L3I COMBINATOIRE — 4 : ENSEMBLES ET CARDINAUX INFINIS

Christian RONSE, ICube, Département d'Informatique de l'Université de Strasbourg

Imaginons un hôtel possédant une infinité de chambres, et affichant complet. Un nouveau client se présente et demande une chambre. Le tenancier va le loger en l'envoyant occuper la chambre d'un 1er client, qui déménagera dans celle d'un 2ème client, qui ira dans celle d'un 3ème, etc.

Par définition, un ensemble est infini s'il est équipotent à une de ses parties propres. On voit qu'un ensemble E est infini si et seulement s'il existe une injection $\mathbb{N} \to E : n \mapsto x_n$, en d'autres termes E contient une suite x_n ($n \in \mathbb{N}$) dont les termes sont mutuellement distincts ($x_m \neq x_n$ pour $m \neq n$). En effet, si on a une bijection $E \to P$ pour $P \subset E$, on prend $x \in E \setminus P$ et on définit $x_n = f^n(x)$ ($n \in \mathbb{N}$), et pour $m < n$ on a $f^{n-m}(x) \in P$, donc $f^{n-m}(x) \neq x$ et ainsi $f^n(x) \neq f^m(x)$. Réciproquement, étant donnée une suite x_n ($n \in \mathbb{N}$) avec $x_m \neq x_n$ pour $m \neq n$, on définit la bijection $f : E \to E \setminus \{x_0\}$ par $f(x_n) = x_{n+1}$ ($n \in \mathbb{N}$) et $f(x) = x$ pour $x \in E \setminus \{x_n \mid n \in \mathbb{N}\}$.

La construction des ordinaux de von Neumann, utilisée pour définir les entiers comme ensembles, peut s'étendre au-delà ; le premier ordinal infini est $\mathbb{N}$, qu'on note ω, et ensuite on a :

$$\begin{aligned}
\omega + 1 &= \omega \cup \{\omega\} \ , \\
\omega + 2 &= (\omega + 1) \cup \{\omega + 1\} = \omega \cup \{\omega + 0, \omega + 1\} \ , \\
\omega + 3 &= (\omega + 2) \cup \{\omega + 2\} = \omega \cup \{\omega + 0, \omega + 1, \omega + 2\} \ , \\
&\vdots \quad \vdots \\
\omega + n + 1 &= (\omega + n) \cup \{\omega + n\} = \omega \cup \{\omega + 0, \ldots, \omega + n\} \ , \\
&\vdots \quad \vdots \\
2\omega &= \omega \cup \{\omega + n \mid n \in \omega\} \ , \\
2\omega + 1 &= 2\omega \cup \{2\omega\} \ , \\
&\vdots \quad \vdots \\
(m+1)\omega &= m\omega \cup \{m\omega + n \mid n \in \omega\} \ , \\
&\vdots \quad \vdots \\
\omega^2 &= \bigcup_{m \in \omega \setminus \{0\}} m\omega \ , \\
&\vdots \quad \vdots
\end{aligned}$$

En fait, on définit de manière générale les ordinaux, ils sont inclus les uns dans les autres, et toute famille d'ordinaux comprend un élément minimum. On peut montrer (avec un axiome supplémentaire...) que tout ensemble est équipotent à un ordinal. Un ordinal est un *cardinal* s'il n'est pas équipotent à un plus petit ordinal, et on définit donc le cardinal d'un ensemble E comme l'ordinal minimum parmi tous ceux équipotents à E, et on le notera $card(E)$. Par exemple les naturels sont des cardinaux, ω est un cardinal, et on a $card(\mathbb{N}) = card(\mathbb{Z}) = \omega$.

Donc pour deux ensembles A et B, on a

$$card(A) = card(B) \iff A \text{ est équipotent à } B \ . \qquad (A)$$

Comme les cardinaux sont inclus les uns dans les autres, on a $card(A) \leq card(B)$ ssi A est équipotent à une partie de B. Donc

$$card(A) \leq card(B) \iff \exists \text{ une injection } A \to B \iff \exists \text{ une surjection } B \to A \ . \qquad (B)$$

Nous avons vu qu'un ensemble E est infini ssi il y a une injection $\mathbb{N} \to E$; alors on a $\omega = card(\mathbb{N}) \leq card(E)$. Donc ω *est le plus petit cardinal infini.* On appelle *dénombrable* un ensemble infini de cardinal ω, c.-à-d. équipotent à $\mathbb{N}$. Par exemple $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^n$ et $\mathbb{Z}^n$ $(n \geq 1)$ sont dénombrables. Il existe des ensembles infinis non dénombrables, par exemple $\mathbb{R}$, voir plus loin.

On peut ignorer la notion d'ordinal et utiliser les équivalences (A) et (B) comme base pour comparer la taille de deux ensembles. Notons que $card(A) = card(B)$ ssi $card(A) \leq card(B)$ et $card(B) \leq card(A)$, effectivement on a :

Théorème de Cantor-Bernstein : *Deux ensembles A et B sont équipotents si et seulement s'il existe une injection $A \to B$ et une injection $B \to A$.*

En effet, si A est équipotent à B, la bijection $A \to B$ et son inverse $B \to A$ sont des injections. Réciproquement, supposons deux injections $f : A \to B$ et $g : B \to A$. Soient $X = Im(g)$ et $h = g \circ f$; donc B est équipotent à X et h est une injection $A \to X$. Posons $A_1 = A \setminus X$ et $A_2 = \{h^n(x) \mid x \in A_1,\ n \in \mathbb{N}^*\}$; donc $A_2 \subseteq X$ et ainsi A_1, A_2 et $X \setminus A_2$ sont mutuellement disjoints et recouvrent A. Nous définissons $k : A \to A$ par $k(x) = h(x)$ pour $x \in A_1 \cup A_2$ et $k(x) = x$ pour $x \in X \setminus A_2$. Alors k est injective et $Im(k) = A_2 \cup (X \setminus A_2) = X$. Donc A est équipotent à X. Par conséquent, A et B, tous deux équipotents à X, sont équipotents.

Le résultat suivant est très connu, il implique que pour tout ensemble infini, il en existe un autre de cardinal plus grand.

Théorème de Cantor : *Pour tout ensemble E, il existe une injection $E \to \mathcal{P}(E)$, mais il n'existe pas de surjection $E \to \mathcal{P}(E)$. Donc $card(E) < card(\mathcal{P}(E))$.*

L'application $E \to \mathcal{P}(E) : x \mapsto \{x\}$ est injective. Soit $f : E \to \mathcal{P}(E)$ et posons $A = \{x \in E \mid x \notin f(x)\}$. Si $A = f(x)$ pour $x \in E$, alors on a $x \in f(x) \Leftrightarrow x \in A \Leftrightarrow x \notin f(x)$, une contradiction ; donc $A \neq f(x)$ pour tout $x \in X$, et ainsi f n'est pas surjective. L'injection $E \to \mathcal{P}(E)$ donne $card(E) \leq card(\mathcal{P}(E))$, et l'absence de surjection $E \to \mathcal{P}(E)$ donne $card(\mathcal{P}(E)) \not\leq card(E)$; donc $card(E) < card(\mathcal{P}(E))$.

Dans le cas où E est dénombrable, cet argument est appelé *diagonalisation*, il permet de montrer que pour toute suite dénombrable de parties de E, on peut construire une partie de E n'en faisant pas partie. On note les éléments de E x_n, $n \in \mathbb{N}$. Toute partie A de E correspond alors à une fonction $f : \mathbb{N} \to \{0, 1\}$, avec pour tout $n \in \mathbb{N}$, $f(n) = 1$ si $x_n \in A$ et $f(n) = 0$ si $x_n \notin A$. Alors pour une suite dénombrable A_n, $n \in \mathbb{N}$, de parties de E correspondant aux fonctions f_n, on construit une partie A de E correspondant à la fonction $f : \mathbb{N} \to \{0, 1\}$ donnée par

$$\forall n \in \mathbb{N}, \qquad f(n) = 1 - f_n(n) \ .$$

Alors pour tout $n \in \mathbb{N}$ on a $f(n) \neq f_n(n)$, donc $f \neq f_n$ et ainsi $A \neq A_n$.

Par exemple pour E fini avec $card(E) = n$, on a $card(\mathcal{P}(E)) = 2^n$, où $2^n > n$ (même pour $n = 0$). Dans le cas infini, on peut montrer que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$ (ou à $2^{\mathbb{N}}$). Donc $\mathbb{R}$ n'est pas dénombrable. On appelle *puissance du continu* le cardinal de $\mathbb{R}$. Par exemple $card(\mathbb{N}^{\mathbb{N}}) = card(\mathbb{R})$, tandis que $card(\mathcal{P}(\mathbb{R})) = card(\mathbb{R}^{\mathbb{R}})$ est plus grand que la puissance du continu.

Le fait que $\mathbb{R}$ soit non dénombrable est à la base de l'analyse. Si $\mathbb{R}$ était dénombrable, toutes les intégrales seraient égales à 0.

Les axiomes de la théorie des ensembles ne permettent pas de déterminer s'il existe ou non une infinité intermédiaire entre le dénombrable et le continu (c.-à-d. un cardinal ε tel que $\omega < \varepsilon < card(\mathbb{R})$). L'*hypothèse du continu* postule qu'il n'y en a pas, donc que toute partie de $\mathbb{R}$ est soit dénombrable, soit de la puissance du continu.