Ensembles, dénombrement

Antoine MOTEAU antoine.moteau@wanadoo.fr

Table des matières

Ensembles, dénombrement.

1 Ensembles finis ou non. Cardinal d'un ensemble.

Le théorie des ensembles est une théorie axiomatique, que nous ne développons pas ici.
La théorie élémentaire (”naïve”) des ensembles conduit au paradoxe suivant :

Paradoxe de la théorie des ensembles

> ”L'ensemble de tous les ensembles” n'est pas un ensemble.
>
> (sinon il s'appartiendrait à lui-même, ce qui est contradictoire avec la théorie des ensembles)

Une bonne question : Mais Zalors qu'est que c'est ? . . . La réponse est dans une théorie ”supérieure”, plutôt complexe . . .

Particularités de l'ensemble vide $\emptyset$.

- L'ensemble vide est unique et il est sous-ensemble de tous les ensembles.
- Par exemple, les propositions suivantes sont des tautologies :
  - $\Big((a \in \emptyset) \Longrightarrow (a \notin \emptyset)\Big)$.
  - $\Big((1 = 2) \Longrightarrow (1 \neq 2)\Big)$.

1.1 Applications d'un ensemble vers un autre.

- Application . . . .
- Application injective . . . .
- Application surjective . . . .

1.2 Cardinal d'un ensemble.

Définition 1.2.1.

Deux ensembles E et F ont ”même cardinal” s'il existe une bijection de l'un dans l'autre.

On écrira alors $\text{card}(E) = \text{card}(F)$.

Définition 1.2.2.

Le cardinal d'un ensemble E est plus petit que le cardinal d'un ensemble F s'il existe une injection de E dans F.

On écrira alors $\text{card}(E) \preceq \text{card}(F)$ et aussi $\text{card}(E) \prec \text{card}(F)$ si $\begin{cases} \text{card}(E) \preceq \text{card}(F) \\ \text{et} \quad \text{card}(E) \neq \text{card}(F). \end{cases}$

Théorème 1.2.1.

Etant donnés des ensembles E, F et G,

- $\Big(\big(\text{card}(E) \preceq \text{card}(F)\big) \vee \big(\text{card}(F) \preceq \text{card}(E)\big)\Big)$.
- $\Big(\big(\text{card}(E) \preceq \text{card}(F)\big) \wedge \big(\text{card}(F) \preceq \text{card}(E)\big)\Big) \Longrightarrow \Big(\text{card}(E) = \text{card}(F)\Big)$.
- $\Big(\big(\text{card}(E) \preceq \text{card}(F)\big) \wedge \big(\text{card}(F) \preceq \text{card}(G)\big)\Big) \Longrightarrow \Big(\text{card}(E) \preceq \text{card}(G)\Big)$.

Pour les ensembles finis, le cardinal est assimilé au nombre d'élements.

- $\text{card}\big(\emptyset\big) = 0$.
- Avec $n \in \mathbb{N}^*$, $\text{card}\big(\{1, 2, 3, \cdots, n\}\big) = n$.

1.3 Cardinaux usuels

On note souvent $|E| = \text{card}(E)$ (simplification d'écriture).

1.3.1 Notation par représentant

Pour les ensembles ayant même cardinal, on choisit souvent le plus courant de ces ensembles comme représentant du cardinal de ces ensembles (ce qui amène parfois, dans un contexte particulier, à faire l'amalgame entre le représentant et le cardinal). Par exemple

- $\mathbb{N}$ est choisi comme représentant des ensembles en bijection avec $\mathbb{N}$ et, dans un certain contexte, on écrit parfois $\mathbb{N} = \text{card}(\mathbb{N})$ $(= |\mathbb{N}|)$.
- $\mathbb{R}$ est choisi comme représentant des ensembles en bijection avec $\mathbb{R}$ et, dans un certain contexte, on écrit parfois $\mathbb{R} = \text{card}(\mathbb{R})$ $(= |\mathbb{R}|)$.
- Avec $n \in \mathbb{N}^*$, $\{1, 2, \cdots n\}$ est choisi comme représentant des ensembles à n éléments, et, dans un certain contexte, on écrit parfois $\{1, 2, \cdots n\} = n$.

1.3.2 Ensemble des applications d'un ensemble vers un autre

Etant donnés deux ensembles E et F, on note

- F^E l'ensemble des applications de E vers F.
- $\big(\text{card}(F)\big)^{\text{card}(E)}$ (ou $|F|^{|E|}$) le cardinal de F^E (même si ces ensembles ne sont pas finis !).

Remarque.
Lorsque E et F sont finis, le cardinal de l'ensemble des applications de E vers F est $\big(\text{card}(F)\big)^{\text{card}(E)}$, ce qui explique la notation F^E et la généralisation (en tant que notation) au cas des ensemble non finis.

Cas particulier des "puissances" finies :

Etant donné un ensemble E, pour $n \in \mathbb{N}$,

- E^n est l'ensemble des n-uplets d'éléments de E.
- E^n est l'ensemble des séquences $(x_1, x_2, \cdots x_n)$ de n éléments de E.
- E^n est l'ensemble des images de $\{1, 2, \cdots, n\}$ par les applications de $\{1, 2, \cdots, n\}$ dans E.
- $E^n = E^{\{1,2,\cdots,n\}}$ (E^n est assimilé à l'ensemble des applications de $\{1, 2, \cdots, n\}$ dans E) .

Théorème 1.3.1.

Soit E un ensemble et $\mathcal{P}(E)$ l'ensemble des parties (ou sous-ensembles) de E.

- $\text{card}\,(\mathcal{P}(E)) = 2^{|E|}$
  ou encore : $\mathcal{P}(E)$ est en bijection avec l'ensemble des applications de E vers $\{0, 1\}$.
- $\text{card}\, E \prec \text{card}\,(\mathcal{P}(E))$.

Preuve.

- On montre que l'application f suivante est une bijection entre $\mathcal{P}(E)$ et $\{0, 1\}^{|E|}$.

$$\left(\begin{array}{ccc} f: & \mathcal{P}(E) & \longrightarrow & \{0,1\}^E \\ & P & \longmapsto & \left(\begin{array}{cccc} f_P: & E & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \begin{cases} 0 \text{ si } x \notin P \\ 1 \text{ si } x \in P \end{cases} \end{array}\right) \end{array}\right)$$

- On montre qu'il n'existe pas de surjection de E dans $\mathcal{P}(E)$ ... .

1.3.3 Exemples

- Ensembles **dénombrables** (en bijection avec $\mathbb{N}$) :

$$\begin{aligned}|\mathbb{N}| &= |\mathbb{N}| = \left|\mathbb{N}^2\right| = \left|\mathbb{N}^3\right| = \cdots = |\mathbb{N}^n| \quad (\text{pour } n \in \mathbb{N}^*)\\ &= |\mathbb{Z}| = \left|\mathbb{Z}^2\right| = \left|\mathbb{Z}^3\right| = \cdots = |\mathbb{Z}^n| \quad (\text{pour } n \in \mathbb{N}^*)\\ &= |\mathbb{Q}| = \left|\mathbb{Q}^2\right| = \left|\mathbb{Q}^3\right| = \cdots = |\mathbb{Q}^n| \quad (\text{pour } n \in \mathbb{N}^*)\end{aligned}$$

- Ensembles **"continus"** (de même cardinal que $\mathbb{R}$) :

$$\begin{aligned}|\mathbb{N}| \prec |\mathbb{R}| &= \left|2^{\mathbb{N}}\right| = \left|\mathbb{N}^{\mathbb{N}}\right|\\ &= |\mathbb{R}| = \left|\mathbb{R}^2\right| = \left|\mathbb{R}^3\right| = \cdots = |\mathbb{R}^n| \quad (\text{pour } n \in \mathbb{N}^*)\\ &= |\mathbb{C}| = \left|\mathbb{C}^2\right| = \left|\mathbb{C}^3\right| = \cdots = |\mathbb{C}^n| \quad (\text{pour } n \in \mathbb{N}^*)\end{aligned}$$

- Ensembles de cardinal supérieur au cardinal de $\mathbb{R}$:
$$\text{card}(\mathbb{R}) \prec \text{card}\,(\mathcal{P}(\mathbb{R})) \prec \text{card}\,\Big(\mathcal{P}\Big(\mathcal{P}(\mathbb{R})\Big)\Big) \prec \ldots.$$

Il y a donc une infinité d'infinis ... et certains sont plus grands que d'autres ....

Hypothèse du continu

L'hypothèse du continu stipule qu'il n'existe pas d'ensemble E tel que $|N| < |E| < |\mathbb{R}|$.

En utilisant un ingénieux procédé diagonal, **Cantor** a prouvé en 1874 que l'ensemble des nombres réels n'a pas même cardinal que l'ensemble des nombres entiers. Il émet à cette occasion la conjecture suivante : tout ensemble contenant l'ensemble des entiers, et contenu dans l'ensemble des nombres réels, aurait ou bien le même cardinal que l'ensemble des entiers, ou bien le même cardinal que l'ensemble des réels. C'est **l'hypothèse du continu**, du nom que l'on donne parfois à l'ensemble des nombres réels (le continuum).
Cette conjecture fut reprise par **David Hilbert** comme le premier de la célèbre liste des **23 problèmes** qu'il posa en 1900.
On sait désormais que l'hypothèse du continu est indécidable, c'est-à-dire qu'elle est indépendante des axiomes standards de la théorie des ensembles.

Précisément, **Gödel** a prouvé en 1940 qu'avec les axiomes standards de la théorie des ensembles (système dit ZF, de **Zermelo-Fraenkel**), on ne pouvait réfuter l'hypothèse du continu.

En écho, en 1963, **Cohen** a démontré qu'on ne pouvait pas à partir des même axiomes démontrer l'hypothèse du continu.

Le même statut particulier est réservé à l'axiome du choix. Pour l'un comme pour l'autre, on peut choisir de l'adjoindre ou non à la liste des axiomes de la théorie des ensembles.

Il semble que des travaux récents, en particulier de **Laurent LAFFORGUE** (*), encore en cours d'élaboration, conduisent à une théorie des ensembles dans laquelle l'hypothèse du continu serait fausse (qui prouverait donc l'existence d'ensembles E tels $|\mathbb{N}| < |E| < |R|$).

(*) **Laurent LAFFORGUE**, mathématicien français, né le 6 novembre 1966 à Antony dans les Hauts-de-Seine. Ancien élève de l'École Normale Supérieure de la rue d'Ulm (promotion 1986), professeur permanent à l'Institut des Hautes Études Scientifiques (IHÉS), directeur de recherche au CNRS. Distingué pour ses travaux sur le **Programme de Langlands**, il reçoit le 20 août 2002, ainsi que **Vladimir VOEVODSKY** (Institute for Advanced Study, Princeton, USA), la **médaille Fields 2002**.

La correspondance (ou programme) de Langlands doit son nom au mathématicien canadien **Robert P. LANGLANDS** qui, dans une lettre adressée en 1967 au mathématicien français **André WEIL**, proposait une série d'idées et de conjectures reliant des parties importantes de la théorie des nombres, de l'algèbre et de l'analyse. Elle est devenue un véritable programme de recherche qui a inspiré de très nombreux travaux de mathématiques fondamentales.

2 Ensembles finis : dénombrement.

2.1 Nombre d'applications d'un ensemble vers un autre

Théorème 2.1.1.

Soit E un ensemble à $p > 0$ éléments et F un ensemble à $n > 0$ éléments.

Il y a n^p applications de E vers F (autrement dit $\left|F^E\right| = |F|^{|E|}$).

Preuve. Par récurence sur p ...

Théorème 2.1.2.

Soit E un ensemble fini à $p \geqslant 0$ éléments et $\mathcal{P}(E)$ l'ensemble des parties (ou sous-ensembles) de E.

$\operatorname{card}(\mathcal{P}(E)) = 2^p$ (autrement dit $|\mathcal{P}(E)| = 2^{|E|}$).

Preuve.

- Pour $p = 0$, $E = \emptyset$ et $\mathcal{P}(E) = \{\emptyset\}$ possède $1 = 2^0$ éléments.
- Pour $p > 0$, $\mathcal{P}(E)$ est en bijection avec l'ensemble $\{0, 1\}^E$ des applications de E vers $\{0, 1\}$.

2.2 Arrangements, nombre d'applications injectives d'un ensemble vers un autre

Définition 2.2.1.

Etant donné un ensemble F à n éléments et un entier $p > 0$, une application injective de $\{1, 2, \cdots, p\}$, s'appelle un arrangement des n éléments de F à p places.

Le nombre d'arrangements de n éléments à p places se note A_n^p.

Remarque. Un arrangement des n éléments de F à p places ($1 \leqslant p \leqslant n$) est assimilable à une séquence ordonnée (numérotée, **"rangée"**) de p éléments de F : $x_1, x_2, \cdots, x_n$.

Théorème 2.2.1.

Soit E un ensemble à p éléments et F un ensemble à $n > 0$ éléments.

- *si $0 < p \leqslant n$, il y a $\dfrac{n!}{(n-p)!}$ applications injectives de E vers F ;* $\left(\text{d'où : } A_n^p = \dfrac{n!}{(n-p)!}\right)$.
- *si $p > n$ ou si $p = 0$, il y a 0 applications injectives de E vers F.*

Preuve. Par récurrence sur p, on montrer qu'il y a $\big(n \times (n-1) \times \cdots \times (n-p+2)\big) \times (n-p+1)$ injections de E vers F :

- Pour $p = 1$, il y a n choix possibles pour l'image d'un élément.
- Pour $p > 1$,
  - On construit les images distinctes des $p-1$ premiers éléments de E en réalisant une injection d'un ensemble à $p-1$ éléments dans F, ce qui donne $n \times (n-1) \times \cdots \times \big(n-(p-1)+1\big)$ possiblilités.
  - Pour chacune des possibilités précédentes, on construit l'image du p-ième élément en choisissant un élément de F qui n'est pas une des $p-1$ images déjà prises, donc un élément parmi les $n-(p-1)$ restants.

  Cela donne en tout $\big(n \times (n-1) \times \cdots \times (n-p+2)\big) \times (n-p+1) = \dfrac{n!}{(n-p)!}$ choix.

Théorème 2.2.2.

Soit E un ensemble à $p > 0$ éléments.

Il u a $p!$ bijections de E dans lui même.

Preuve. Conséquence imédiate du théorème précédent, avec $n = p$.

2.3 Combinaisons, nombre de parties à p éléments dans un ensemble à n éléments

Définition 2.3.1.

Etant donné un ensemble F à n éléments et un entier p, une partie (sous-ensemble) de F à p éléments s'appelle une combinaison des n éléments de F à p places.

Le nombre de combinaisons de n éléments à p places se note C_n^p ou $\binom{n}{p}$.

Théorème 2.3.1.

Soit F un ensemble à n éléments et $p \in N$.

- *si $0 \leqslant p \leqslant n$, il y a $\dfrac{n!}{(n-p)!\,p!}$ parties de F ayant p éléments ;*

  soit $\dfrac{n!}{(n-p)!\,p!}$ combinaisons des n éléments de F à p places. $\boxed{\binom{n}{p} = \dfrac{n!}{(n-p)!\,p!}}$.

- *si $p > n$ ou si $p = 0$, il y a 0 applications injectives de E vers F* $\left(\text{ou : } \binom{n}{p} = 0\right)$.

<u>*Preuve*</u>.

- Pour décrire une partie à p éléments d'un ensemble F à n éléments, avec $1 \leqslant p \leqslant n$, on <u>enumère</u> p éléments de F, par exemple en les numérotant :

$$\{x_1, x_2, \cdots, x_p\}$$

  ce qui, en fait, décrit <u>une application injective</u> de $\{1, 2, \cdots, p\}$ dans F.
  Mais en prenant les mêmes éléments, décrits dans un autre ordre, on obtient <u>le même ensemble</u>, par exemple

$$\{x_p, x_{p-1}, \cdots, x_1\}$$

  Ainsi, si on compte les applications injectives de $\{1, 2, \cdots, p\}$ dans F, la même partie de F à p éléments sera comptée autant de fois que l'on peut changer l'ordre d'énumération de ses éléments, c'est à dire autant de fois que l'on peut réaliser une bijection de $\{1, 2, \cdots, p\}$ dans lui même, c'est à dire $p!$ fois.
  On en déduit qu'il y a $\dfrac{A_n^p}{p!}$ parties de F ayant p éléments, soit que $\binom{n}{p} = \dfrac{n!}{(n-p)!\,p!}$.

- Bien évidement, si $p < 0$ ou $p > n$, il y a 0 parties de F à n éléments.

<u>**Propriétés élémentaires**</u> **:** (pour $n \in \mathbb{N}^*$, avec F ensemble à n éléments)

- $\binom{n}{0} = 1$ ($\emptyset$ est la seule partie de F à 0 éléments) .
- $\binom{n}{n} = 1$ (F est la seule partie de F à n éléments) .
- $\binom{n}{1} = n$ (Il y a n singletons dans F) .
- $\binom{n}{n-p} = \binom{n}{p}$ <u>choisir</u> une partie à p éléments, c'est <u>choisir</u> de "ne pas choisir" son complémentaire qui en a $n-p$.
- $\binom{n}{n-1} = n$ (conséquence immédiate de ce qui précède).
- ....

2.4 Triangle de Pascal

0	**1**							
1	**1**	**1**						
2	**1**	2	**1**					
3	**1**	3	3	**1**				
4	**1**	4	6	4	**1**			
5	**1**	5	10	$\boxed{10}$ +	$\boxed{5}$ =	**1**		
6	**1**	6	15	20	$\boxed{15}$	6	**1**	
7	**1**	4	21	35	35	21	7	**1**

$$\boxed{\binom{n}{0} = \binom{n}{n} = 1}$$ (bordure du triangle)

$$\boxed{\binom{n}{p-1} + \binom{n}{p}} \boxed{= \binom{n+1}{p}}$$

Théorème 2.4.1. *Formule du triangle de Pascal .*

Pour $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ avec $1 \leqslant p \leqslant n$,

$$\binom{n}{p-1} + \binom{n}{p} = \binom{n+1}{p}$$

Preuve.

Soit $n \in \mathbb{N}^*$, $p \in \mathbb{N}$ tel que $1 \leqslant p \leqslant n$. Prenons un ensemble F à $n+1$ éléments et fixons un élément a de F.

Une partie à p élément de F peut, exclusivement, contenir a ou ne pas contenir a.

- Si une partie contient a, le reste de cette partie est un sous-ensemble à $p-1$ éléments de $F \setminus \{a\}$.
  On en déduit qu'il y a $\binom{n}{p-1}$ parties de F qui contiennent a.
- Si une partie ne contient pas a, c'est un sous-ensemble à p éléments de $F \setminus \{a\}$.
  On en déduit qu'il y a $\binom{n}{p}$ parties de F qui ne contiennent pas a.

Au total il y a $\binom{n}{p-1} + \binom{n}{p}$ parties de F à p éléments, CQFD.

Quelques propriétés élémentaires :

- $\displaystyle\sum_{p=0}^{n} \binom{n}{p} = 2^n$: $\mathcal{P}(F)$ est la réunion des sous-ensembles des parties à p éléments.
- $\displaystyle\sum_{p=0}^{E(n/2)} \binom{n}{2\,p} = \sum_{p=0}^{E((n-1)/2)} \binom{n}{2\,p+1} = 2^{n-1}$:
  - si n est impair, il y a autant de parties paires que de parties impaires.
  - si n est pair, les parties impaires sont déduites des parties paires (non $\emptyset$) par suppression d'un élément.
- ...

2.5 Formule du binome de Newton, de Liebniz

Théorème 2.5.1. *Formule du binôme de Newton.*

Soit $(\mathcal{A},+,\times)$ *un anneau.*
Si a *et* b *sont deux éléments de* $\mathcal{A}$ **qui commutent** *(tels que* $a\times b=b\times a$*), alors, pour* $n\in\mathbb{N}$*,*

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}\ a^k\,b^{n-k}\qquad=\sum_{k=0}^{n}\binom{n}{k}\ a^{n-k}\,b^k$$

Preuve.

Démonstration par récurrence sur n, à partir de la formule du triangle de Pascal. Eléments :

$$\begin{aligned}(a+b)^{n+1}=a\,(a+b)^n+b\,(a+b)^n&=\sum_{k=0}^{n}\binom{n}{k}\ a^{k+1}\,b^{n-k}+\sum_{k=0}^{n}\binom{n}{k}\ a^k\,b^{n-(k-1)}\\
&=\sum_{p=1}^{n+1}\binom{n}{p-1}\ a^p\,b^{n+1-p}+\sum_{p=0}^{n}\binom{n}{p}\ a^p\,b^{n+1-p}\\
&=\sum_{p=1}^{n}\binom{n}{p-1}\ a^p\,b^{n+1-p}+\binom{n}{n}+\binom{n}{0}+\sum_{p=1}^{n}\binom{n}{p}\ a^p\,b^{n+1-p}\\
&=\binom{n+1}{0}+\sum_{p=1}^{n}\left(\binom{n}{p-1}+\binom{n}{p}\right)\ a^p\,b^{n+1-p}+\binom{n+1}{n+1}\\
&=\sum_{p=0}^{n+1}\binom{n+1}{p}\ a^p\,b^{n+1-p}\end{aligned}$$

Soit $A=\mathcal{M}_n(\mathbb{K})$, l'ensemble des matrice carrées d'ordre $n>1$, à coefficients dans $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$. On sait que

$$\big(\mathcal{M}_n(\mathbb{K}),+,\times\big)\ \text{est un anneau \underline{non commutatif}.}$$

Par conséquent, avant d'appliquer la formule du binome avec deux éléments de $\mathcal{M}_n(\mathbb{K})$, il faut s'assurer que l'on est bien dans le cas particulier où ces deux éléments commutent.

Théorème 2.5.2. *Formule de Liebniz.*

Soient f *et* g *deux applications de* $\mathbb{R}^p$ *vers* $\mathbb{R}^q$ *et* φ *une application* *bilinéaire* *de* $\mathbb{R}^q\times\mathbb{R}^q$ *vers* $\mathbb{R}^r$*.*
En notant, pour $m=(x_1,x_2,\cdots,x_p)\in\mathbb{R}^p$*,* $\big(\varphi(f,g)\big)(m)=\varphi\big(f(m),g(m)\big)$*, on a :*

$$\textit{Pour } x=x_i\ ,\quad \frac{\partial^n}{\partial x^n}\big(\varphi(f\,,\,g)\big)=\sum_{k=0}^{n}\binom{n}{k}\ \varphi\left(\frac{\partial^k f}{\partial x^k}\,,\,\frac{\partial^{n-k} g}{\partial x^{n-k}}\right)$$

En particulier, pour des fonctions de la seule variable x*,*

- $(f\,g)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}\ f^{(k)}\,g^{(n-k)}$ (dérivation d'un produit ordinaire : $q=r=1$).
- $(<f\,|\,g>)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}\ <f^{(k)}\,|\,g^{(n-k)}>$ (dérivation d'un produit scalaire : $r=1$).
- $(f\wedge g)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}\ f^{(k)}\wedge g^{(n-k)}$ (dérivation d'un produit vectoriel : $q=r=3$).

Preuve.

Démonstration par récurrence sur n, à partir de la formule du triangle de Pascal (quasi la même démonstration que pour le binome de Newton).

< $\mathcal{FIN}$ >