3 Aparté : comparaison des cardinaux infinis

Section hors-programme

Cet aparté est présenté à titre purement culturel et ne figure pas au programme de B/L.

Bien que l'ensemble des entiers naturels et l'ensemble des nombres réels soient tous deux infinis, il semble intuitivement qu'il y ait incommensurablement plus d'éléments dans $\mathbb{R}$ que dans $\mathbb{N}$, comme si, en un sens, l'infinité de $\mathbb{R}$ était d'un « ordre » supérieur à celle de $\mathbb{N}$... ce que ne reflètent pas vraiment les écritures $|\mathbb{R}| = +\infty$ et $|\mathbb{N}| = +\infty$!

La notion d'application permet de donner une assise formelle à l'idée de comparaison de cardinaux infinis. En effet, on a vu que si A et B sont des ensembles **finis**, on a $|A| \leqslant |B|$ si et seulement s'il existe une injection de A dans B, et $|A| = |B|$ si et seulement s'il existe une bijection de A dans B. On peut transformer cette propriété en définition pour l'appliquer à des ensembles éventuellement infinis :

Définition A (Comparaison de cardinaux)**.** Soient A et B deux ensembles.

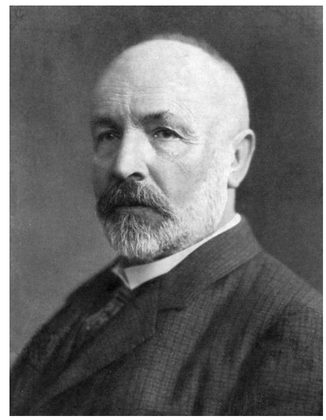
On dit que *le cardinal de A est inférieur ou égal au cardinal de B* si et seulement s'il existe une injection de A dans B. On note alors $|A| \leqslant |B|$.

On dit que A et B ont *même cardinal*, ou qu'ils sont *équipotents*, si et seulement s'il existe une bijection de A dans B. On note alors $|A| = |B|$.

Si $|A| \leqslant |B|$ mais si l'on n'a pas $|B| \leqslant |A|$, on dit que A est de cardinal *strictement inférieur à B* et on note $|A| < |B|$.

Cette définition est somme toute assez raisonnable : dire qu'il existe une bijection entre A et B signifie que l'on peut mettre en correspondance chaque élément de B avec un et un seul élément de A, et donc qu'il y a « autant d'éléments dans A que dans B »...

Cette idée, on va le voir, ouvre pourtant la voie à une série de résultats pour le moins étonnants.



Georg Cantor (1845 – 1918), considéré comme le créateur de la théorie des ensembles, fut à l'origine d'un véritable changement de paradigme lorsqu'il étendit aux ensembles infinis les considérations de cardinalité réservées depuis Aristote aux ensembles finis. Le caractère dérangeant et non constructiviste de certains de ses résultats lui valut l'opposition farouche de nombre de ses contemporains, dont Kronecker et, plus tard, des intuitionnistes menés par Brouwer.
Les concepts et résultats présentés dans cette section sont en grande partie issus de ses travaux à l'importance philosophique considérable.

3.1 Premiers exemples

Commençons par examiner quelques exemples.

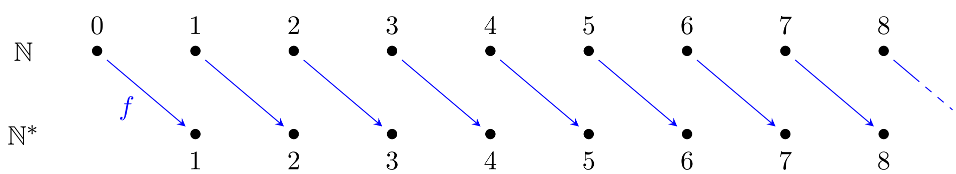
Exemple ($\mathbb{N}$ et $\mathbb{N}^*$ ont même cardinal)**.** L'application

$$f : \begin{array}{rcl} \mathbb{N} & \longrightarrow & \mathbb{N}^* \\ n & \longmapsto & n+1 \end{array}$$

est bijective. Ainsi, on a $|\mathbb{N}| = |\mathbb{N}^*|$: il existe autant d'entiers naturels que d'entiers naturels non nuls.

Pour vérifier que f est bijective, on peut par exemple exhiber sa réciproque

$$f^{-1} : \begin{array}{rcl} \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ n & \longmapsto & n-1. \end{array}$$



L'exemple ci-dessus illustre un principe important : dans les ensembles infinis, il n'est pas correct de dire que si $A \subsetneq B$ alors $|A| < |B|$. En d'autres termes, A et B peuvent avoir le même nombre d'éléments même si B contient A *et* certains éléments supplémentaires.

Exemple ($\mathbb{N}$ et $2\mathbb{N}$ ont même cardinal)**.** On peut aller plus loin et montrer qu'il existe le même nombre d'entiers naturels que d'entiers naturels *pairs*. En effet, si l'on note $2\mathbb{N}$ l'ensemble des entiers naturels pairs, alors l'application

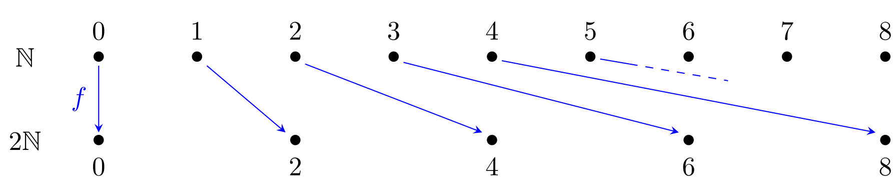
Cette affirmation ne veut bien sûr pas dire que tous les entiers naturels sont pairs !

$$f : \begin{array}{rcl} \mathbb{N} & \longrightarrow & 2\mathbb{N} \\ n & \longmapsto & 2n \end{array}$$

est bijective : si $n, n' \in \mathbb{N}$ sont tels que $f(n) = f(n')$, alors $2n = 2n'$ donc $n = n'$ (ce qui assure l'injectivité de f), et si $p \in 2\mathbb{N}$, on peut par définition de l'ensemble $2\mathbb{N}$ écrire p sous la forme $2k$ avec $k \in \mathbb{N}$, soit $p = f(k)$ (d'où la surjectivité de f).

On pouvait aussi exhiber la bijection réciproque

$$f^{-1} : \begin{array}{rcl} 2\mathbb{N} & \longrightarrow & \mathbb{N} \\ p & \longmapsto & \frac{p}{2}. \end{array}$$



> Il en va bien sûr de même pour l'ensemble $2\mathbb{N}+1$ des entiers naturels impairs : ainsi, $\mathbb{N}$ peut être partitionné en deux sous-ensembles qui sont des copies de $\mathbb{N}$ lui-même !

En 1632, Galilée s'étonnait déjà du fait qu'il existe autant de nombres entiers que de carrés de nombres entiers, c'est-à-dire du fait que les ensembles $\mathbb{N}$ et $\{n^2 : n \in \mathbb{N}\}$ soient en bijection... et ce, malgré la raréfaction des nombres de la forme n^2 à mesure que l'on parcourt l'ensemble des entiers naturels !

Fait plus troublant encore : on peut trouver dans $\mathbb{N}$ une *infinité* de copies de $\mathbb{N}$ deux à deux disjointes, par exemple les ensembles $A_p := \{p^{n+1}, n \in \mathbb{N}\} \subset \mathbb{N}$ pour p premier, c'est-à-dire

$$A_2 = \{2, 4, 8, \dots\}, \quad A_3 = \{3, 9, 27, \dots\}, \quad A_5 = \{5, 25, 125, \dots\}, \ \dots$$

Il est amusant de constater que ces ensembles ne constituent pas une partition de $\mathbb{N}$ car ils ne parviennent même pas à couvrir tout $\mathbb{N}$ (par exemple, l'entier 6 n'est pas une puissance de nombre premier) !

3.2 Dénombrabilité

Malgré ces propriétés étonnantes, l'ensemble $\mathbb{N}$ est, en un certain sens, le *plus petit ensemble infini* :

Une illustration des propriétés vertigineuses de l'ensemble des entiers naturels a été proposée au début du XX$^{\text{ème}}$ siècle par le mathématicien allemand David Hilbert dans une expérience de pensée connue sous le nom d'« Hôtel de Hilbert ». Cette dernière est présentée dans une courte vidéo accessible grâce au code ci-dessous :

Proposition B. Si A est un ensemble infini, alors $|\mathbb{N}| \leqslant |A|$.

Démonstration de la proposition B — Si A est infini, on peut appliquer le protocole suivant pour définir une suite d'éléments de A :

- On choisit un élément dans A, que l'on note x_0.
- On choisit un élément dans A distinct de x_0, que l'on note x_1.
- On choisit un élément dans A distinct de x_0 et x_1, que l'on note x_2.
- On procède de même pour tout entier naturel n : supposant les éléments $x_0, \dots, x_n$ déjà sélectionnés, on choisit un élément dans A distinct de $x_0, \dots, x_n$ (ce qui est possible puisque A est infini), et on le note x_{n+1}.

On dispose ainsi d'une collection $\{x_n,\, n \in \mathbb{N}\}$ d'éléments de A deux à deux distincts, ce qui signifie que l'application

$$\begin{aligned} f : \mathbb{N} &\longrightarrow A \\ n &\longmapsto x_n \end{aligned}$$

est une injection. Ainsi, on a bien $|\mathbb{N}| \leqslant |A|$. □

Tout ensemble infini contient donc une copie de $\mathbb{N}$. En s'inspirant de la preuve ci-dessus, on peut démontrer qu'un ensemble infini est en *bijection* avec $\mathbb{N}$ dès lors que ses éléments peuvent être numérotés.

Proposition C. Si A est un ensemble et s'il est possible de définir une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de A deux à deux distincts tels que l'on ait

$$A = \{x_n,\, n \in \mathbb{N}\},$$

alors A est équipotent à $\mathbb{N}$, c'est-à-dire que $|A| = |\mathbb{N}|$.

Démonstration de la proposition C — Sous l'hypothèse de la proposition, l'application

$$\begin{aligned} f : \mathbb{N} &\longrightarrow A \\ n &\longmapsto x_n \end{aligned}$$

est injective (car les x_n sont deux à deux distincts) et surjective (car A est l'ensemble des x_n par hypothèse) : elle est donc bijective, ce qui permet d'écrire que $|A| = |\mathbb{N}|$. □

Exemple D ($\mathbb{N}$ et $\mathbb{Z}$ ont même cardinal)**.** On peut numéroter les éléments de $\mathbb{Z}$ de la façon suivante : on note $x_0 = 0$, $x_1 = 1$, $x_2 = -1$, $x_3 = 2$, $x_4 = -2$ et ainsi de suite en alternant entre entiers positifs et négatifs. Ce faisant, on numérote bien tous les entiers relatifs sans numéroter deux fois aucun d'entre eux : on en déduit que $|\mathbb{Z}| = |\mathbb{N}|$ d'après la proposition C. On peut donc affirmer (et cela ne nous étonne plus guère !) qu'il existe le même nombre d'entiers relatifs que d'entiers naturels.

La numérotation explicite est définie par la règle suivante :

$$x_n = \begin{cases} -\dfrac{n}{2} & \text{si } n \text{ est pair} \\[2mm] \dfrac{n+1}{2} & \text{si } n \text{ est impair.} \end{cases}$$

Entier		−4	−3	−2	−1	0	1	2	3	4	
	...	•	•	•	•	•	•	•	•	•	...
Numéro		8	6	4	2	0	1	3	5	7	

Ce principe de numérotation justifie l'emploi de la terminologie suivante :

Définition E (Ensemble dénombrable)**.** Un ensemble infini A est dit *dénombrable* lorsque $|A| = |\mathbb{N}|$, c'est-à-dire lorsqu'il peut s'écrire sous la forme

$$A = \{x_n,\, n \in \mathbb{N}\}$$

avec les x_n deux à deux distincts.

Un ensemble non dénombrable est dit *indénombrable*.

On a donc montré que les ensembles $\mathbb{N}^*$, $2\mathbb{N}$ et $\mathbb{Z}$ sont dénombrables. Avant de statuer sur la dénombrabilité d'autres ensembles usuels, dotons-nous de quelques résultats généraux sur l'équipotence.

3.3 Quelques propriétés générales sur l'équipotence

Si A et B sont deux ensembles tels que $|A| = |B|$, il existe par définition une bijection $f : A \to B$, donc il existe aussi une bijection de B dans A (sa réciproque f^{-1}). Ainsi, on a la propriété suivante :

$$|A| = |B| \iff |B| = |A|,$$

c'est-à-dire que la relation d'équipotence est *symétrique*.

Si C est un troisième ensemble tel qu'il existe une bijection $g : B \to C$, alors $g \circ f$ est une bijection de A dans C. On peut donc écrire

$$\big(|A| = |B| \quad \text{et} \quad |B| = |C|\big) \implies |A| = |C|,$$

c'est-à-dire que la relation d'équipotence est *transitive*.

La composée de deux bijections est en effet une bijection (voir l'exercice 34 accompagnant ce chapitre.

Les bijections étant par ailleurs des injections, on a l'implication

$$|A| = |B| \implies (|A| \leqslant |B| \quad \text{et} \quad |B| \leqslant |A|)\,.$$

L'implication réciproque est quant à elle moins évidente : elle est fournie par le théorème suivant, qui fait l'objet de l'exercice 40 de ce chapitre.

Ces résultats sont d'une extrême trivialité si les cardinaux de A et B sont finis, mais le cas intéressant est justement le cas infini !

Théorème F (de Cantor-Bernstein)**.** Soient A et B deux ensembles. S'il existe une injection de A dans B et une injection de B dans A, alors il existe une bijection entre A et B.

On a donc bien la rassurante équivalence suivante :

$$|A| = |B| \iff (|A| \leqslant |B| \quad \text{et} \quad |B| \leqslant |A|)\,.$$

On dit cette fois que la relation d'ordre $\leqslant$ entre les cardinaux d'ensembles est *antisymétrique*.

Corollaire G. Si A est un ensemble infini indénombrable et si $A \subset B$, alors B est un ensemble infini indénombrable.

Démonstration du corollaire G — Plaçons-nous sous les hypothèses de la proposition et supposons que B soit dénombrable. Il existe alors une bijection $f : B \to \mathbb{N}$. La restriction $f|_A$ de f à A est alors une injection de A dans $\mathbb{N}$, si bien que $|A| \leqslant |\mathbb{N}|$. Or on sait que $|\mathbb{N}| \leqslant |A|$ (puisque A est infini), donc $|\mathbb{N}| = |A|$, contrairement à l'hypothèse. Ainsi, l'ensemble B est bien indénombrable. □

Le fait que la restriction d'une application injective est injective est démontré dans l'exercice 32.

On démontrera en exercice plusieurs autres propriétés de la relation d'ordre $\leqslant$ entre cardinaux infinis.

Théorème H (de Cantor). Pour tout ensemble A (fini ou infini), on a $|A| < |\mathcal{P}(A)|$.

Démonstration du théorème H — Soit A un ensemble. L'application

$$\begin{aligned} f : A &\longrightarrow \mathcal{P}(A) \\ x &\longmapsto \{x\} \end{aligned}$$

étant clairement injective, on a $|A| \leqslant |\mathcal{P}(A)|$. Il reste donc à montrer qu'il n'existe pas d'application injective de $\mathcal{P}(A)$ dans A, ce qui revient d'après le théorème de Cantor-Bernstein à montrer qu'il n'existe pas d'application *bijective* $g : A \to \mathcal{P}(A)$.

Raisonnons par l'absurde et supposons qu'il existe une telle bijection, et considérons l'ensemble

$$D := \{x \in A \, : \, x \notin g(x)\}.$$

La notation $x \notin g(x)$, troublante de prime abord, a bien un sens puisque si $x \in A$, l'image $g(x)$ est une partie de A !

Cet ensemble, par définition, est bien une partie de A ; il doit donc admettre un antécédent $a \in A$ par g, c'est-à-dire que $g(a) = D$. Alors de deux choses l'une :

- Si $a \in D$, alors $a \notin g(a) = D$ par définition de D, ce qui est contradictoire.
- Si $a \notin D$, soit $a \notin g(a)$, on peut en déduire par définition de D que $a \in D$, ce qui est encore une fois contradictoire.

On aboutit dans tous les cas à une contradiction, ce qui montre que A et $\mathcal{P}(A)$ ne sont pas en bijection et clôt la preuve. $\square$

Le théorème de Cantor nous fournit un premier exemple d'ensemble indénombrable : il montre que $\mathbb{N}$ ne peut être mis en bijection avec l'ensemble de ses parties, c'est-à-dire que $\mathcal{P}(\mathbb{N})$ est indénombrable. Il résulte aussi du théorème de Cantor que le cardinal de $\mathcal{P}(\mathbb{N})$ est strictement inférieur à celui de $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, et ainsi de suite. En notant symboliquement

La lettre $\aleph$ se lit « aleph » ; cette fois, il ne s'agit d'une lettre grecque mais de la première lettre de l'alphabet hébraïque !

$$\aleph_0 := |\mathbb{N}|, \quad 2^{\aleph_0} := |\mathcal{P}(\mathbb{N})|, \quad 2^{2^{\aleph_0}} := \big|\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)\big|$$

et ainsi de suite, on a donc

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

Les cardinaux ci-dessus représentent divers « degrés d'infinité » ; à la suite de Cantor, on leur donne le nom de *nombres transfinis*.

3.4 Dénombrabilité d'ensembles classiques

On peut à présent statuer sur la dénombrabilité de certains ensembles de référence :

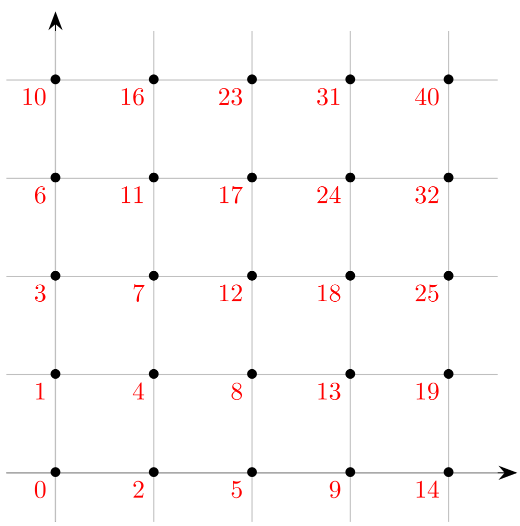
Théorème I (Dénombrabilité d'ensembles célèbres)**.**

- $\mathbb{Z}$ est dénombrable.
- $\mathbb{N}^2 = \{(a,b) \ : \ a,b \in \mathbb{N}\}$ est dénombrable.
- $\mathbb{Q}$ est dénombrable.

Démonstration du théorème I — La dénombrabilité de $\mathbb{Z}$ a été établie dans l'exemple D.

Pour montrer que $\mathbb{N}^2$ est dénombrable, il suffit de remarquer que l'on peut numéroter ses éléments en partant de 0 puis en décrivant chaque ensemble diagonal $A_n := \{(a,b) \in \mathbb{N}^2 \ : \ a+b=n\}$ de gauche à droite avant de passer au suivant, comme sur le schéma ci-dessous :

On peut démontrer que la règle de numérotation appliquée revient à associer au couple (a,b) le numéro $a + \frac{(a+b)(a+b+1)}{2}$.



Le même raisonnement peut être utilisé pour montrer que l'ensemble $\mathbb{N}^n$ est dénombrable quel que soit $n \geqslant 1$.

Ainsi, on a bien $|\mathbb{N}^2| = |\mathbb{N}|$.

« Je le vois, mais je ne le crois pas », écrivit Cantor à Dedekind (en français dans le texte) au sujet de ce résultat.

Le même type de numérotation s'applique à $\mathbb{N}\times\mathbb{Z}^*$, en alternant les points du plan situés au-dessus de l'axe des ordonnées (c'est-à-dire les éléments de $\mathbb{N}\times\mathbb{N}^*$) et ceux situés en-dessous (les éléments de $\mathbb{N}\times\mathbb{Z}^*_-$). On en déduit que $|\mathbb{N}\times\mathbb{Z}^*| = |\mathbb{N}|$.

Or l'application

$$f : \begin{array}{rcl} \mathbb{Q} & \longrightarrow & \mathbb{N} \times \mathbb{Z}^* \\ \frac{p}{q} \text{ irréductible} & \longmapsto & (p,q) \end{array}$$

est une injection de $\mathbb{Q}$ dans $\mathbb{N} \times \mathbb{Z}^*$ puisqu'un élément $(p,q) \in \mathbb{N} \times \mathbb{Z}^*$ ne peut admettre que le nombre $\frac{p}{q}$ pour antécédent (ce qui est le cas si $\frac{p}{q}$ est irréductible, sinon (p,q) n'admet aucun antécédent). On en déduit que $|\mathbb{Q}| \leqslant |\mathbb{N} \times \mathbb{Z}^*|$, soit $|\mathbb{Q}| \leqslant |\mathbb{N}|$: ainsi, $\mathbb{Q}$ est bien dénombrable. □

Le fait de demander à la fraction $\frac{p}{q}$ d'être irréductible assure que l'application f est bien définie : sans cela, il serait impossible de savoir si l'on associe au rationnel $\frac{2}{3} = \frac{4}{6}$ le couple $(2,3)$ ou le couple $(4,6)$.

La dénombrabilité de $\mathbb{Q}$ est l'exemple emblématique des résultats surprenants de la théorie de l'équipotence : alors même qu'il est possible de trouver des nombres rationnels dans n'importe quel intervalle de $\mathbb{R}$ de longueur strictement positive (voir le chapitre 3), ces nombres sont exactement aussi nombreux que les nombres entiers, dont la répartition le long de $\mathbb{R}$ est bien moins dense.

Remarque — *On ne prétend pas, en revanche, pouvoir énumérer les éléments de $\mathbb{Q}$ dans l'ordre croissant ! Une numérotation explicite de $\mathbb{Q}$ inspirée de la preuve ci-dessus est la suivante :*

$$x_0 = 0, \quad x_1 = \frac{1}{1}, \quad x_2 = -\frac{1}{1}, \quad x_3 = \frac{2}{1}, \quad x_4 = -\frac{2}{1}, \quad x_5 = \frac{1}{2},$$
$$x_6 = -\frac{1}{2}, \quad x_7 = \frac{3}{1}, \quad x_8 = -\frac{3}{1}, \quad x_9 = \frac{1}{3}, \quad x_{10} = -\frac{1}{3}, \quad x_{11} = \frac{2}{3}, \quad x_{12} = -\frac{2}{3}, \quad \ldots$$

Nombre	-3	-2	-1	$-\frac{2}{3}$	$-\frac{1}{2}$	$-\frac{1}{3}$	0	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	1	2	3
Numéro	8	4	2	12	6	10	0	9	5	11	1	3	7

Il est naturel de pousser ce questionnement à l'étape suivante et de se demander si l'ensemble $\mathbb{R}$ est lui aussi dénombrable. La réponse est cette fois négative :

Théorème J (Indénombrabilité d'ensembles célèbres)**.**

- L'intervalle $[0,1]$ est indénombrable.
- $\mathbb{R}$ est indénombrable.
- $\mathbb{R} \setminus \mathbb{Q}$ est indénombrable.

Démonstration du théorème J — On va au préalable montrer par l'absurde que l'intervalle $[0,1[$ est indénombrable. Supposons donc que cet ensemble est dénombrable et écrivons-le sous la forme

$$[0,1[= \{x_n,\ n \in \mathbb{N}^*\}.$$

On commence ici la numérotation à 1 pour ne pas avoir à considérer la n-ème décimale de x_{n+1} dans la suite de la démonstration, mais il est bien évident que cela ne change rien à l'affaire.

Définissons à présent le réel x comme l'élément de $[0,1[$ dont pour tout $n \in \mathbb{N}^*$, la n-ième décimale vaut 1 si la n-ième décimale de x_n vaut 0, et vaut 0 sinon. Par exemple, dans la situation représentée ci-dessous, on a $x = 0,01100...$:

$$\begin{array}{lcl}
x_1 = 0,\ 3\ 1\ 4\ 8\ 2\ \ldots & \longrightarrow & 0 \\
x_2 = 0,\ 7\ 0\ 3\ 1\ 7\ \ldots & \longrightarrow & 1 \\
x_3 = 0,\ 9\ 0\ 0\ 1\ 2\ \ldots & \longrightarrow & 1 \\
x_4 = 0,\ 4\ 9\ 0\ 8\ 1\ \ldots & \longrightarrow & 0 \\
x_5 = 0,\ 4\ 7\ 5\ 6\ 6\ \ldots & \longrightarrow & 0
\end{array}$$

La démonstration donnée ici est connue sous le nom d'*argument diagonal de Cantor*.

Par construction, le réel x est un élément de $[0,1[$, et pour tout $n \in \mathbb{N}^*$, il diffère du réel x_n par sa n-ième décimale au moins. Ainsi, il existe un élément de $[0,1[$ qui ne soit égal à aucun des x_n, contrairement à l'hypothèse que nous avons faite. On en déduit que $[0,1[$ est indénombrable.

Une conséquence immédiate de ce résultat et de la proposition G est que $[0,1]$ et $\mathbb{R}$, qui contiennent $[0,1[$, sont eux aussi indénombrables.

Montrons enfin que $\mathbb{R} \setminus \mathbb{Q}$ est indénombrable. On raisonne une fois encore par l'absurde en supposant qu'il soit dénombrable et en le notant sous la forme $\{x_n,\ n \in \mathbb{N}\}$. Comme $\mathbb{Q}$ est dénombrable, on peut aussi le noter sous la forme $\{y_n,\ n \in \mathbb{N}\}$. En définissant pour tout $n \in \mathbb{N}$ les nombres $z_{2n} = x_n$ et $z_{2n+1} = y_n$, on voit que l'ensemble

$$\{z_n,\ n \in \mathbb{N}\} = \{z_0, z_1, z_2, z_3, z_4, \ldots\} = \{x_0, y_0, x_1, y_1, \ldots\}$$

Cet argument permet plus généralement de montrer que l'union de deux ensembles dénombrables est elle-même dénombrable, et donc que le complémentaire d'un ensemble dénombrable dans un ensemble indénombrable ne peut être qu'indénombrable.

contient tous les éléments de $\mathbb{R} \setminus \mathbb{Q}$ et de $\mathbb{Q}$, donc tous les réels. Ainsi, on a montré que $\mathbb{R}$ est dénombrable, ce qui contredit le point précédent. On en déduit que $\mathbb{R} \setminus \mathbb{Q}$ est lui aussi indénombrable. □

On dit qu'un ensemble équipotent à $\mathbb{R}$ a la *puissance du continu* (voir le Zoom page suivante) : cette terminologie est justifiée par le fait que $\mathbb{R}$ est l'ensemble des nombres représentés en traçant une ligne continue jusqu'à l'infini. Le cardinal de $\mathbb{R}$ (la fameuse *puissance du continu*) est symboliquement noté $\mathfrak{c}$.

On montrera dans l'exercice 50 que $\mathfrak{c} = 2^{\aleph_0}$.

L'hypothèse du continu

Il est possible de trouver des ensembles dénombrables bien plus imposants que $\mathbb{Q}$ (par exemple l'ensemble des nombres réels *algébriques*, c'est-à-dire racines de polynômes à coefficients entiers), ainsi que des ensembles indénombrables bien plus restrictifs que $\mathbb{R}$ (par exemple l'ensemble des nombres réels non algébriques, aussi dits *transcendants*). Cependant, on remarque empiriquement que tous les exemples connus de parties indénombrables de $\mathbb{R}$ peuvent être mis en bijection avec $\mathbb{R}$ lui-même. C'est cette observation qui conduisit Cantor à formuler l'*hypothèse du continu*, qui s'énonce comme suit :

Toute partie infinie de $\mathbb{R}$ *peut être mise en bijection soit avec* $\mathbb{N}$*, soit avec* $\mathbb{R}$*.*

Cette conjecture stipule qu'il n'existe pas de degré d'infinité intermédiaire entre l'infini dénombrable $\aleph_0$, cardinal de $\mathbb{N}$, et la puissance du continu $\mathfrak{c}$, cardinal de $\mathbb{R}$.

On peut établir théoriquement l'existence d'un plus petit nombre transfini strictement supérieur à $\aleph_0$, que l'on note $\aleph_1$. L'hypothèse du continu se reformule en disant que $\aleph_1$ est égal à la puissance du continu $\mathfrak{c}$, c'est-à-dire que $\aleph_1 = 2^{\aleph_0}$. Sous cette hypothèse, on peut montrer que le nombre transfini directement supérieur à $\aleph_1$, noté $\aleph_2$, vaut $2^{\aleph_1} = 2^{2^{\aleph_0}}$, et ainsi de suite : la chaîne d'égalités

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

donnée page 6 ne se contenterait donc pas de comparer entre eux *certains* nombres transfinis, mais donnerait la liste de *tous* les « degrés d'infinité » successifs.

Mais alors, l'hypothèse du continu est-elle vraie ou fausse ? On aurait pu penser que ce problème en apparence relativement simple – l'existence d'un ensemble E tel que $\mathbb{N} \subset E \subset \mathbb{R}$ et qui ne soit en bijection ni avec $\mathbb{N}$, ni avec $\mathbb{R}$ – ne résisterait pas longtemps à l'analyse d'un mathématicien tel que Cantor. Ce dernier se cassa pourtant les dents sur l'hypothèse du continu, qui l'obséda jusqu'à la fin de sa vie et dont la validité resta un mystère mathématique pendant des décennies.

David Hilbert, en 1900, fit figurer la preuve de l'hypothèse du continu en tête d'une liste de 23 problèmes majeurs non résolus (les fameux *problèmes de Hilbert*), et déclarait encore trente ans plus tard : « *Il n'y a pas, pour nous, d'*ignorabimus [*en sciences naturelles*]*. Nous devons savoir, et nous saurons* ». La suite de l'histoire réservait pourtant un rebondissement spectaculaire. En 1938, Kurt Gödel établit que l'hypothèse du continu n'est pas réfutable dans le cadre de la théorie des ensembles classique. En 1963, Paul Cohen prouva qu'elle n'est pas non plus démontrable dans le cadre de cette théorie : elle est donc indécidable (voir le Zoom sur l'axiomatique dans le chapitre « Logique et ensembles ») !

On peut voir dans cette réponse inattendue l'apothéose d'une théorie dérangeante par bien des aspects, de l'aveu même de son créateur. L'aventure n'est cependant pas terminée, et certains chercheurs sont toujours en quête d'axiomes supplémentaires naturels pour enrichir la théorie des ensembles et pouvoir trancher, dans cette nouvelle axiomatique, en faveur ou en défaveur de l'hypothèse du continu...