Un regard sur l'infini mathématique

Ivo Dell'Ambrogio
Université de Lille 1

$$\aleph_0 < ? < 2^{\aleph_0}$$

Cours Euler ∞
27 avril 2016

Nombres naturels et “taille” d’un ensemble

Voici les nombres naturels :

$$0, 1, 2, 3, 4, \ldots$$

Leur utilité pratique la plus fondamentale est celle de mesurer la *taille* d’un ensemble d’objets.

Par exemple, voici quelques ensembles de taille 4, c’est à dire, qui contiennent exactement 4 éléments :

$$X = \boxed{\begin{matrix} \clubsuit & \diamondsuit \\ \heartsuit & \spadesuit \end{matrix}} \qquad Y = \{a, b, c, d\}$$

$$Z = \{n \in \mathbb{N} \mid n \geq 4 \text{ et } n < 8\} = \{4, 5, 6, 7\}$$

Nous allons dénoter la taille avec des barres verticales :

$$|X| = 4 \qquad |Y| = 4 \qquad |Z| = 4$$

C'est util d'inclure 0 parmi les nombres naturels, car il fournit la taille de l'ensemble vide :

$$|\emptyset| = 0$$

Par contre, les nombres naturels ne suffisent plus lorsqu'on veut mesurer des ensemble *infinis* !

Par exemple :

$$\mathbb{N} = \{0, 1, 2, \ldots\} \qquad \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

$$\mathbb{Q} : \text{ les nombres rationels} \qquad \mathbb{R} : \text{ les nombres réels}$$

ou l'ensemble de tous les nombres premiers :

$$P = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$$

Qu'est-ce qu'on peut dire sur la taille de tels ensembles ?

$$|\mathbb{N}| = ? \qquad\qquad |\mathbb{R}| = ?$$

On pourrait introduire un nouveau numéro, ∞, et l'appeler "infini". Alors on disposerait des tailles suivantes

$$0, 1, 2, 3, 4, 5, \ldots, \infty$$

et on aurait tout simplement :

$$|P| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{R}| = \infty \qquad \text{etc.}$$

Mais est-ce que cela est vraiment satisfaisant ? Après tout, on a

$$P \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

et donc pourquoi devraient-ils avoir la même taille ?

Qu'est-ce qu'on peut dire sur la taille de tels ensembles ?

$$|\mathbb{N}| = ? \qquad |\mathbb{R}| = ?$$

On pourrait introduire un nouveau numéro, ∞, et l'appeler "infini". Alors on disposerait des tailles suivantes

$$0, 1, 2, 3, 4, 5, \ldots, \xcancel{\infty}$$

et on aurait tout simplement :

$$\xcancel{|P| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{R}| = \infty \qquad \text{etc.}}$$

Mais est-ce que cela est vraiment satisfaisant ? Après tout, on a

$$P \subsetneq \mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$$

et donc pourquoi devraient-ils avoir la même taille ?

D'autre part, considérons les deux ensembles suivants :

$$\mathbb{N}^* = \{1, 2, 3, 4, \ldots\} \qquad \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

Est-ce qu'on veut vraiment que $|\mathbb{N}^*| < |\mathbb{N}|$?

Car il est facile de mettre ces deux ensembles en correspondence :

$$\begin{array}{rcccccc} \mathbb{N}^* = \{ & 1 & 2 & 3 & \ldots & \} \\ & \updownarrow & \updownarrow & \updownarrow & & \\ \mathbb{N} = \{ & 0 & 1 & 2 & \ldots & \} \end{array}$$

Pour des ensembles *finis*, on a bien que deux ensembles ont la même taille précisément si on peut mettre leurs éléments en correspondence bijective :

$$\begin{array}{rcccccc} X = \{ & \clubsuit & \diamondsuit & \heartsuit & \spadesuit & \} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ Y = \{ & a & b & c & d & \} \end{array}$$

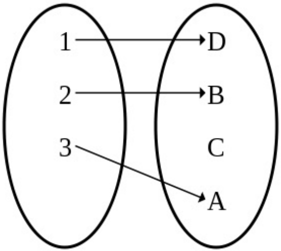
Quelques rappels sur les applications

Soient X et Y deux ensembles quelconques.
Soit $f\colon X \to Y$ une application quelconque.

Définition

On dit que l'application $f\colon X \to Y$ est **injective**, ou une **injection**, si :

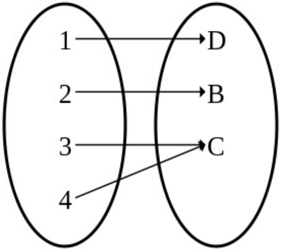
$$\text{Pour tous } x_1, x_2 \in X \text{ différents, alors } f(x_1) \neq f(x_2)\,.$$



Définition

On dit que $f\colon X \to Y$ est **surjective**, ou une **surjection**, si :

$$\text{Pour tout } y \in Y, \text{ il existe au moins un } x \in X \text{ tel que } f(x) = y\,.$$



Définition

On dit que l'application $f\colon X \to Y$ est **bijective**, ou une **bijection**, si :

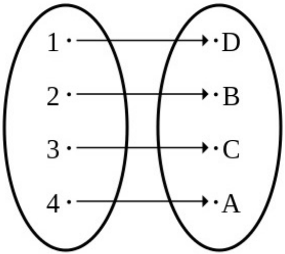
$$f \text{ est surjective et injective} \quad ,$$

ou, de façon équivalente, si :

$$\text{pour tout } y \in Y, \text{ il existe un unique } x \in X \text{ tel que } f(x) = y\,,$$

ou encore, si :

$$\exists\, f^{-1}\colon Y \to X \text{ telle que } f \circ f^{-1} = \mathrm{id}_Y \text{ et } f^{-1} \circ f = \mathrm{id}_X\,.$$



Démontrons rigoureusement ce qu'on avait dit tout à l'heure :

Proposition

Soient X et Y deux ensembles finis. Alors X et Y ont le même nombre d'éléments si et seulement si il existe une bijection $f\colon X \to Y$.

Démonstration :

- Soit n le nombre d'éléments de X et m celui de Y (pour $n, m \in \mathbb{N}$).
- Admettons qu'il existe une application bijective $f\colon X \to Y$.
- En particulier, f est injective, ce qui implique $n \leq m$.
- f est aussi surjective, ce qui implique $n \geq m$.
- On en conclut que $n = m$.
- Inversement, admettons que $n = m$. Nous pouvons choisir un ordre pour les éléments de X et Y :

$$X = \{x_1, \dots, x_n\} \qquad Y = \{y_1, \dots, y_n\}$$

- L'application $f\colon X \to Y$ qui envoit $x_i \mapsto y_i$ $(i = 1, \dots, n)$ est alors une bijection, avec réciproque $y_i \mapsto x_i$. CQFD

Une nouvelle définition

Très bien ! Nous pouvons maintenant utiliser la même idée pour comparer la taille de deux ensemble infinis.

Soient X et Y deux ensembles quelconques (finis ou infinis !).

Définition

On dit que X et Y **sont de même cardinalité**, ou que X et Y **ont le même cardinal**, s'il existe une bijection $f\colon X \to Y$. (Ou de façon équivalente, s'il existe une bijection $g\colon Y \to X$.)

On écrit alors :

$$|X| = |Y|$$

Quelques exemples :

- Nous avons vu qu'il y a une bijection

$$\begin{array}{ccccccc} \mathbb{N}^* = \{ & 1 & 2 & 3 & \dots & \} \\ & \updownarrow & \updownarrow & \updownarrow & & \\ \mathbb{N} = \{ & 0 & 1 & 2 & \dots & \} \end{array}$$

  ce qui démontre que

$$|\mathbb{N}^*| = |\mathbb{N}| .$$

- Il y a aussi une bijection entre $\mathbb{N}$ et $\mathbb{Z}$:

$$\begin{array}{ccccccccccc} \mathbb{N} = \{ & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots & \} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \\ \mathbb{Z} = \{ & 0 & 1 & -1 & 2 & -2 & 3 & -3 & \dots & \} \end{array}$$

  Donc nous avons aussi

$$|\mathbb{N}| = |\mathbb{Z}| .$$

En fait, il y beaucoup d'ensembles qui ont le même cardinal que $\mathbb{N}$ (on en verra d'autres dans les exercices !).

Il convient donc d'introduire un adjectif :

Définition

On dit qu'un ensemble infini X est **dénombrable** si $|X| = |\mathbb{N}|$.

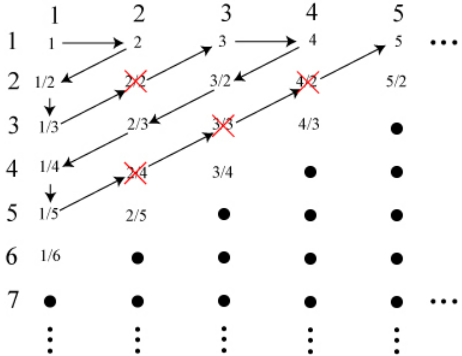
L'idée est qu'une application bijective $f : \mathbb{N} \to X$ n'est rien d'autre qu'un **dénombrement** de tous les éléments de X (une façon de les compter) :

$$\begin{array}{ccccccc} \mathbb{N} = \{ & 0 & 1 & 2 & \dots & \} \\ & \updownarrow & \updownarrow & \updownarrow & & \\ X = \{ & x_0 & x_1 & x_2 & \dots & \} \end{array} \qquad\qquad \begin{array}{ccc} n & \in & \mathbb{N} \\ \big\downarrow & & \big\downarrow f \\ x_n & \in & X \end{array}$$

Voici un autre exemple :

- L'ensemble $\mathbb{Q}$ des nombres rationnels est dénombrable !

  On peut construire une bijection $\mathbb{N} \to \mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x > 0\}$:



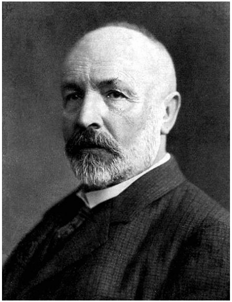
  Il est facile de modifier cela en une bijection $\mathbb{N} \to \mathbb{Q}$ (exercice !).

Mais alors, est-ce qu'ils existent des ensembles infinis non-dénombrables ?

Oui !

Théorème (Georg Cantor 1874)

L'ensemble $\mathbb{R}$ des nombres réels n'est pas dénombrable.



Georg Cantor
1845-1918

Démonstration du Théorème :

- Nous allons démontrer que déjà l'intervalle $]0,1[\subset \mathbb{R}$ est trop gros pour être dénombrable.
  (Il est facile de montrer que, si un ensemble X est dénombrable, alors toute partie $A \subset X$ est soit dénombrable soit finie.)
- Chaque nombre réel $x \in]0,1[$ est déterminé par son développement décimal après la virgule, par exemple :

$$x = \sqrt{2} - 1 = 0,414213562\ldots$$

- Soit $f\colon \mathbb{N} \to]0,1[$ une application quelconque, c'est à dire une liste $x_0, x_1, x_2, \ldots$ de nombres réels entre 0 et 1.

- Nous allons voir que f n'est pas surjective.

  Écrivons cette liste de nombres, avec leurs développements décimaux :

$$
\begin{array}{rlcccccccccc}
x_0 = & 0, & \color{red}{2} & 3 & 0 & 4 & 8 & 9 & 3 & 3 & \ldots \\
x_1 = & 0, & 4 & \color{red}{1} & 4 & 2 & 1 & 3 & 5 & 6 & \ldots \\
x_2 = & 0, & 1 & 1 & \color{red}{9} & 0 & 0 & 9 & 0 & 7 & \ldots \\
x_3 = & 0, & 0 & 0 & 8 & \color{red}{6} & 3 & 0 & 1 & 9 & \ldots \\
x_4 = & 0, & 5 & 0 & 0 & 0 & \color{red}{0} & 0 & 0 & 0 & \ldots \\
x_5 = & 0, & 9 & 9 & 9 & 7 & 0 & \color{red}{5} & 2 & 1 & \ldots \\
\vdots & & & & & & & & \color{red}{\ddots} & &
\end{array}
$$

- Regardons les chiffres sur la diagonale (en rouge).

- Changeons chaqu'un de ces chiffres, par exemple selon le schéma :

$$n \mapsto \begin{cases} n+1 & \text{si } n \neq 9 \\ 0 & \text{si } n = 9 \end{cases}$$

- Nous obtenons de cette façon un nouveau nombre réel :

$$x^* = \ 0, \ 3 \ 2 \ 0 \ 7 \ 1 \ 6 \ \ldots$$

- Par construction, x^* est un nombre réel dans $]0,1[$ et tel que

il diffère de x_0 au 1-er chiffre décimale,

il diffère de x_1 au 2-ème chiffre décimale,

...

il diffère de x_n au $(n+1)$-ème chiffre décimale.

- Donc x^* diffère de tous les x_n, c'est à dire n'appartient pas à l'image de l'application $f : \mathbb{N} \to \mathbb{R}$. Donc f n'est pas surjective.
- Ceci montre qu'il n'existe pas de bijection $f : \mathbb{N} \to \mathbb{R}$.

CQFD

Comparaisons

Pour l'instant, nous savons que : $\quad |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \quad \neq \quad |\mathbb{R}|.$

En effet, on aimerait écrire que : $\quad |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \quad < \quad |\mathbb{R}|.$

Car pour tout ensemble dénombrable X, on trouve une injection $X \to \mathbb{R}$ (il suffit de composer une bijection $X \to \mathbb{N}$ avec l'inclusion $\mathbb{N} \to \mathbb{R}$).

De plus, pour deux ensemble *finis* X et Y, l'existence d'une injection $X \to Y$ implique que $|X| \leq |Y|$.

Définition

Pour deux ensembles X et Y, s'il existe une injection $f : X \to Y$ on écrit

$$|X| \leq |Y|$$

et si de plus $|X| \neq |Y|$, on écrit $|X| < |Y|$.

Quelle sorte de relation entre “cardinalités” est $\leq$? Une relation d'ordre ?

- **Réflexivité :** on a $|X| \leq |X|$, car l'application identité $id_X : X \to X$ est injective.
- **Transitivité :** si $|X| \leq |Y|$ et $|Y| \leq |Z|$, alors $|X| \leq |Z|$, car si on a deux applications injectives $f : X \to Y$ et $g : Y \to Z$, la composée $g \circ f : X \to Z$ est aussi injective.
- **Anti-symétrie :** si $|X| \leq |Y|$ et $|X| \geq |Y|$, est-ce que $|X| = |Y|$?

C'est sûrement le cas pour les ensemble finis.

En général, aussi :

Théorème de l'équivalence de Cantor-Schröder-Bernstein

Soient X et Y deux ensembles quelconques. Si $|X| \leq |Y|$ et $|X| \geq |Y|$, alors $|X| = |Y|$.

La preuve sera dans les exercices.

Nous avons donc la hiérarchie suivante pour les cardinalités qu'on connait :

$$\underbrace{0 < 1 < 2 < 3 < \ldots < n < \ldots}_{\text{cardinaux finis} \quad (n \in \mathbb{N})} \quad \underbrace{< |\mathbb{N}| < |\mathbb{R}|}_{\text{cardinaux infinis}}$$

Est-ce qu'il y en a d'autres ?

$$0 < 1 < 2 < 3 < \ldots < n < \ldots \quad < |\mathbb{N}| < ? < |\mathbb{R}| < ?$$

(On voit par contre qu'il n'y a pas d'autres cardinaux entre les nombres finis et l'infini dénombrable $|\mathbb{N}|$, car tout ensemble X soit il est fini, soit il contient une partie dénombrable et donc $|\mathbb{N}| \leq |X|$.)

Nous pouvons répondre à une de ces questions :

Théorème de Cantor (Georg Cantor 1891)

Soit X un ensemble quelconque, et soit

$$\mathcal{P}(X) = \{A \subseteq X \mid A \text{ est une partie de } X\}$$

l'ensemble des parties de X. Alors

$$|X| < |\mathcal{P}(X)|.$$

Corollaire

Il existe au moins une infinité dénombrable de cardinaux infini :

$$|\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < \ldots |\mathcal{P}^n(\mathbb{R})| < \ldots$$

De plus, on a que $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ (exercice !).

Démonstration du Théorème de Cantor :

- L'application
$$X \longrightarrow \mathcal{P}(X) \qquad x \mapsto \{x\}$$
est injective, ce qui montre que $|X| \leq |\mathcal{P}(X)|$.
- Il nous reste à démontrer que $|X| \neq |\mathcal{P}(X)|$.
Pour cela, il suffira de montrer qu'aucune application $f\colon X \to \mathcal{P}(X)$ ne peut être surjective.
- Soit donc $f\colon X \to \mathcal{P}(X)$ une application quelconque.
- Définissons la partie suivante de X :
$$A \overset{\text{def.}}{=} \{x \in X \mid x \notin f(x)\}\,.$$

$$A = \{x \in X \mid x \notin f(x)\} \quad \in \quad \mathcal{P}(X)$$

- Admettons, par absurde, que $f\colon X \to \mathcal{P}(X)$ soit surjective.
- Dans ce cas, il existe un $x_A \in X$ tel que $f(x_A) = A$.
- Est-ce que $x_A \in A$?
- On a les équivalences suivantes :

$$\begin{aligned} x_A \in A \quad &\Longleftrightarrow \quad x_A \notin f(x_A) && \text{par la définition de } A \\ &\Longleftrightarrow \quad x_A \notin A && \text{car } f(x_A) = A \end{aligned}$$

  ce qui est une contradiction !
- Donc l'élément x_A n'existe pas, et par conséquent f n'est pas surjective. Il ne peut donc exister aucune bijection $f\colon X \to \mathcal{P}(X)$.

CQFD

Remarques finales

Cet argument ressemble beaucoup à celui du **Paradoxe de Russell**, dans sa forme de théorème :

Théorème de Russell (1901)

L'ensemble de tous les ensemble n'existe pas.

Mais il ressemble aussi à l'argument de la diagonale que nous avons utilisé pour montrer que $\mathbb{R}$ est indénombrable. En fait, ce dernier en est le cas spéciale avec $X = \mathbb{N}$, car $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

En réalité, il s'agit à chaque fois de la même preuve : il existe un **"théorème générale de la diagonale"**, qui a comme corollaires le Théorème de Cantor, le Théorème de Russell, et d'autres !

Remarques finales

Il reste encore beaucoup de questions... Par exemple :

- Qu'est-ce qu'un **nombre cardinal**, précisément ? On aimerait le définir comme une classe d'équivalence d'ensembles, par la relation déquivalence "avoir le même cardinal". Mais il s'agirait d'une relation d'équivalence sur l'ensemble de tous les ensembles, qui n'existe pas !

- Est-qu'il existe un cardinal α tel que $|\mathbb{N}| < \alpha < |\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$?

  Ou tel que $|X| < \alpha < |\mathcal{P}(X)|$, si X est infini ?

  Cette question s'appèle **Hypothèse (Généralisée) du Continu**.
  Il a été démontré par Kurt Gödel (1940) et Paul Cohen (1963) que *la réponse peut être OUI ou NON, selon la définition précise de "ensemble" qu'on décide d'utiliser !*

Si vous êtes intéressés à approfondir ces idées, vous pouvez commencer à réfléchir sur la feuille d'exercices après la pause.

La partie des mathématique qui étudie ces questions sur l'infini, depuis déjà plus d'un siècle, est la **Théorie des Ensembles**.

MERCI DE VOTRE ATTENTION !