(x)) = (g \circ f)(x)$, ce qui montre que z a pour antécédent x par $g \circ f$. Comme z était quelconque, la surjectivité de $g \circ f$ est établie. Ainsi $g \circ f$ est une bijection de E sur G. En conservant les notations, $(g \circ f)^{-1}(z) = x$. D'autre part $x = f^{-1}(y)$ et $y = g^{-1}(z)$, d'où $x = f^{-1}(g^{-1}(z)) = (f^{-1} \circ g^{-1})(z)$. Donc pour z quelconque dans G, $(g \circ f)^{-1}(z) = x = (f^{-1} \circ g^{-1})(z)$, d'où $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

1.2 Ensembles finis et dénombrement

Définition 1.9. *Un ensemble E est dit fini s'il est vide ou s'il est en bijection avec $[\![1, n]\!]$ pour un certain entier $n \geqslant 1$. Un tel n est alors unique et est appelé* cardinal *de E (notation* $\operatorname{card} E$*). Par convention le cardinal de l'ensemble vide est* 0.

La cohérence de la définition 1.9 repose sur le lemme suivant (pourquoi ?).

Lemme 1.10. *Si n et m sont deux entiers distincts, il n'existe pas de bijection entre $[\![1, n]\!]$ et $[\![1, m]\!]$.*

Preuve. On peut toujours supposer sans perte de généralité que $0 \leqslant n < m$. Dans le cas où $n = 0$, l'ensemble $[\![1, n]\!]$ est l'ensemble des entiers j tels que $1 \leqslant j \leqslant 0$, c'est donc l'ensemble vide. On prouve le résultat par récurrence sur n en adoptant comme hypothèse de récurrence :

$$(\mathcal{H}_n) \quad \forall m > n, \quad \text{il n'existe pas de bijection } [\![1, n]\!] \to [\![1, m]\!].$$

Initialisation. $(\mathcal{H}_0)$ est clairement vraie, car on ne peut définir aucune application sur l'ensemble vide donc *a fortiori* aucune bijection.

Induction. Montrons que si $(\mathcal{H}_n)$ est vérifiée pour un certain n, alors $(\mathcal{H}_{n+1})$ l'est aussi. Pour cela on raisonne par l'absurde : si $(\mathcal{H}_{n+1})$ n'était pas pas vérifiée, il existerait un entier $m > n+1$ et une bijection $f : [\![1, n+1]\!] \to [\![1, m]\!]$. Nous allons construire à partir de f une bijection $g : [\![1, n+1]\!] \to [\![1, m]\!]$ telle que $g(n+1) = m$. Notons $j = f(n+1)$. Si $j = m$, il suffit de prendre $g = f$. Si $j \neq m$, considérons la transposition $\tau : [\![1, m]\!] \to [\![1, m]\!]$ qui échange j et m et laisse les autres éléments inchangés. C'est une bijection et l'application composée $g = \tau \circ f$ est une bijection $[\![1, n+1]\!] \to [\![1, m]\!]$ vérifiant $g(n+1) = m$.

La restriction $\tilde{g}$ de g à $[\![1, n]\!]$ est une bijection de $[\![1, n]\!]$ sur $\{1, \ldots, m-1\}$ et comme $m > n+1$, on a bien $m - 1 > n$, ce qui contredit $(\mathcal{H}_n)$. Nous venons d'établir l'implication $(\mathcal{H}_n) \Rightarrow (\mathcal{H}_{n+1})$, ce qui achève la récurrence. □

Remarque 1.11. Si l'ensemble F est en bijection avec un ensemble fini E, alors F est fini et a même cardinal que E. En effet en notant $n = \operatorname{card} E$, il existe une bijection $f : [\![1, n]\!] \to E$ et une bijection $g : E \to F$. La composée $g \circ f$ réalise alors une bijection de $[\![1, n]\!]$ sur F.

Proposition 1.12. *Soient E et F deux ensembles finis.*

$$\textit{Si } E \cap F = \varnothing, \quad \operatorname{card}(E \cup F) = \operatorname{card} E + \operatorname{card} F. \tag{1.2}$$

Preuve. Dans le cas où l'un des deux ensembles est vide, (1.2) est triviale. On suppose désormais que $\operatorname{card} E = n \geqslant 1$ et $\operatorname{card} F = m \geqslant 1$. Il existe alors des bijections

$$f : [\![1, n]\!] \to E, \quad g : [\![1, m]\!] \to F.$$

On prouve (1.2) en construisant une bijection h de $[\![1, n+m]\!]$ sur $E \cup F$. La translation

$$t : [\![n+1, n+m]\!] \to [\![1, m]\!], \quad i \mapsto i - n$$

est une bijection et l'application $g \circ t$ réalise une bijection de $[\![n+1, n+m]\!]$ sur F. Définissons alors h par

$$h(i) := \begin{cases} f(i) & \text{si } i \in [\![1, n]\!], \\ (g \circ t)(i) & \text{si } i \in [\![n+1, n+m]\!]. \end{cases}$$

Pour vérifier la surjectivité de h, soit z un élément quelconque de $E \cup F$. Si $z \in E$, alors il a un antécédent i dans $[\![1, n]\!]$ par la surjection f et comme $h(i) = f(i) = z$, i est aussi antécédent de z par h. Si $z \in F$, il a un antécédent j dans $[\![1, m]\!]$ par la surjection g et j a un antécédent i dans $[\![n+1, n+m]\!]$ par la surjection t. Alors $h(i) = g(t(i)) = g(j) = z$ donc i est antécédent de z par h.

Pour vérifier l'injectivité de h, notons i et i' deux éléments distincts de $[\![1, n+m]\!]$. S'ils sont l'un dans $[\![1, n]\!]$ et l'autre dans $[\![n+1, n+m]\!]$, leurs images $h(i)$ et $h(i')$ sont l'une dans E et l'autre dans F qui sont *disjoints* ($E \cap F = \emptyset$) donc $h(i) \neq h(i')$. Sinon i et i' sont tous deux dans $[\![1, n]\!]$ (resp. dans $[\![n+1, n+m]\!]$) et $h(i) \neq h(i')$ en raison de l'injectivité de f (resp. de $g \circ t$). □

Corollaire 1.13 (de la proposition 1.12)**.**

a) Si $E_1, \dots, E_d$ sont d ensembles finis deux à deux disjoints*, $E_1 \cup \cdots \cup E_d$ est un ensemble fini et*

$$\operatorname{card}\left(\bigcup_{i=1}^{d} E_i\right) = \sum_{i=1}^{d} \operatorname{card} E_i.$$

b) Si E et F sont des ensembles finis quelconques (pas forcément disjoints), $E \cup F$ est fini et

$$\operatorname{card}(E \cup F) = \operatorname{card} E + \operatorname{card} F - \operatorname{card}(E \cap F).$$

Preuve. Laissée en exercice. □

Proposition 1.14. *Soient E et F deux ensembles finis. Leur produit cartésien a pour cardinal*

$$\operatorname{card}(E \times F) = \operatorname{card} E \times \operatorname{card} F. \tag{1.3}$$

Preuve. Le cas où l'un des deux ensembles E ou F est vide étant trivial, on suppose désormais qu'aucun des deux n'est vide. On fait une récurrence sur $n = \operatorname{card} E$, en prenant pour hypothèse de récurrence :

$(\mathcal{H}_n)$ si $\operatorname{card} E = n$, alors $\operatorname{card}(E \times F) = n \operatorname{card} F$ pour tout F fini non vide.

Initialisation. Si $\operatorname{card} E = 1$, E n'a qu'un élément x_1 et l'application $h : \{x_1\} \times F \to F$, $(x_1, y) \mapsto y$ est clairement une bijection donc $\operatorname{card}(\{x_1\} \times F) = \operatorname{card} F$ et $(\mathcal{H}_1)$ est vérifiée.

Induction. Supposons $(\mathcal{H}_n)$ vraie pour un certain n et soit E un ensemble de cardinal $n+1$. Il existe une bijection $f : [\![1, n+1]\!] \to E$ permettant de numéroter les éléments de E en posant pour tout $i \in [\![1, n+1]\!]$, $x_i := f(i)$. La restriction de f à $[\![1, n]\!]$ est une bijection de $[\![1,n]\!]$ sur son image $E' = \{x_1, \dots, x_n\}$. Ainsi E' est de cardinal n et E est l'union de ses deux sous-ensembles disjoints E' et $\{x_{n+1}\}$. On en déduit immédiatement que $E \times F$ est l'union des deux produits cartésiens disjoints $E' \times F$ et $\{x_{n+1}\} \times F$. Par la proposition 1.12 on a alors

$$\operatorname{card}(E \times F) = \operatorname{card}(E' \times F) + \operatorname{card}(\{x_{n+1}\} \times F).$$

En utilisant $(\mathcal{H}_n)$ et $(\mathcal{H}_1)$, on obtient alors

$$\operatorname{card}(E \times F) = n \operatorname{card} F + \operatorname{card} F = (n+1) \operatorname{card} F,$$

donc $(\mathcal{H}_{n+1})$ est vérifiée. $\square$

Remarque 1.15. On aurait pu aussi prouver (1.3) en construisant explicitement une bijection $E \times F \to [\![1,nm]\!]$ (avec $\operatorname{card} E = n$ et $\operatorname{card} F = m$). Voici une façon de la construire. On note $f : [\![1,n]\!] \to E$, $i \mapsto x_i := f(i)$ et $g : [\![1,m]\!] \to F$, $j \mapsto y_j := g(j)$ des numérotations bijectives de E et F. On définit alors $h : E \times F \to [\![1,nm]\!]$ en posant $h(x_i, y_j) := m(i-1)+j$, ou de manière plus formelle $h(x,y) := m(f^{-1}(x)-1)+g^{-1}(y)$ pour tout $(x,y) \in E \times F$. On laisse en exercice la vérification de la bijectivité de h. L'idée de sa construction est simplement de ranger les couples éléments de $E \times F$ sous la forme d'un tableau où le couple (x_i, y_j) se trouve à l'intersection de la ligne i et de la colonne j et de numéroter les éléments de ce tableau en balayant chaque ligne de gauche à droite de la ligne 1 jusqu'à la ligne n.

Corollaire 1.16 (de la proposition 1.14)**.** *Si $E_1, \dots, E_d$ sont d ensembles finis,*

$$\operatorname{card}(E_1 \times \cdots \times E_d) = \prod_{i=1}^{d} \operatorname{card} E_i.$$

Preuve. Une récurrence immédiate sur d fournit le résultat. $\square$

Proposition 1.17 (nombre d'applications $E \to F$ et cardinal de $\mathcal{P}(E)$)**.**

(a) Si $\operatorname{card} E = n$ et $\operatorname{card} F = p$, l'ensemble F^E des applications de E dans F est fini et a pour cardinal p^n, autrement dit :

$$\operatorname{card}\bigl(F^E\bigr) = (\operatorname{card} F)^{\operatorname{card} E}.$$

(b) Comme $\mathcal{P}(E)$ est en bijection avec l'ensemble $\{0,1\}^E$ des applications de E dans $\{0,1\}$,

$$\operatorname{card} \mathcal{P}(E) = 2^n = 2^{\operatorname{card} E}.$$

Preuve. Le (a) se démontre facilement par récurrence sur le cardinal de E, en notant que si on ajoute un élément x_{n+1} à E, il y a p façons différentes de prolonger $f : E \to F$ en attribuant comme image à x_{n+1} l'un des éléments de F. La rédaction détaillée est laissée en exercice.

Une bijection naturelle entre $\mathcal{P}(E)$ et $\{0,1\}^E$ est l'application φ qui à toute partie A de E associe sa fonction *indicatrice* :

$$\varphi : \mathcal{P}(E) \to \{0,1\}^E \qquad A \mapsto \varphi(A) := \mathbf{1}_A.$$

Rappelons que l'indicatrice d'une partie A de E est l'application

$$\mathbf{1}_A : E \to \{0,1\} \qquad \omega \mapsto \mathbf{1}_A(\omega) := \begin{cases} 1 & \text{si } \omega \in A, \\ 0 & \text{si } \omega \notin A. \end{cases}$$

La vérification de la bijectivité de φ est laissée en exercice [4]. □

Définition 1.18 (arrangement)**.** *Si E est un ensemble de cardinal n et $k \in [\![1,n]\!]$, on appelle* arrangement *de k éléments de E tout k-uplet $(x_1, x_2, \dots, x_k)$ d'éléments* tous distincts *de E.*

Proposition 1.19 (dénombrement des arrangements)**.** *Le nombre d'arrangements de k éléments de E ($1 \leqslant k \leqslant n = \operatorname{card} E$) est*

$$A_n^k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}. \tag{1.4}$$

A_n^k est aussi le nombre d'injections d'un ensemble I de cardinal k, par exemple $[\![1,k]\!]$, dans E. En particulier pour $I = E$ (et donc $k = n$), on obtient le nombre de bijections de E dans lui même (appelées aussi permutations *de E) :*

$$\text{nombre de permutations de } E = A_n^n = n!$$

Preuve. On prouve (1.4) par récurrence finie sur k, le cas $k = 1$ étant évident. Supposons donc (1.4) vraie pour un $k < n$ et montrons qu'alors elle est aussi vraie pour $k+1$. Un arrangement $(x_1, \dots, x_{k+1})$ de $k+1$ éléments de E est déterminé de manière unique par le choix de l'arrangement $(x_1, \dots, x_k)$ de k éléments de E et le choix de l'élément $x_{k+1} \in E \setminus \{x_1, \dots, x_k\}$. Cela laisse donc $n-k$ choix possibles pour x_{k+1}, d'où

$$A_n^{k+1} = A_n^k(n-k) = n(n-1)(n-2)\cdots(n-k+1)(n-k),$$

ce qui montre que (1.4) est vérifiée au rang $k+1$.

Rappelons qu'un k-uplet $(x_1, \dots, x_k)$ de E^k peut être vu comme l'application $f : [\![1,k]\!] \to E$, $i \mapsto f(i) = x_i$. Cette représentation définit une bijection φ entre l'ensemble des applications $f : [\![1,k]\!] \to E$, autrement dit $E^{[\![1,k]\!]}$ et l'ensemble E^k des k-uplets de E. Dans la représentation ci-dessus, f est injective si et seulement si les x_i sont tous distincts. Donc l'image par φ de l'ensemble des applications injectives $[\![1,k]\!] \to E$ est exactement l'ensemble des k-uplets de E qui sont des arrangements. Ces deux ensembles ont donc même cardinal et A_n^k est bien le nombre d'injections de $[\![1,k]\!] \to E$. Soit maintenant I un ensemble de cardinal k et fixons une bijection

4. Ni la définition de φ, ni la preuve de sa bijectivité n'utilisent la finitude de E. Ainsi $\mathcal{P}(E)$ et $\{0,1\}^E$ sont en bijection quel que soit l'ensemble $E \neq \varnothing$, fini ou infini.