Table des matières

I Entiers naturels

I.1 Les propriétés admises de l'ensemble $\mathbb{N}$

Conformément au programme, l'ensemble $\mathbb{N} = \{0, 1, 2, \ldots\}$ est supposé connu, ainsi que ses propriétés (opérations $+$ et $\times$, relation d'ordre). Voici quelques-unes de ces propriétés.

- **Addition**
  - L'opération $+$ est *associative* : $\forall (m, n, p) \in \mathbb{N}^3, m + (n + p) = (m + n) + p$.
  - Elle est $+$ est *commutative* : $\forall (m, n) \in \mathbb{N}^2, m + n = n + m$.
  - 0 est *élément neutre* : $\forall n \in \mathbb{N}, n + 0 = n$.
    On note $\mathbb{N}^*$ l'ensemble $\mathbb{N}$ privé de 0.
  - Tout élément de $\mathbb{N}$ est *simplifiable pour l'addition* :
    $\forall (m, n, p) \in \mathbb{N}^3, m + p = n + p \Rightarrow m = n$.
  - $\forall (m, n) \in \mathbb{N}^2, m + n = 0 \Leftrightarrow m = n = 0$.

- **Multiplication**
  - L'opération $\times$ est associative : $\forall (m, n, p) \in \mathbb{N}^3, m(np) = (mn)p$.
  - Elle est commutative : $\forall (m, n) \in \mathbb{N}^2, mn = nm$.
  - Elle est *distributive* par rapport à la loi $+$: $\forall (m, n, p) \in \mathbb{N}^3, m(n + p) = mp + mp$.
  - 1 est élément neutre : $\forall n \in \mathbb{N},\ n1 = n$.
  - Tout élément *non nul* de $\mathbb{N}$ est simplifiable pour le produit :
    $\forall (m, n) \in \mathbb{N}^2, \forall p \in \mathbb{N}^*, mp = np \Rightarrow m = n$.

- **Relation d'ordre**

  On pose : $\forall (m, n) \in \mathbb{N}^2,\ m \leqslant n \Leftrightarrow \exists p \in \mathbb{N},\ m + p = n$.
  - C'est une relation d'*ordre total* sur $\mathbb{N}$ (ça signifie que deux éléments m et n de $\mathbb{N}$ sont toujours *comparables* : on a toujours $m \leqslant n$ ou $n \leqslant m$)
  - L'entier 0 est le minimum de $\mathbb{N}$ pour cette relation d'ordre.

    ▶ *Démonstration:*

    Cela résulte évidemment de l'égalité $0 + n = n$, valable pour tout n de $\mathbb{N}$ ◀
  - Pour tous entiers m, n, p, si $m \leqslant n$ alors $\begin{cases} m + p \leqslant n + p \\ mp \leqslant np \end{cases}$

Remarques

- Si $m \leqslant n$, l'entier p tel que $m + p = n$ est noté $n - m$.
  L'opération différence n'est pas partout définie sur $\mathbb{N}$ (l'entier p n'existe que si $m \leqslant n$) et n'est pas très "intéressante" (pas commutative, ni associative, pas d'élément neutre).
- On note indifféremment $n \geqslant m$ et $m \leqslant n$ (mais plus souvent $m \leqslant n$).
  On note $m < n$ pour écrire : $(m \leqslant n)$ et $(m \neq n)$.
  Soit (m, n) dans $\mathbb{N}^2$. On pose : $[\![m, n]\!] = \{p \in \mathbb{N}, m \leqslant p \leqslant n\}$ (ensemble vide si $n < m$).
- On $mn = 1 \Leftrightarrow m = n = 1$, et on a $mn = 0 \Leftrightarrow (m = 0)$ ou $(n = 0)$.

– Si $a_m, a_{m+1}, \ldots, a_n$ sont dans $\mathbb{N}$, on notera $\sum_{j=m}^{n} a_j$, ou $\prod_{m\leqslant j\leqslant n} a_j$, plutôt que $a_m + a_{m+1} + \ldots + a_n$.
De même on notera $\prod_{j=m}^{n} a_j$, ou $\prod_{m\leqslant j\leqslant n} a_j$ plutôt que $a_m a_{m+1} \ldots a_n$.
Par convention, dans le cas où $n < m$ on pose $\sum_{j=m}^{n} a_j = 0$ et $\prod_{j=m}^{n} a_j = 1$.

Factorielle

Pour tout n de $\mathbb{N}$, on note $n! = \prod_{k=1}^{n} k$ (et en particulier $0! = 1$)

Puissances d'un entier

Pour tous m, n de $\mathbb{N}$, on pose $m^n = \prod_{j=1}^{n} m$ (et en particulier $m^0 = 1$).

On a alors les propriétés suivantes : $m^n\, m^p = m^{n+p}$, $(m^n)^p = m^{np}$, $(mn)^p = m^p\, n^p$.

I.2 Le principe de récurrence

Dans $\mathbb{N}$, on admet en particulier la propriété fondamentale :

Toute partie non vide de $\mathbb{N}$ possède un plus petit élément

Remarques et exemples

– Soit n dans $\mathbb{N}$. L'ensemble $A = \{m \in \mathbb{N},\ m > n\}$ est non vide.
Le plus petit élément de A est bien sûr $n+1$ (c'est le *successeur* de n).
Autrement dit, pour tout n de $\mathbb{N}$, on a : $m > n \iff m \geqslant n+1$.

– Soit n dans $\mathbb{N}^*$. L'ensemble A des m de $\mathbb{N}$ tel que $m < n$ est non vide (il contient 0).
Le plus grand élément de cet ensemble est bien sûr $n-1$ (c'est le *prédécesseur* de n).
Autrement dit, pour tout n de $\mathbb{N}$, on a : $m < n \iff m \leqslant n-1$.

La propriété "du plus petit élément" possède deux corollaires très importants :

Principe de récurrence

Soit A une partie de $\mathbb{N}$, contenant 0. On suppose que : $\forall\, n \in A,\ n+1 \in A$. Alors $A = \mathbb{N}$.

Autrement dit, si une partie A de $\mathbb{N}$ contient 0 et si elle contient le successeur de chacun de ses éléments, alors cette partie A est égale à $\mathbb{N}$ tout entier.

▶ *Démonstration:*

On raisonne par l'absurde, donc on suppose que le complémentaire B de A dans $\mathbb{N}$ n'est pas vide.
Soit b le plus petit élément de B (on utilise l'axiome du plus petit élément).
On trouve $b \geqslant 1$ (car 0 est dans A, donc pas dans B, et b est dans B).
On peut donc parler de l'entier $a = b-1$, et a est dans A.
Par hypothèse sur A, on en déduit que $b = a+1$ est dans A, et c'est absurde.

Plus grand élément d'une partie non vide majorée

Toute partie majorée non vide de $\mathbb{N}$ possède un plus grand élément

► *Démonstration:*

Soit A une partie majorée non vide de $\mathbb{N}$. Soit B l'ensemble des majorants de A.
L'ensemble B est une partie non vide de $\mathbb{N}$ donc possède un plus petit élément b.
Pour tout élément a de A, on a l'inégalité $a \leqslant b$.
Si $b = 0$, alors nécessairement $A = \{0\}$ et A possède bien un plus grand élément...
On suppose donc $b > 0$. Par définition de b, l'entier $b-1$ n'est pas dans B.
Il existe donc un élément a de A tel que $b - 1 < a$.
On a alors $b - 1 < a \leqslant b$, ce qui implique $b = a$: l'entier b est donc dans A.
Ainsi b est un majorant de A qui appartient à A : c'est l'élément maximum de A ◄

I.3 Division euclidienne

Définition

On dit que n *divise* m (ou que m est un *multiple* de n) si : $\exists\, q \in \mathbb{N}, m = nq$.
On note alors $n \mid m$. On définit ainsi une relation d'ordre partiel sur $\mathbb{N}$.
Pour cette relation, 1 est le minimum de $\mathbb{N}$.

► *Démonstration:*

Pour tout entier n, on a $n = n \cdot 1$ donc $\begin{cases} n \mid n & \text{(la relation est réflexive)} \\ 1 \mid n & \text{(l'entier 1 est minimum)} \end{cases}$
La relation est transitive car $\begin{cases} n \mid n' \\ n' \mid n'' \end{cases} \Rightarrow \begin{cases} n' = nq \\ n'' = n'q' \end{cases} \Rightarrow n'' = n(qq') \Rightarrow n \mid n''.$
$\begin{cases} n \mid m \\ m \mid n \end{cases} \Rightarrow \begin{cases} m = nq \\ n = mp \end{cases} \Rightarrow n = n(qp) \Rightarrow \begin{cases} n = 0 \text{ ou} \\ pq = 1 \end{cases} \Rightarrow \begin{cases} m = n = 0 \text{ ou} \\ p = q = 1 \end{cases} \Rightarrow m = n$
C'est un ordre partiel car par exemple 2 et 3 ne sont pas comparables ◄

Définition

Soit (m, n) dans $\mathbb{N} \times \mathbb{N}^*$.
Il existe un unique couple (q, r) de $\mathbb{N}^2$ tel que : $(m = nq + r)$ et $(r \leqslant n - 1)$
Le passage du couple (m, n) au couple (q, r) s'appelle *division euclidienne* de m par n.
Dans cette division, m est le *dividende*, n le *diviseur*, q le *quotient*, et r le *reste*.

► *Démonstration:*

Soit A le sous-ensemble de $\mathbb{N}^*$ formé des entiers k tels que $m < kn$.
Notons que $k = m + 1$ convient toujours car $(m+1)n - m = m(n-1) + n \geqslant n \geqslant 1$.
L'ensemble A étant non vide, il a un minimum $q' \geqslant 1$. Notons $q' = q + 1$ $(q \in \mathbb{N})$.
Par définition $\begin{cases} q \notin A \\ q + 1 \in A \end{cases}$ *c'est-à-dire* $\begin{cases} qn \leqslant m \\ m < (q+1)n \end{cases}$
Ainsi $r = m - nq$ est un entier naturel strictement inférieur à n.
On a donc trouvé un couple $(q, r) \in \mathbb{N}^2$ tel que $m = nq + r$, avec $r \leqslant n - 1$.
Supposons alors qu'on ait aussi $m = nq' + r'$, avec $(q', r') \in \mathbb{N}^2$ et $r' \leqslant n - 1$.
On doit montrer que les couples (q, r) et (q', r') sont égaux.
Sans perdre de généralité, on peut supposer $q' \geqslant q$.
Par différence on trouve $n(q' - q) = r - r' \leqslant r < n$. La seule possibilité est $q' - q = 0$.
On trouve donc $q' = q$, puis $r' = r$. Le couple (q, r) obtenu plus haut est donc unique ◄

Remarque

$n \mid m \Leftrightarrow (m = n = 0)$ ou ($n \neq 0$ et le reste dans la division de m par n est nul).

I.4 Raisonnement par récurrence

Soit $\mathcal{P}$ un prédicat, de référentiel $\mathbb{N}$.

Rappelons qu'on écrit $\mathcal{P}(n)$ pour dire "$\mathcal{P}(n)$ est vraie".

Récurrence simple (ou faible)

$\left\{\begin{array}{l}\text{On suppose } \mathcal{P}(0) \text{ et, pour tout entier } n,\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1).\\ \text{Alors, pour tout entier } n,\ \mathcal{P}(n).\end{array}\right.$

▶ *Démonstration:*

Notons A l'ensemble des entiers n de $\mathbb{N}$ pour lesquels $\mathcal{P}(n)$ est vraie.
Les deux hypothèses signifient que 0 est dans A et que : $\forall n \in A,\ n+1 \in A$.
L'axiome de récurrence donne $A = \mathbb{N}$: la propriété $\mathcal{P}$ est donc vraie pour tout n de $\mathbb{N}$ ◀

Voici donc comment montrer qu'une propriété $\mathcal{P}(n)$ est vraie pour tous les entiers naturels :

- On vérifie que l'entier 0 satisfait à la propriété : c'est le *pas initial* de la récurrence.
- On se **donne** ensuite un entier n, pour lequel on suppose que $\mathcal{P}(n)$ est vraie.
  C'est l'*hypothèse de récurrence*.
- On démontre alors que $\mathcal{P}(n+1)$ est vraie (c'est le "*passage du rang n au rang $n+1$*").
  On exprime l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ en disant que la propriété $\mathcal{P}$ est *héréditaire*.
- On conclut en annonçant que, par récurrence, la propriété est vraie pour tout entier n.

I.5 Pratique du raisonnement par récurrence

Le raisonnement de récurrence admet plusieurs variantes, dont celle-ci, qui ne diffère de l'original que par le "pas initial" qui peut se situer en n_0 (entier naturel) plutôt qu'en 0 :

Soit n_0 un entier naturel.

$\left\{\begin{array}{l}\text{On suppose } \mathcal{P}(n_0).\\ \text{On suppose également que : } \forall\, n \geqslant n_0,\ \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1).\\ \text{Alors, } \forall\, n \geqslant n_0,\ \mathcal{P}(n).\end{array}\right.$

Une autre variante réside dans la manière d'avancer dans la récurrence.

Il arrive en effet que l'hypothèse $\mathcal{P}(n)$ seule soit insuffisante pour démontrer $\mathcal{P}(n+1)$.

Le cas le plus fréquent est celui de la *récurrence double*, où le pas initial et l'hypothèse de récurrence portent sur deux entiers consécutifs.

Récurrence de pas double

Soit n_0 un entier naturel.

$\left\{\begin{array}{l}\text{On suppose } \mathcal{P}(n_0) \text{ et } \mathcal{P}(n_0+1).\\ \text{On suppose également que : } \forall\, n \geqslant n_0,\ (\mathcal{P}(n) \text{ et } \mathcal{P}(n+1)) \Rightarrow \mathcal{P}(n+2).\\ \text{Alors, } \forall\, n \geqslant n_0,\ \mathcal{P}(n).\end{array}\right.$

Il reste à voir une dernière version du raisonnement par récurrence. Pour démontrer $\mathcal{P}(n+1)$, on peut en effet utiliser tout ou partie des hypothèses $\mathcal{P}(n_0)$, $\mathcal{P}(n_0+1)$, …, et $\mathcal{P}(n)$.

Récurrence forte

$\left\{\begin{array}{l}\text{Soit } n_0 \text{ un entier naturel. On suppose } \mathcal{P}(n_0).\\ \text{On suppose aussi que : } \forall\, n \geqslant n_0,\ (\mathcal{P}(n_0), \mathcal{P}(n_0+1), \ldots, \mathcal{P}(n)) \Rightarrow \mathcal{P}(n+1).\\ \text{Alors, } \forall\, n \geqslant n_0, \mathcal{P}(n).\end{array}\right.$

Voici enfin quelques conseils pour "réussir" un raisonnement par récurrence :

- Ne pas oublier le "pas initial" (la propriété est souvent triviale, mais on **doit** la prouver).
- Ne pas écrire : "Supposons que pour **tout** n, $\mathcal{P}(n)$. Montrons $\mathcal{P}(n+1)$" alors qu'il faut écrire : "**Soit** n un entier naturel ; on suppose $\mathcal{P}(n)$. Montrons $\mathcal{P}(n+1)$".
- Bien articuler le pas initial et l'hypothèse de récurrence.
  Si le pas initial est par exemple n_0, et si on veut démontrer $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$, alors n doit être supérieur ou égal à n_0. On peut tout à fait prouver $\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$, mais dans ce cas n doit être strictement supérieur à n_0.
- Bien séparer le "passage du rang n au rang $n+1$", où l'entier n est **fixé**, et la conclusion finale (qui est obligatoire, et qui doit porter sur **tous** les entiers naturels n).

II Ensembles finis

II.1 Cardinal d'un ensemble fini

Pour tout entier naturel, on note $E_n = \{m \in \mathbb{N}, 1 \leqslant m \leqslant n\}$. En particulier $E_0 = \emptyset$.

Dans les trois énoncés suivants, n et p sont des entiers naturels.

Proposition

Il existe une *injection* de E_n dans E_p si et seulement si $n \leqslant p$.
Il existe une *surjection* de E_n sur E_p si et seulement si $n \geqslant p$.
Il existe une *bijection* de E_n sur E_p si et seulement si $n = p$.

- ▶ *Démonstration:*

  Si $n \leqslant p$, on définit une injection f de E_n dans E_p en posant : $\forall\, k \in E_n, f(k) = k$.
  Réciproquement, prouvons que l'existence d'une injection de E_n dans E_p implique $n \leqslant p$.
  On va le montrer par récurrence sur n. Si $n = 1$ c'est évident puisque par hypothèse $1 \leqslant p$.
  Soit n dans $\mathbb{N}^*$. Supposons la propriété démontrée "au rang n".
  On suppose alors qu'il existe une injection $f : E_{n+1} \to E_p$: il faut prouver $n+1 \leqslant p$.
  Tout d'abord $p > 1$, sinon f ne serait pas injective (on aurait $f(1) = f(2) = 1$.)
  Si $f(n+1) < p$, soit g la bijection de E_p sur lui-même qui échange $f(n+1)$ et p en laissant fixe tous les autres. Si au contraire $f(n+1) = p$, soit g l'application identité de E_p.
  Par construction $h = g \circ f$ est une injection de E_{n+1} dans E_p telle que $h(n+1) = p$.
  Sa restriction à E_n est donc une injection de E_n dans E_{p-1}.
  L'hypothèse de récurrence nous donne alors $n \leqslant p-1$ donc $n+1 \leqslant p$.
  On a ainsi prouvé la propriété au rang $n+1$, ce qui achève la récurrence ◀

– ▶ *Démonstration:*

Si $n \geqslant p$, l'application $f : E_n \to E_p$ définie par $f(k) = \min(k, p)$ est surjective.
Réciproquement supposons qu'il existe une surjection f de E_n sur E_p.
On définit alors une application g de E_p dans E_n en associant à tout j de E_p l'un quelconque (il y en a toujours au moins un) des éléments k de E_n tels que $f(k) = j$.
Par construction, l'application $f \circ g$ est l'identité de E_p.
Puisque $f \circ g$ est injective, il en est de même de g.
L'existence d'une injection g de E_p dans E_n implique donc $p \leqslant n$ (proposition précédente.) ◀

– ▶ *Démonstration:*

Si $n = p$, l'application identité est une bijection de E_n sur E_p.
Réciproquement c'est une simple conséquence des deux propriétés précédentes ◀

Proposition

Soit n un entier naturel non nul, et f une application de E_n dans lui-même.
Alors : f est bijective $\Leftrightarrow$ f est injective $\Leftrightarrow$ f est surjective.

▶ *Démonstration:*

Il suffit de vérifier l'équivalence entre "f injective" et "f surjective".

◇ *Soit f une injection de E_n dans lui-même.*

Supposons par l'absurde que f ne soit pas surjective.

Alors il existe k de E_n qui ne possède pas d'antécédent par f.

On remarque que cette situation implique nécessairement $n \geqslant 2$.

Si $k < n$, on note g la bijection de E_n sur lui-même qui échange k et n et laisse fixe tous les autres. Si $k = n$, on prend pour g l'identité de E_n.

Par construction $g \circ f$ est une injection de E_n dans E_{n-1}, ce qui est absurde.

Conclusion : si f est injective de E_n dans lui-même, alors elle est bijective.

◇ *Soit f une surjection de E_n sur lui-même.*

On définit une application g de E_n dans lui-même en associant à tout j de E_n l'un quelconque (il y en a toujours au moins un) des éléments k de E_n tels que $f(k) = j$.

Par construction, l'application $f \circ g$ est l'identité de E_n.

Puisque $f \circ g$ est injective, il en est de même de g.

La démonstration précédente nous apprend alors que g est bijective.

Puisque $f \circ g$ est l'identité de E_n, il en découle $f = g^{-1}$. L'application f est donc bijective.

Conclusion : si f est surjective de E_n sur lui-même, alors elle est bijective ◀

On peut maintenant donner la définition d'un ensemble fini.

Proposition

Un ensemble non vide E est dit *fini* s'il existe une bijection de E_n sur E, avec $n \geqslant 0$.
L'entier n, s'il existe, est unique et est appelé le *cardinal* de E. On note $n = \text{card}\,(E)$.
En particulier $\text{card}\,(\emptyset) = 0$. Un ensemble non fini est dit *infini*.

▶ *Démonstration:*

L'unicité de l'entier n résulte du fait que s'il existe une bijection f de E_n sur E et une bijection g de E_p sur E alors $g^{-1} \circ f$ est une bijection de E_n sur E_p, ce qui implique $n = p$ ◀

Remarques

- $\text{card}\,(E)$ représente bien sûr le "nombre d'éléments" de E.
- Dans la définition, on aurait pu aussi bien dire : "s'il existe une bijection de E sur E_n"
- Si $m \leqslant n$, l'intervalle $[\![m, n]\!]$ est fini de cardinal $n - m + 1$. En effet l'application f définie par $f(k) = k - m + 1$ est bijective de $[\![m, n]\!]$ sur E_{n-m+1}.
- S'il existe une bijection f de E fini sur F, alors F est fini et $\text{card}\,(E) = \text{card}\,(F)$.

  ▶ *Démonstration:*

  Si $E = \emptyset$ alors $F = \emptyset$. Sinon, soit g une bijection de E_n sur E, avec $n = \text{card}\,(E) \geqslant 1$.
  Alors $f \circ g$ est une bijection de E_n sur F. L'ensemble F est donc fini de cardinal n ◀

On peut caractériser les parties finies de $\mathbb{N}$:

Proposition

Une partie A non vide de $\mathbb{N}$ est finie $\Leftrightarrow$ elle est majorée. En particulier $\mathbb{N}$ est infini.

▶ *Démonstration:*

◇ *Montrons par récurrence que toute partie A de $\mathbb{N}$, de cardinal $n \geqslant 1$, est majorée.*
Si $n = 1$: A qui est en bijection avec $E_1 = \{1\}$ et est donc un singleton est majoré...
Supposons la propriété vraie pour un entier $n \geqslant 1$ donné, et soit $A \subset \mathbb{N}$ de cardinal $n + 1$.
Soit f une bijection de E_{n+1} sur A, et soit $a = f(n + 1)$.
La restriction de f à E_n est une bijection de E_n sur $B = A \setminus \{a\}$.
L'ensemble B est de cardinal n donc majoré. Soit m un majorant de B.
Pour tout x de A, on a $x \leqslant \max(a, m)$. Donc A est majoré, ce qui achève la récurrence.

◇ *Montrons par récurrence sur n que si $A \subset [\![0, n]\!]$, alors A est fini et $\text{card}\,(A) \leqslant n + 1$.*
Si $n = 0$, alors $A = \{0\}$. Donc A est fini et $\text{card}\,(A) = 1$.
Supposons la propriété vraie pour $n \geqslant 0$ donné. Soit A une partie de $[\![0, n + 1]\!]$.
Il faut montrer que A est finie et que $\text{card}\,(A) \leqslant n + 2$.
Si $A \subset [\![0, n]\!]$, on applique l'hypothèse de récurrence : $\text{card}\,(A) \leqslant n + 1 \leqslant n + 2$.
Sinon $n + 1$ est dans A. Si $A = \{n + 1\}$, il est fini de cardinal $1 \leqslant n + 2$...
Sinon l'ensemble $B = A \setminus \{n + 1\}$ est non vide et inclus dans $[\![0, n]\!]$.
Cet ensemble est donc fini et $\text{card}\,(B) = p \leqslant n + 1$. Soit f une bijection E_p sur B.
On prolonge f en une bijection g de E_{p+1} sur A en posant $f(p + 1) = n + 1$.
Il en résulte que A est fini avec $\text{card}\,(A) = p + 1 \leqslant n + 2$, ce qui achève la récurrence.

◇ *$\mathbb{N}$ est infini car non majoré (conséquence de l'existence de l'application "succession")* ◀

On en déduit le résultat suivant :

Proposition

Soit E un ensemble fini. Soit A une partie de E.
Alors A est un ensemble fini et $\text{card}\,(A) \leqslant \text{card}\,(E)$.
Plus précisément, on a $\text{card}\,(A) = \text{card}\,(E)$ si et seulement si $A = E$.

► *Démonstration:*

◇ *Soit A une partie de l'ensemble fini E. Si $A = \emptyset$, il est fini et $\text{card}(A) \leqslant \text{card}(E)$...*
On suppose donc A non vide. Soit $n = \text{card}(E) \geqslant 1$ et f une bijection de E sur E_n.
L'application $g : k \mapsto g(k) = f(k) - 1$ est bijective de E dans $[\![0, n-1]\!]$.
Elle induit donc une bijection de A sur une partie non vide $B = f(A)$ de $[\![0, n-1]\!]$.
La proposition précédente nous apprend que B est finie, et que $\text{card}(B) \leqslant n$.
Or il y a une bijection de A sur B. Donc A est fini et $\text{card}(A) = \text{card}(B) \leqslant \text{card}(E)$.

◇ *Soit $A \subset E$, avec E fini et $\text{card}(A) = \text{card}(E)$. Il faut montrer que $A = E$.*
Si A est vide, alors $\text{card}(E) = \text{card}(A) = 0$: l'ensemble E est vide également.
Sinon soient $n = \text{card}(A) = \text{card}(E) \geqslant 1$, $f : E_n \to A$ et $g : E \to E_n$ deux bijections.
Soit φ l'injection canonique de A dans E, définie par $\varphi(a) = a$ pour tout a de A.
L'application $\psi = g \circ \varphi \circ f$ est une injection de E_n dans lui-même.
On sait que cela implique que l'application ψ est bijective.
On en déduit que $\varphi = g^{-1} \circ \psi \circ f^{-1}$ est bijective et en particulier surjective.
Autrement dit tout élément de E est un élément de A. On a donc l'égalité $A = E$ ◄

Remarque

Si E est infini, il peut exister des bijections de E sur une partie stricte de E.

Par exemple, l'application $n \mapsto 2n$ est une bijection de $\mathbb{N}$ sur l'ensemble des entiers pairs, et la succession $n \mapsto n+1$ est une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$.

Les deux propositions suivantes peuvent permettre de montrer qu'un ensemble est fini.

Proposition

Soit E un ensemble fini. Soit F un ensemble quelconque.
Soit f une application surjective de E sur F.
Alors F est fini, et $\text{card}(F) \leqslant \text{card}(E)$.
De plus on a $\text{card}(F) = \text{card}(E) \Leftrightarrow f$ est bijective.

► *Démonstration:*

◇ *On définit une application g de F vers E en associant à tout y de F l'un quelconque (il en existe toujours au moins un) des éléments x de E tels que $f(x) = y$.*
Par construction, l'application $f \circ g$ est l'identité de F. En particulier g est injective.
L'application g réalise donc une bijection de F sur son image $A = g(F)$.
Puisque A est une partie de E, A est finie et $\text{card}(A) \leqslant \text{card}(E)$.
La bijection entre A et F montre que F est fini et $\text{card}(F) = \text{card}(A) \leqslant \text{card}(E)$.

◇ *Si f est injective, c'est une bijection de E sur F. Donc $\text{card}(F) = \text{card}(E)$.*
Inversement : $\text{card}(F) = \text{card}(E) \Rightarrow \text{card}(A) = \text{card}(E)$ (notations précédentes.)
Or $A \subset E$. Il en découle $A = E$. Mais par construction deux éléments distincts de A ont des images distinctes par f. Il en découle que f est injective ◄

Proposition

Soient E et F deux ensembles.
Soit f une application injective de E dans F.
Si $f(E)$ est fini, alors E est fini et $\text{card}(E) = \text{card}(f(E))$.

► *Démonstration:*

C'est évident puisque f réalise une bijection de E sur $f(E)$ ◄

Voici des résultats très proches des précédents. Il s'agit plutôt ici de caractériser l'existence d'applications injectives, surjectives ou bijectives entre deux ensembles dont l'un est fini.

Proposition

Soient E et F deux ensembles non vides, l'ensemble F étant fini.
Il existe une injection de E dans $F \Leftrightarrow (E$ est fini et $\text{card}\,(E) \leqslant \text{card}\,(F))$.

► *Démonstration:*

◇ *Soit f une injection de E dans F. L'ensemble $f(E)$ est une partie de l'ensemble fini F.*
Ainsi $f(E)$ est fini, puis E lui-même car f est injective (proposition précédente.)
On a enfin $\text{card}\,(E) = \text{card}\,(f(E)) \leqslant \text{card}\,(F)$.

◇ *Réciproquement, on suppose $n \leqslant m$, avec $n = \text{card}\,(E)$ et $m = \text{card}\,(F)$.*
Puisque $n \leqslant m$, on sait qu'il existe une injection f de E_n dans E_m.
Soit g une bijection de E sur E_n, et h une bijection de E_m sur F.
Alors $h \circ f \circ g$ est une injection de E dans F ◄

Proposition

Soient E et F deux ensembles non vides, l'ensemble E étant fini.
Il existe une surjection de E sur $F \Leftrightarrow (F$ est fini et $\text{card}\,(F) \leqslant \text{card}\,(E))$.
Il existe une bijection de E sur $F \Leftrightarrow (F$ est fini et $\text{card}\,(E) = \text{card}\,(F))$.

► *Démonstration:*

◇ *Pour la première propriété, le sens direct a déjà été vu.*
Réciproquement, on suppose $m \leqslant n$, avec $m = \text{card}\,(F)$ et $n = \text{card}\,(E)$.
Puisque $n \geqslant m$, on sait qu'il existe une surjection f de E_n dans E_m.
Soit g une bijection de E sur E_n, et h une bijection de E_m sur F.
Alors $h \circ f \circ g$ est une surjection de E dans F.

◇ *On sait que si E est fini et si $f : E \to F$ est bijective, alors F est fini et $\text{card}\,(E) = \text{card}\,(F)$.*
Réciproquement, si F est fini et si $\text{card}\,(F) = \text{card}\,(E) = n \geqslant 1$, il existe une bijection f de E sur E_n et une bijection g de E_n sur F : $g \circ f$ est alors une bijection de E sur F ◄

Proposition

Soient E et F deux ensembles finis non vides de même cardinal.
Soit f une application de E vers F.
f est bijective $\Leftrightarrow$ f est injective $\Leftrightarrow$ f est surjective.

► *Démonstration:*

On pose $n = \text{card}\,(E)$. On utilise la proposition analogue avec E_n à la place de E et F.
On sait qu'il existe une bijection g de E_n sur E et une bijection h de F sur E_n.
Si f est injective alors $\varphi = h \circ f \circ g$ est injective de E_n dans lui-même.
On en déduit que φ est bijective, ainsi donc que $f = h^{-1} \circ \varphi \circ g^{-1}$.
C'est la même démonstration si on suppose au départ que f est surjective ◄

II.2 Propriétés des cardinaux

On voit ici comment calculer le cardinal d'ensembles construits à partir d'ensembles finis.

Proposition *(Réunion d'ensembles finis disjoints)*

Si E et F sont finis disjoints, alors $E \cup F$ est fini et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$.

Si $E_1, \dots, E_n$ sont finis disjoints deux à deux, $\bigcup_{i=1}^{n} E_i$ est fini et $\text{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \text{card}(E_i)$.

▶ *Démonstration:*

Soient E et F deux ensembles finis disjoints.
Si l'un d'eux est vide, alors $E \cup F$ est fini et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F)$.
On suppose donc $\text{card}(E) = n \geqslant 1$ et $\text{card}(F) = m \geqslant 1$.
Soit f une bijection de E sur E_n et g une bijection de F sur E_m.
On définit alors $h : E \cup F \to E_{m+n}$ par $\begin{cases} \forall x \in E,\ h(x) = f(x) \\ \forall x \in F,\ h(x) = n + g(x) \end{cases}$
Il est clair que h est bijective, avec : $\begin{cases} \forall k \in \{1, \dots, n\},\ h^{-1}(k) = f^{-1}(k) \\ \forall k \in \{n+1, \dots, n+m\},\ h^{-1}(k) = g^{-1}(k-n) \end{cases}$
Donc $E \cup F$ est fini et $\text{card}(E \cup F) = n + m = \text{card}(E) + \text{card}(F)$.
Par récurrence, on généralise à n ensembles $E_1, E_2, \dots, E_n$, finis et disjoints deux à deux ◀

Proposition *(Réunion de deux ensembles finis)*

Si E et F sont finis, alors $E \cup F$ est fini et $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$.

En particulier : $\text{card}(E \cup F) \leqslant \text{card}(E) + \text{card}(F)$, avec égalité $\Leftrightarrow E \cap F = \emptyset$.

▶ *Démonstration:*

L'ensemble $E \setminus F$ est fini car inclus dans E. On a l'union disjointe $E = (E \setminus F) \cup (E \cap F)$.
On en déduit $\text{card}(E) = \text{card}(E \setminus F) + \text{card}(E \cap F)$.
De même, on a l'union disjointe $E \cup F = (E \setminus F) \cup F$.
Ainsi : $\text{card}(E \cup F) = \text{card}(E \setminus F) + \text{card}(F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F)$.
Enfin : $\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) \Leftrightarrow \text{card}(E \cap F) = 0 \Leftrightarrow E \cap F = \emptyset$ ◀

Proposition *(Généralisation à n ensembles finis)*

Si $E_1, E_2, \dots, E_n$ sont finis, alors $\bigcup_{i=1}^{n} E_i$ est fini et $\text{card}\left(\bigcup_{i=1}^{n} E_i\right) \leqslant \sum_{i=1}^{n} \text{card}(E_i)$.

On a l'égalité $\text{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \text{card}(E_i) \Leftrightarrow$ les E_i sont disjoints deux à deux.

▶ *Démonstration:*

On procède par récurrence sur l'entier $n \geqslant 2$. Le résultat est connu si $n = 2$.
On suppose que ces propriétés sont vraies pour un entier $n \geqslant 2$ donné.
On se donne $n+1$ ensembles finis $E_1, E_2, \dots, E_n, E_{n+1}$. Soit $F = \bigcup_{i=1}^{n} E_i$.
Par hypothèse de récurrence, F est fini et $\text{card}(F) \leqslant \sum_{i=1}^{n} \text{card}(E_i)$.
Donc $\bigcup_{i=1}^{n+1} E_i = F \cup E_{n+1}$ est fini et $\text{card}\left(\bigcup_{i=1}^{n+1} E_i\right) \leqslant \text{card}(F) + \text{card}(E_{n+1}) \leqslant \sum_{i=1}^{n+1} \text{card}(E_i)$.
L'égalité $\text{card}\left(\bigcup_{i=1}^{n+1} E_i\right) = \sum_{i=1}^{n+1} \text{card}(E_i)$ équivaut à $\begin{cases} \text{card}(F \cup E_{n+1}) = \text{card}(F) + \text{card}(E_{n+1}) \\ \text{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{i=1}^{n} \text{card}(E_i) \end{cases}$
et signifie que E_{n+1} est disjoint de $F = \bigcup_{i=1}^{n} E_i$, les ensembles $E_1, \dots, E_n$ étant eux-mêmes disjoints deux à deux. Ceci prouve la propriété au rang $n+1$ et achève la récurrence ◀

Le résultat précédent peut être généralisé (mais la démonstration est admise) :

Proposition *(Formule du crible)*

Soient E_1, …, E_n des ensembles finis. Posons $I = \{1, 2, \ldots, n\}$.

On a $\operatorname{card}\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{J \subset I} (-1)^{1+\operatorname{card}(J)} \operatorname{card}\left(\bigcap_{j \in J} E_j\right)$

Par exemple, si E, F, G sont trois ensembles finis :

$$\begin{aligned}\operatorname{card}(E \cup F \cup G) = \; & \operatorname{card}(E) + \operatorname{card}(F) + \operatorname{card}(G) \\ & - \operatorname{card}(E \cap F) - \operatorname{card}(E \cap G) - \operatorname{card}(F \cap G) \\ & + \operatorname{card}(E \cap F \cap G).\end{aligned}$$

▶ *Démonstration:*

Soit $H = F \cup G$. On a $\operatorname{card}(E \cup F \cup G) = \operatorname{card}(E \cup H) = \operatorname{card}(E) + \operatorname{card}(H) - \operatorname{card}(E \cap H)$.
Mais $\operatorname{card}(H) = \operatorname{card}(F) + \operatorname{card}(G) - \operatorname{card}(F \cap G)$.
On a donc déjà : $\operatorname{card}(E \cup F \cup G) = \operatorname{card}(E) + \operatorname{card}(F) + \operatorname{card}(G) - \operatorname{card}(F \cap G) - \operatorname{card}(E \cap H)$.
D'autre part, $E \cap H = E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$. On en déduit :

$$\begin{aligned}\operatorname{card}(E \cap H) &= \operatorname{card}(E \cap F) + \operatorname{card}(E \cap G) - \operatorname{card}((E \cap F) \cap (E \cap G)) \\ &= \operatorname{card}(E \cap F) + \operatorname{card}(E \cap G) - \operatorname{card}((E \cap F \cap G))\end{aligned}$$

L'expression attendue de $\operatorname{card}(E \cup F \cup G)$ en découle ◀

Proposition *(Principe des bergers)*

Soit E, F deux ensembles finis, et f une application de E vers F.

Alors $\operatorname{card}(E) = \sum_{y \in F} \operatorname{card} f^{-1}(\{y\})$.

Donc si tous les éléments de F ont le même nombre q d'antécédents : $\operatorname{card}(E) = q \operatorname{card}(F)$.

▶ *Démonstration:*

En effet, les ensembles $A_y = f^{-1}(\{y\})$, quand y parcourt F, forment une partition de E.
Ils sont donc disjoints deux à deux et leur réunion est égale à E.
Il en découle $\operatorname{card}(E) = \operatorname{card}\left(\bigcup_{y \in F} A_y\right) = \sum_{y \in F} \operatorname{card}(A_y)$.
Si tous les y de F ont q antécédents, chaque $\operatorname{card}(A_y)$ vaut q, et il y a $\operatorname{card}(F)$ éléments y dans F. On en déduit $\operatorname{card}(E) = q \operatorname{card}(F)$ ◀

Proposition *(Produit cartésien d'ensembles finis)*

Si E et F sont finis, alors $E \times F$ est fini et $\operatorname{card}(E \times F) = \operatorname{card}(E) \operatorname{card}(F)$.

Plus généralement, si E_1, E_2, …, E_n sont finis, alors $\operatorname{card}\left(\prod_{i=1}^{n} E_i\right) = \prod_{i=1}^{n} \operatorname{card}(E_i)$.

En particulier, si E est fini, alors pour tout $n \geqslant 1$: $\operatorname{card}(E^n) = \operatorname{card}(E)^n$.

▶ *Démonstration:*

Si E ou F est vide, alors $E \times F$ est vide et on a $\operatorname{card}(E \times F) = \operatorname{card}(E) \operatorname{card}(F) = 0$.
Sinon, soit f l'application de $E \times F$ vers F définie par : $\forall (x, y) \in E \times F,\ f(x, y) = y$.
L'application f est surjective. Pour tout y de F, $A_y = f^{-1}(y) = \{(x, y), x \in E\}$.
L'application $g_y : E \to A_y$ définie par $g_y(x) = (x, y)$ est visiblement une bijection.
Il en découle que pour tout y de F, on a $\operatorname{card}(A_y) = q = \operatorname{card}(E)$.
Le principe des bergers donne : $\operatorname{card}(E \times F) = q \operatorname{card}(F) = \operatorname{card}(E) \operatorname{card}(F)$.
La suite de la proposition se démontre par une récurrence évidente sur n ◀

III Dénombrements

III.1 Applications entre ensembles finis

On note $\mathcal{F}(E,F)$ l'ensemble des applications d'un ensemble E vers un ensemble F.

Proposition *(Nombre d'applications entre deux ensembles finis)*

Si E et F sont finis non vides, $\mathcal{F}(E,F)$ est fini et $\text{card}\,(\mathcal{F}(E,F)) = \text{card}\,(F)^{\,\text{card}\,(E)}$.

Ce résultat justifie que l'on note souvent F^E l'ensemble $\mathcal{F}(E,F)$.

▶ *Démonstration:*

Posons $n = \text{card}\,(E)$. Soit a une bijection de E_n sur E. On note $E = \{a_1, a_2, \dots, a_n\}$.
Toute application $f : E \to F$ est caractérisée par le n-uplet $(f(a_1), f(a_2), \dots, f(a_n))$.
L'application $\varphi : \mathcal{F}(E,F) \to F^n$ définie par $\varphi(f) = (f(a_1), \dots, f(a_n))$ est donc bijective.
On en déduit $\text{card}\,(\mathcal{F}(E,F)) = \text{card}\,(F^n) = \text{card}\,(F)^n = \text{card}\,(F)^{\text{card}\,(E)}$ ◀

Proposition *(Ensemble des parties d'un ensemble fini)*

Soit E un ensemble fini, de cardinal n. Alors $\mathcal{P}(E)$ est fini et $\text{card}\,(\mathcal{P}(E)) = 2^n$.

▶ *Démonstration:*

A toute partie A de E, on associe sa fonction caractéristique $\chi_A : E \to \{0,1\}$.
On sait que l'application $A \mapsto \chi_A$ est une bijection de $\mathcal{P}(E)$ sur l'ensemble $\mathcal{F}(E,\{0,1\})$.
On sait que l'ensemble $\mathcal{F}(E,\{0,1\})$ est fini, de cardinal 2^n.
On en déduit $\text{card}\,(\mathcal{P}(E)) = 2^n$ ◀

Proposition *(Nombre d'injections ou de bijections entre deux ensembles finis)*

Soient E et F deux ensembles finis non vides.

Notons $\text{card}\,(E) = p$, et $\text{card}\,(F) = n$, avec $1 \leqslant p \leqslant n$.

Le nombre d'injections de E dans F est $\dfrac{n!}{(n-p)!}$.

En particulier, si $\text{card}\,(E) = \text{card}\,(F) = n$, le nombre de bijections de E dans F est $n!$

C'est le cas si $E = F$ (les bijections de E sur E sont appelées *permutations* de E).

▶ *Démonstration:*

Soit $\mathcal{I}(E,F)$ l'ensemble des applications injectives de E dans F.
C'est un ensemble non vide car $p \leqslant n$, et il est fini car inclus dans $\mathcal{F}(E,F)$.
On raisonne par récurrence sur l'entier $p \geqslant 1$.
Si $p = 1$, c'est évident : il y a n applications de E dans F, toutes injectives !
Supposons le résultat prouvé à l'ordre $p \geqslant 1$.
On se donne donc E de cardinal $p+1$, et F de cardinal $n \geqslant p+1$.
Soit a un élément fixé de E, et soit $E' = E - \{a\}$.
A tout élément f de $\mathcal{I}(E,F)$, on associe $\varphi(f) = f(a)$, image de a par f.
On définit ainsi une application φ de $\mathcal{I}(E,F)$ dans F.
Soit b un élément de F. Posons $F' = F - \{b\}$.
Une injection $g : E' \to F'$ a un seul prolongement injectif $f : E \to F$ tel que $f(a) = b$.
On dispose ainsi d'une bijection de $\varphi^{-1}(b)$ sur $\mathcal{I}(E',F')$.
L'hypothèse de récurrence donne : $\text{card}\,(\mathcal{I}(E',F')) = \dfrac{(n-1)!}{((n-1)-p))!} = \dfrac{(n-1)!}{(n-(p+1))!}$
On en déduit $\text{card}\,\varphi^{-1}(b) = \dfrac{(n-1)!}{(n-(p+1))!}$ pour tout b de F.
Le lemme des bergers donne alors $\text{card}\,(\mathcal{I}(E,F)) = \text{card}\,(F)\dfrac{(n-1)!}{(n-(p+1))!} = \dfrac{n!}{(n-(p+1))!}$.

On a ainsi démontré la propriété au rang $p+1$, ce qui achève la récurrence.
Puisque E est fini, une application $f : E \to E$ est bijective si et seulement si elle est injective.
Le nombre de bijections de E dans E est donc $\dfrac{n!}{(n-n)!} = \dfrac{n!}{0!} = n!$ ◄

III.2 Arrangements et combinaisons

Définition

Soient p, n deux entiers tels que $0 \leqslant p \leqslant n$.

On pose $\mathrm{A}_n^p = \dfrac{n!}{(n-p)!}$ et $\binom{n}{p} = \dfrac{1}{p!}\mathrm{A}_n^p = \dfrac{n!}{p!(n-p)!}$

On constate que, si $1 \leqslant p \leqslant n$: $\begin{cases} \mathrm{A}_n^p = n(n-1)\cdots(n-p+1) \\ \binom{n}{p} = \dfrac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 2\cdot 1} \end{cases}$

Par exemple : $\begin{cases} \forall\, n \in \mathbb{N}, \mathrm{A}_n^0 = 1,\ \mathrm{A}_n^n = n!,\ \binom{n}{0} = \binom{n}{n} = 1. \\ \forall\, n \in \mathbb{N}^*, \mathrm{A}_n^1 = n,\ \mathrm{A}_n^{n-1} = n!,\ \binom{n}{1} = \binom{n}{n-1} = n. \end{cases}$

On sait que si $1 \leqslant p \leqslant n$, A_n^p représente le nombre d'applications injectives d'un ensemble à p éléments vers un ensemble à n éléments.

Proposition *(Arrangements)*

Soit F un ensemble fini de cardinal $n \geqslant 1$. Soit p un entier vérifiant $1 \leqslant p \leqslant n$.

Un *arrangement* de p éléments de F est un p-uplet $(y_1, y_2, \ldots, y_p)$ formé de p éléments de F, distincts deux à deux.

Le nombre d'arrangements de p éléments de F est A_n^p (on parle souvent d'arrangements de p éléments parmi n).

► *Démonstration:*

Se donner un arrangement $(y_1, y_2, \cdots, y_p)$ de p éléments de F, c'est se donner une application injective f de E_p dans F, définie par : $\forall\, k \in E_p, f(k) = y_k$. Il y a donc autant d'arrangements de p éléments de F que de telles applications injectives, c'est-à-dire A_n^p ◄

Proposition *(Combinaisons)*

Soit F un ensemble fini de cardinal $n \geqslant 1$. Soit p un entier vérifiant $0 \leqslant p \leqslant n$.

Une *combinaison* de p éléments de F est une partie de F, de cardinal p.

Si $p \geqslant 1$, elle peut donc s'écrire $\{y_1, y_2, \ldots, y_p\}$, où y_1, y_2, …, y_p sont distincts deux à deux dans F (on parle souvent de combinaison *sans répétitions*).

Le nombre de combinaisons de p éléments de F est égal à $\binom{n}{p}$ (on parle souvent de combinaisons de p éléments parmi n).

► *Démonstration:*

Il y a un seul arrangement de 0 éléments de F : c'est la partie vide, et on a bien $\binom{n}{0} = 1$.

On suppose donc $p \geqslant 1$. Soit φ l'application qui à un arrangement $(y_1, y_2, \ldots, y_p)$ de p éléments de F associe la combinaison $\{y_1, y_2, \ldots, y_p\}$. L'application φ est sujective et chaque combinaison de p éléments de F est l'image de $p!$ arrangements différents.

En effet les arrangements fournissant la même combinaison que $(y_1, y_2, \dots, y_p)$ sont ceux qui s'en déduisent par une des $p!$ permutations possibles sur les p éléments $y_1, y_2, \dots, y_p$.

Le principe des bergers permet alors d'écrire : $\mathrm{A}_n^p = p!\binom{n}{p}$.

On en déduit $\binom{n}{p} = \frac{1}{p!}\mathrm{A}_n^p = \frac{n!}{p!(n-p)!}$ ◀

Propriétés fondamentales des coefficients $\binom{n}{p}$

$\begin{cases} \text{Pour tous entiers } n, p \text{ avec } 0 \leqslant p \leqslant n : \binom{n}{p} = \binom{n}{n-p}. \\ \text{Si } 1 \leqslant p \leqslant n-1, \text{ alors } \binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}. \end{cases}$

▶ *Démonstration:*

◇ *Soit E un ensemble fini de cardinal n.*
Pour tout k de $\{0, \dots, n\}$, soit $\mathcal{P}_k(E)$ l'ensemble des parties de E ayant k éléments.
L'application $A \mapsto \overline{A}$ est une bijection de $\mathcal{P}(E)$ sur lui-même.
Pour tout p de $\{0, \dots, n\}$, elle induit une bijection de $\mathcal{P}_p(E)$ sur $\mathcal{P}_{n-p}(E)$.
Il en résulte l'égalité $\mathrm{card}\,(\mathcal{P}_p(E)) = \mathrm{card}\,(\mathcal{P}_{n-p}(E))$.
On a donc prouvé l'égalité $\binom{n}{p} = \binom{n}{n-p}$.
Remarque : on peut bien sûr écrire $\binom{n}{n-p} = \frac{n!}{(n-p)!\,(n-(n-p))!} = \frac{n!}{(n-p)!p!} = \binom{n}{p}$.

◇ *On pourrait mettre en place des bijections, mais un simple dénombrement suffit.*
On suppose que les entiers n et p vérifient $1 \leqslant p \leqslant n-1$.
On fixe un élément a d'un ensemble E de cardinal n.
Il y a $\binom{n}{p}$ manières différentes de choisir une partie A de E ayant p éléments.
Deux cas sont possibles, qui s'excluent mutuellement :
- *Ou bien a n'appartient pas à A :*
  Il y a alors $\binom{n-1}{p}$ manières de former A car il reste à choisir p éléments parmi les $n-1$ éléments de $E \setminus \{a\}$.
- *Ou bien a appartient à A :*
  Il y a alors $\binom{n-1}{p-1}$ manières de former A car il reste à choisir $p-1$ éléments parmi les $n-1$ éléments de $E \setminus \{a\}$.

Ce dénombrement prouve que $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$ ◀

Cette dernière formule, avec $\binom{n}{0} = \binom{n}{n} = 1$, permet de calculer les $\binom{n}{p}$ de proche en proche. On place souvent les $\binom{n}{p}$ dans un tableau triangulaire, dont les lignes et les colonnes sont numérotées à partir de 0. Le coefficient $\binom{n}{p}$ vient alors se placer à l'intersection de la ligne d'indice n et de la colonne d'indice p.
Le tableau ci-dessous est connu sous le nom de "triangle de Pascal" :

	$p=0$	$p=1$	$p=2$	$p=3$	$p=4$	$p=5$	$p=6$	$\cdots$
$n=0$	1							
$n=1$	1	1						
$n=2$	1	2	1					
$n=3$	1	3	3	1				
$n=4$	1	4	6	4	1			
$n=5$	1	5	10	10	5	1		
$n=6$	1	6	15	20	15	6	1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\ddots$
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\ddots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Autres propriétés

Sous réserve que les coefficients ci-dessous soient définis, on a les égalités :

$$\binom{n}{p+1} = \frac{n-p}{p+1}\binom{n}{p}, \quad \binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}, \quad \binom{n}{p} = \frac{n}{n-p}\binom{n-1}{p}$$

▶ *Démonstration:*

◇ *On suppose* $0 \leqslant p < n$: $\binom{n}{p+1} = \dfrac{n!}{(p+1)!(n-p-1)!} = \dfrac{n-p}{p+1}\dfrac{n!}{p!(n-p)!} = \dfrac{n-p}{p+1}\binom{n}{p}$.

◇ *On suppose* $1 \leqslant p \leqslant n$: $\binom{n}{p} = \dfrac{n!}{p!(n-p)!} = \dfrac{n}{p}\dfrac{(n-1)!}{(p-1)!((n-1)-(p-1))!} = \dfrac{n}{p}\binom{n-1}{p-1}$.

◇ *On suppose* $0 \leqslant p < n$: $\binom{n}{p} = \dfrac{n!}{p!(n-p)!} = \dfrac{n}{n-p}\dfrac{(n-1)!}{p!(n-p-1)!} = \dfrac{n}{n-p}\binom{n-1}{p}$ ◀

III.3 Binôme de Newton

Le résultat suivant est particulièrement important.

C'est sans doute en utilisant la formule du binôme qu'on a le plus de chances de rencontrer les coefficients $\binom{n}{p}$ (qui pour cette raison sont appelés *coefficients du binôme*).

Proposition *(Formule du binôme de Newton)*

$\forall (x,y) \in \mathbb{C}^2, \forall n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. En particulier : $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$.

▶ *Démonstration:*

On procède par récurrence sur $\mathbb{N}$. *La propriété est évidente si* $n = 0$.
En effet $(xy)^0 = 1$ *et* $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \binom{n}{0} x^0 y^0 = 1$.
Supposons la propriété démontrée au rang $n \geqslant 0$, *et considérons* $(x+y)^{n+1}$. *On a :*

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\Big(\sum_{k=0}^{n}\binom{n}{k}x^k\,y^{n-k}\Big)\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}\,y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k\,y^{n+1-k}\\
&= \binom{n}{n}x^{n+1}\,y^0 + \sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}\,y^{n-k} + \sum_{k=1}^{n}\binom{n}{k}x^k\,y^{n+1-k} + \binom{n}{0}x^0\,y^{n+1}\\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^k\,y^{n+1-k} + \sum_{k=1}^{n}\binom{n}{k}x^k\,y^{n+1-k} + y^{n+1}\\
&= x^{n+1} + \sum_{k=1}^{n}\Big(\binom{n}{k-1} + \binom{n}{k}\Big)x^k\,y^{n+1-k} + y^{n+1}\\
&= \binom{n+1}{n+1}x^{n+1}y^0 + \sum_{k=1}^{n}\binom{n+1}{k}x^k\,y^{n+1-k} + \binom{n+1}{0}x^0y^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k\,y^{n+1-k}
\end{aligned}
$$

Ce qui démontre la propriété au rang $n+1$ et achève la récurrence ◀

Compléments

Axiomes de Peano

On pourrait définir l'ensemble $\mathbb{N}$ à partir d'un nombre réduit d'axiomes.

Une telle définition est hors-programme en MPSI.

L'introduction la plus connue de $\mathbb{N}$ est par les *Axiomes de Peano*.

Si on est intéressé par le sujet, on pourra se référer à

`http://megamaths.perso.neuf.fr/cenn0001.pdf`
`http://fr.wikipedia.org/wiki/Axiomes_de_Peano`
`http://fr.wikipedia.org/wiki/Giuseppe_Peano`

Ensembles dénombrables

NB : la notion d'ensemble dénombrable est hors-programme des classes préparatoires.

Définition

Un ensemble E est dit *dénombrable* s'il existe une bijection de $\mathbb{N}$ sur E.
Un ensemble E est dit *au plus dénombrable* s'il est fini ou dénombrable.

Remarques

– $\mathbb{N}$ est évidemment lui-même un ensemble dénombrable.

$\mathbb{N}^*$ est dénombrable car la succession $n \mapsto n+1$ est une bijection de $\mathbb{N}$ sur $\mathbb{N}^*$.

De même, l'ensemble des entiers pairs et celui des entiers impairs sont dénombrables (considérer les applications $n \mapsto 2n$ et $n \mapsto 2n+1$.)

– Tout ensemble dénombrable est infini (car $\mathbb{N}$ est lui-même infini.)

– Si E est dénombrable, et si on note $n \mapsto a_n$ une bijection de $\mathbb{N}$ sur E, on peut donc écrire $E = \{a_n, n \in \mathbb{N}\}$, les a_n étant distincts deux à deux. Le caractère dénombrable de E est donc une manière de "numéroter" distinctement les différents éléments de E.

– Si E est dénombrable (resp. au plus dénombrable) et s'il existe une bijection de E sur un ensemble F, alors F est dénombrable (resp. au plus dénombrable).

Proposition *(Parties d'un ensemble dénombrable)*

Toute partie F d'un ensemble dénombrable E est au plus dénombrable.

▶ *Démonstration:*

Quitte à utiliser une bijection de $\mathbb{N}$ sur E, on peut toujours supposer que $E = \mathbb{N}$.
Soit F une partie de $\mathbb{N}$. Montrons que si F est infinie alors F est dénombrable.
On forme une application f de $\mathbb{N}$ dans F, par récurrence, de la manière suivante :

◇ *$f(0)$ est le minimum de F (qui est une partie non vide de $\mathbb{N}$.)*

◇ *Pour tout n de $\mathbb{N}^*$, $f(n) = \min(F \setminus \{f(0), \dots, f(n-1)\})$ (non vide car F est infini.)*

f est injective. En effet, si $m < n$, alors $f(n) \notin \{f(0), \dots, f(m)\} \Rightarrow f(n) \neq f(m)$.
L'application f réalise donc une bijection de $\mathbb{N}$ sur $f(\mathbb{N})$. Il en découle que $f(\mathbb{N})$ est infini.
Supposons par l'absurde que f ne soit pas bijective.
Il existe alors un élément x de F qui n'a pas d'antécédent par f.
Pour tout entier $n \geqslant 1$, l'elément x est donc dans $F \setminus \{f(0), \dots, f(n-1)\}$.
Par définition de $f(n)$, il en découle $f(n) \leqslant a$. Or on a également $f(0) \leqslant a$.
L'ensemble $f(\mathbb{N})$ est donc inclus dans $[\![0, a]\!]$, ce qui implique qu'il est majoré donc fini.
On arrive ainsi à une absurdité.
L'application f est donc une bijection de $\mathbb{N}$ sur F : l'ensemble F est dénombrable ◀

Proposition *(Produit cartésien d'ensembles dénombrables)*

L'ensemble $\mathbb{N} \times \mathbb{N}$ est dénombrable.

Si $E_1, \dots, E_n$ sont dénombrables, leur produit cartésien $\prod_{k=1}^{n} E_k$ est dénombrable.

► *Démonstration:*

◇ *Tout entier n non nul s'ecrit d'une manière unique $n = 2^p(2q+1)$, avec $(p, q) \in \mathbb{N}^2$.*
En effet, p est l'exposant maximum k tel que $2^k \mid n$, et $2q+1$ est l'entier (nécessairement impair) résultant du quotient exact de n par 2^p.
L'application $(p, q) \mapsto 2^p(2q+1)$ est donc une bijection de $\mathbb{N}^2$ sur $\mathbb{N}^*$.
Comme $\mathbb{N}^*$ est dénombrable, il en résulte que $\mathbb{N}^2$ est dénombrable.

◇ *On commence par traiter le cas de la réunion de deux ensembles dénombrables.*
Soient E_1 et E_2 deux ensembles dénombrables.
Soient $f : \mathbb{N} \to E_1$ et $g : \mathbb{N} \to E_2$ deux bijections.
Alors l'application $h : \mathbb{N}^2 \to E_1 \times E_2$ définie par $h(m, n) = (f(m), g(n))$ est une bijection.
Il en découle que l'ensemble $E_1 \times E_2$ est dénombrable.
Le passage au cas de plus de deux ensembles s'effectue par une récurrence évidente ◀

Proposition *(Une caractérisation des ensembles au plus dénombrables)*

Soient E un ensemble dénombrable. Un ensemble F non vide est au plus dénombrable si et seulement s'il existe une surjection de E sur F.

► *Démonstration:*

◇ *Quitte à utiliser une bijection de $\mathbb{N}$ sur E, on peut toujours supposer que $E = \mathbb{N}$.*
Soit f une surjection de $\mathbb{N}$ vers F.
Pour tout y de F, on note $g(y)$ le plus petit des antécédents de y par f.
On définit ainsi une application $g : F \to \mathbb{N}$ qui vérifie $f \circ g = \mathrm{Id}_F$ par construction.
L'application $f \circ g$ étant injective, il en est de même de g.
L'application g réalise donc une bijection de F sur une partie de $\mathbb{N}$.
Cette dernière étant au plus dénombrable, il en est de même de F.

◇ *La réciproque est évidente.*
Si F est dénombrable il existe une bijection (donc une surjection) f de $\mathbb{N}$ sur F.
Supposons donc $\mathrm{card}\,(F) = n \geqslant 1$, et soit f une bijection de $[\![0, n-1]\!]$ sur F.
L'application g définie par $g(k) = \min(k, n-1)$ est alors une surjection de $\mathbb{N}$ sur F ◀

Remarques et conséquences

– La proposition précédente signifie qu'un ensemble non vide E est au plus dénombrable si et seulement s'il peut s'écrire $E = \{a_n, n \in \mathbb{N}\}$, (les a_n étant non nécessairement distincts.)

– L'ensemble $\mathbb{Z}$ est dénombrable car il est infini (il contient $\mathbb{N}$) et l'application définie sur $\mathbb{N}^2$ par $f(m,n) = m - n$ est une sujection de $\mathbb{N}^2$ sur $\mathbb{Z}$.

– L'ensemble $\mathbb{Q}$ est dénombrable car il est infini (il contient $\mathbb{N}$) et l'application f définie sur $\mathbb{Z} \times \mathbb{N}^*$ par $f(m,n) = \dfrac{m}{n}$ est une surjection de $\mathbb{Z} \times \mathbb{N}^*$ sur $\mathbb{Q}$.

Proposition *(Réunions d'ensembles au plus dénombrables)*

Soit $(E_n)_{n\in\mathbb{N}}$ une suite d'ensembles au plus dénombrables.
Alors leur réunion $F = \bigcup_{n\in\mathbb{N}} E_n$ est un ensemble au plus dénombrable.

► *Démonstration:*

Pour tout n de $\mathbb{N}$, on sait qu'il existe une surjection, que nous noterons f_n, de $\mathbb{N}$ sur E_n.
On définit alors $g : \mathbb{N}^2 \to F$ en posant $g(n,m) = f_n(m)$. Montrons que g est surjective.
Soit x un élément de F. Il existe au moins un entier n tel que x appartienne à E_n.
Mais l'application $f_n : \mathbb{N} \to E_n$ étant surjective, il existe m dans $\mathbb{N}$ tel que $f_n(m) = x$.
On a ainsi trouvé (n,m) dans $\mathbb{N}^2$ tel que $g(n,m) = x$. L'application g est donc surjective.
Il en découle que F est au plus dénombrable ◄

Remarques

– Si l'un au moins des E_n est dénombrable, alors $F = \bigcup_{n\in\mathbb{N}} E_n$ est dénombrable.

– Une union *finie* d'ensembles au plus dénombrables est au plus dénombrable : il suffit en effet de compléter une famille finie $E_0, E_1, \ldots, E_n$ par des E_k égaux par exemple à E_n.

Proposition

L'ensemble $\mathcal{P}(\mathbb{N})$ est infini non dénombrable.

► *Démonstration:*

Supposons par l'absurde qu'il existe une surjection f de $\mathbb{N}$ sur $\mathcal{P}(\mathbb{N})$.
Considérons la partie de A de $\mathbb{N}$ définie par $A = \{n \in \mathbb{N},\ n \notin f(n)\}$.
Puisque f est surjective, il existe un élément a de $\mathbb{N}$ tel que $f(a) = A$.
On se pose alors la question de savoir si a est ou n'est pas élément de A.

– *Si $a \in A$, cela signifie, par définition de A, que a n'est pas dans $f(a) = A$: c'est absurde.*

– *Si $a \notin A$, cela signifie que a est dans $f(a) = A$: c'est toujours aussi absurde.*

Conclusion : l'hypothèse de l'existence d'une surjection de $\mathbb{N}$ dans $\mathcal{P}(\mathbb{N})$ est absurde.
Il en résulte que l'ensemble $\mathcal{P}(\mathbb{N})$ (qui est manifestement infini) est non dénombrable ◄

Proposition

L'ensemble $\mathbb{R}$ est infini non dénombrable.

► *Démonstration:*

Tout x de $[0,1[$ a un unique développement décimal illimité $x = 0,a_1a_2\ldots a_n\ldots$
Pour simplifier les notations, on note $a_k = d_k(x)$. Soit f une application de $\mathbb{N}^*$ sur $[0,1[$.
On définit $x = 0,a_1a_2\ldots a_n\ldots$ par son développement décimal de la manière suivante :
Si $d_n(f(n)) = 0$ alors $d_n(x) = 1$. Sinon $d_n(x) = 0$.
Ainsi : $\forall\, n \in \mathbb{N}^*$, $x \neq f(n)$ car leurs décimales de rang n sont distinctes.
Le réel x n'a donc pas d'antécédent par f. On peut donc conclure :
Il n'y a pas de surjection de $\mathbb{N}^*$ sur $[0,1[$ donc à fortiori sur $\mathbb{R}$: $\mathbb{R}$ n'est pas dénombrable ◄

Si on est intéressé par le sujet “dénombrabilité”, on pourra se référer à

`http://fr.wikipedia.org/wiki/Ensemble_dénombrable`

Plus précisément, pour la non-dénombrabilité de $\mathbb{R}$, on pourra consulter :

`http://fr.wikipedia.org/wiki/Argument_de_la_diagonale_de_Cantor`