Martin Aigner - Günter M. Ziegler
Traduction : Nicolas Puech

Raisonnements divins

Quelques démonstrations mathématiques particulièrement élégantes

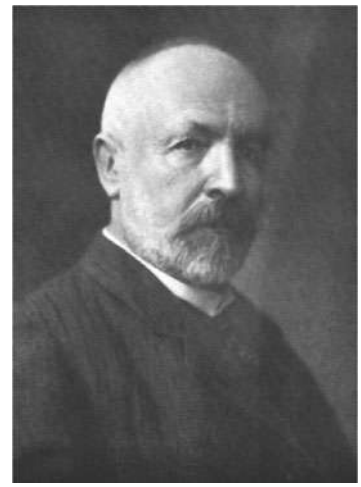
Troisième édition

Springer

Ensembles, fonctions et hypothèse du continu

Chapitre 17

La théorie des ensembles, élaborée par Georg Cantor dans la seconde moitié du 19^e siècle, a profondément transformé les mathématiques. Les mathématiques modernes sont inconcevables sans le concept d'ensemble et, comme l'a affirmé David Hilbert : « Personne ne nous chassera du paradis (de la théorie des ensembles) que Cantor a créé pour nous ».



Georg Cantor

L'un des concepts fondamentaux introduits par Cantor est la notion de *taille* ou de *cardinal* d'un ensemble M, noté $|M|$. Pour les ensembles finis, la notion ne présente pas de difficulté : on compte simplement le nombre d'éléments et l'on dit que M est un n-ensemble ou qu'il a n pour cardinal si M contient précisément n éléments. Deux ensembles finis M et N ont donc le même cardinal $|M| = |N|$ s'ils contiennent le même nombre d'éléments.

Pour étendre cette notion d'*égalité* de taille aux ensembles infinis, recourons à l'expérience pratique suivante pour les ensembles finis : supposons qu'un certain nombre de personnes montent dans un bus. Quand peut-on dire que le nombre de personnes est le même que le nombre de sièges libres ? Une façon simple de procéder consiste à laisser tout le monde s'asseoir. Si chacun trouve un siège et si aucun siège ne reste libre, alors le nombre d'éléments de l'ensemble des personnes est le même que le nombre d'éléments de l'ensemble des sièges. En d'autres termes, les deux ensembles ont le même cardinal s'il existe une *bijection* de l'un des ensembles sur l'autre.

Nous prendrons donc cette définition : deux ensembles arbitraires M et N (finis ou infinis) ont même *taille* (ou *cardinal*) si et seulement s'il existe une bijection de M sur N. Il est clair que cette notion d'égalité de taille définit une (sorte de) relation d'équivalence sur les ensembles et l'on peut ainsi associer un nombre, appelé *nombre cardinal*, à chaque classe d'ensembles de même cardinal. Pour les ensembles finis, par exemple, on obtient les nombres cardinaux $0, 1, 2, \ldots, n, \ldots$; l'entier k est le cardinal de la classe des k-ensembles et, en particulier, 0 est celui de l'*ensemble vide* $\varnothing$. En outre, on observe le fait évident qu'un sous-ensemble propre d'un ensemble fini M a toujours un cardinal plus petit que celui de M.

La théorie devient très intéressante et nettement moins intuitive lorsqu'on se tourne vers les ensembles infinis. Considérons à cet effet l'ensemble $\mathbb{N}^* = \{1, 2, 3, \ldots\}$ des nombres entiers non nuls. Un ensemble M est dit *dénombrable* s'il peut être mis en bijection [1] avec $\mathbb{N}^*$. En d'autres termes,

1. N.d.T. : nous conservons les définitions du texte original, d'où la mise en bijection avec $\mathbb{N}^*$ et non $\mathbb{N}$ comme le veut l'usage français. L'usage anglo-saxon veut en effet que $\mathbb{N}$ soit défini comme $\{1, 2, 3, \ldots\}$ et non comme $\{0, 1, 2, 3, \ldots\}$. Nous avons choisi de garder la notation française $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ par respect pour les habitudes du lecteur. Il en résulte quelques occurrences de $\mathbb{N}^*$ qui peuvent sembler superflues au premier abord...

M est dénombrable si l'on peut numéroter la liste des éléments de M de la manière suivante : $m_1, m_2, m_3, \ldots$ Toutefois un étrange phénomène se produit alors. Supposons qu'on ajoute à $\mathbb{N}^*$ un nouvel élément x : l'ensemble $\mathbb{N}^* \cup \{x\}$ est toujours dénombrable et son cardinal est donc encore égal à celui de $\mathbb{N}^*$!

Ce résultat est agréablement illustré par l'« hôtel de Hilbert ». Supposons qu'un hôtel dispose d'un ensemble infini dénombrable de chambres numérotées $1, 2, 3, \ldots$ et que chaque chambre i est occupée par un hôte g_i si bien que l'hôtel est complet. À son arrivée, un nouvel hôte x qui demande une chambre se voit répondre : « désolé, toutes les chambres sont réservées ». « Pas de problème », dit le nouvel arrivant, « déplacez simplement l'hôte g_1 dans la chambre 2, l'hôte g_2 dans la chambre 3 et ainsi de suite, puis je prendrai la chambre 1 ». À la surprise du gérant (il n'est pas mathématicien), ce système fonctionne : il parvient à loger tous ses hôtes ainsi que le nouvel arrivant x !

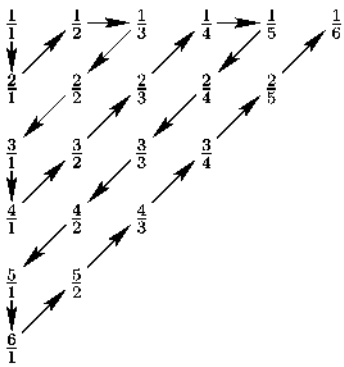
Il est maintenant clair qu'il peut encore loger un nouvel arrivant y, puis encore un autre z, etc. Ainsi, contrairement au cas fini, il peut très bien arriver qu'un sous-ensemble propre d'un ensemble *infini* M ait le même cardinal que M. En fait, comme nous allons le voir, c'est une caractérisation de l'infinité : un ensemble est infini si et seulement s'il a le même cardinal que l'un de ses sous-ensembles propres.

Laissons là l'hôtel de Hilbert et examinons les ensembles de nombres usuels. L'ensemble $\mathbb{Z}$ des entiers est encore dénombrable puisqu'on peut énumérer $\mathbb{Z}$ de la manière suivante $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$. Il est peut-être plus surprenant que l'ensemble $\mathbb{Q}$ des nombres rationnels soit aussi dénombrable.

Théorème 1. *L'ensemble $\mathbb{Q}$ des nombres rationnels est dénombrable.*

■ **Preuve.**

En listant l'ensemble $\mathbb{Q}^+$ des rationnels positifs comme indiqué sur la figure ci-contre, tout en éliminant les nombres déjà rencontrés, on observe que $\mathbb{Q}^+$ est dénombrable ; $\mathbb{Q}$ l'est donc aussi puisqu'il suffit d'en faire la liste en commençant par 0 et en plaçant $-\frac{p}{q}$ juste après $\frac{p}{q}$. Avec ce procédé d'énumération :



$$\mathbb{Q} = \{0, 1, -1, 2, -2, \tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{1}{3}, -\tfrac{1}{3}, 3, -3, 4, -4, \tfrac{3}{2}, -\tfrac{3}{2}, \ldots\}$$

□

On peut aussi interpréter la figure autrement et dire que :

Une réunion dénombrable d'ensembles dénombrables M_n est dénombrable.

En effet, il suffit de poser $M_n = \{a_{n1}, a_{n2}, a_{n3}, \ldots\}$ et de lister :

$$\bigcup_{n=1}^{\infty} M_n = \{a_{11}, a_{21}, a_{12}, a_{13}, a_{22}, a_{31}, a_{41}, a_{32}, a_{23}, a_{14}, \ldots\}$$

exactement comme précédemment.

Observons l'énumération des rationnels positifs selon le schéma de Cantor un peu plus attentivement. En considérant la figure, nous avions obtenu la suite :

$$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{1}{3}, \frac{2}{2}, \frac{3}{1}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{1}{5}, \frac{2}{4}, \frac{3}{3}, \frac{4}{2}, \frac{5}{1}, \ldots$$

de laquelle il convenait de retirer les doublons comme $\frac{2}{2} = \frac{1}{1}$ ou $\frac{2}{4} = \frac{1}{2}$.
En fait il existe une manière encore plus élégante et systématique de lister les éléments en question qui évite les doublons. Elle a été proposée très récemment par Neil Calkin et Herbert Wilf. Leur liste commence par :

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \ldots .$$

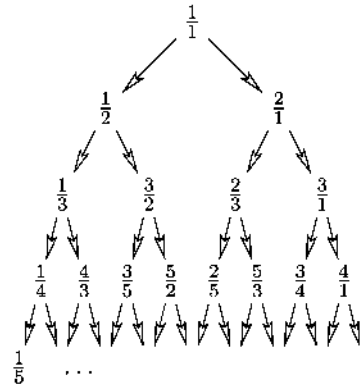
Le dénominateur du n-ième rationnel de la suite est égal au numérateur du $(n+1)$-ième. En d'autres termes, la n-ième fraction est de la forme $b(n)/b(n+1)$ où $\big(b(n)\big)_{n\geqslant 0}$ est une suite qui commence par :

$$(1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, \ldots).$$

Dans un article de 1858, le mathématicien allemand Moritz Abraham Stern est le premier à s'être intéressé à cette suite, désormais connue sous le nom de *suite diatomique de Stern*.

Comment obtenir les éléments de cette suite et ainsi une manière efficace de lister les rationnels positifs ? Considérons l'arbre binaire infini représenté dans la marge. Il est facile de constater la nature récursive de sa construction :

– $\frac{1}{1}$ figure à la racine de l'arbre ;
– chaque nœud $\frac{i}{j}$ a deux fils : le fils gauche est $\frac{i}{i+j}$ et le fils droit est $\frac{i+j}{j}$.



On vérifie facilement les propriétés suivantes :

(1) Toutes les fractions qui apparaissent dans l'arbre sont réduites, c'est-à-dire que lorsqu'une fraction $\frac{r}{s}$ apparaît dans l'arbre, r et s sont premiers entre eux.

La propriété est vraie pour la racine de l'arbre $\frac{1}{1}$ et l'on va procéder par récurrence vers le bas de l'arbre. Si r et s sont premiers entre eux, alors il en va de même pour r et $r+s$, comme pour s et $r+s$.

(2) Toute fraction réduite $\frac{r}{s} > 0$ apparaît dans l'arbre.

On procède par récurrence sur la somme $r+s$. La plus petite valeur possible pour cette somme est $r+s=2$, correspondant à $\frac{r}{s} = \frac{1}{1}$, valeur qui apparaît à la racine de l'arbre. Si $r > s$, alors, d'après l'hypothèse de récurrence, $\frac{r-s}{s}$ apparaît déjà dans l'arbre et l'on obtient $\frac{r}{s}$ comme son fils droit. De manière analogue, si $r < s$, $\frac{r}{s-r}$ apparaît déjà dans l'arbre et $\frac{r}{s}$ apparaît comme son fils gauche.

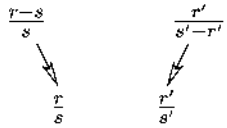
(3) Toute fraction réduite apparaît exactement une fois.

Si $\frac{r}{s}$ apparaissait plus d'une fois dans l'arbre, alors $r \neq s$ puisque tout nœud de l'arbre, à l'exception de la racine, est de la forme $\frac{i}{i+j} < 1$ ou $\frac{i+j}{j} > 1$. Comme $r > s$ ou $s > r$, on procède par récurrence, comme on l'a fait dans le point précédent.

Tout rationnel positif apparaît donc exactement une fois dans l'arbre et on peut écrire la suite de ces nombres de gauche à droite, niveau par niveau, en descendant dans l'arbre[2]. On obtient ainsi les premiers termes listés précédemment.

(4) Le dénominateur de la n-ième fraction de la suite est égal au numérateur de la $(n+1)$-ième.

Le résultat est évident pour $n = 0$ ou lorsque la n-ième fraction est un fils gauche. On raisonne par récurrence. Supposons, que la n-ième fraction $\frac{r}{s}$ est un fils droit. Si $\frac{r}{s}$ est l'élément le plus à droite d'un niveau, alors $s = 1$ si bien que la fraction qui lui succède se trouve la plus à gauche dans le niveau suivant et présente un numérateur qui est 1. Si, en revanche, $\frac{r}{s}$ n'est pas au bord de son niveau et, si $\frac{r'}{s'}$ désigne la fraction qui la suit immédiatement, alors $\frac{r}{s}$ est le fils droit de $\frac{r-s}{s}$ et $\frac{r'}{s'}$ est le fils gauche de $\frac{r'}{s'-r'}$ et alors, d'après l'hypothèse de récurrence, le dénominateur de $\frac{r-s}{s}$ est le numérateur de $\frac{r'}{s'-r'}$ si bien que $s = r'$.



Tout cela est très bien mais il y a encore mieux. Deux questions se présentent de manière naturelle :

- Est-ce que la suite $\big(b(n)\big)_{n\geqslant 0}$ a une « signification » ? En d'autres termes, est-ce que $b(n)$ dénombre quelque chose de simple ?
- Étant donné $\frac{r}{s}$, dispose-t-on d'un moyen simple pour calculer son successeur dans la suite ?

Pour répondre à la première question, nous allons montrer que le nœud $b(n)/b(n+1)$ admet les fils $b(2n+1)/b(2n+2)$ et $b(2n+2)/b(2n+3)$. La procédé de construction de l'arbre conduit à la récurrence :

$$b(2n+1) = b(n) \quad \text{et} \quad b(2n+2) = b(n) + b(n+1). \tag{1}$$

Posant $b(0) = 1$, la suite $(b(n))_{n\geqslant 0}$ est parfaitement définie par les relations (1).

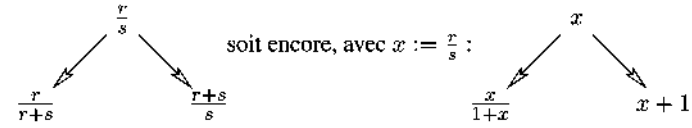
Ainsi la question devient : y a-t-il une « jolie » suite « connue » satisfaisant à ces relations de récurrence ? La réponse est affirmative. Nous savons que tout nombre n peut être écrit de manière unique comme la somme de puissances de 2 distinctes : c'est l'habituelle représentation binaire de n. Une représentation *hyperbinaire* de n est une décomposition de n en somme de puissances de 2 dans laquelle chaque puissance peut apparaître au plus *deux fois*. Soit $h(n)$ le nombre de représentations hyperbinaires possibles pour n. Le lecteur est invité à constater que la suite de terme général $h(n)$ satisfait aux relations de récurrence (1), ce qui suffit à prouver que $b(n) = h(n)$ pour tout n.

Par exemple, $h(6) = 3$, avec les représentations hyperbinaires possibles suivantes :
$6 = 4 + 2$
$6 = 4 + 1 + 1$
$6 = 2 + 2 + 1 + 1$.

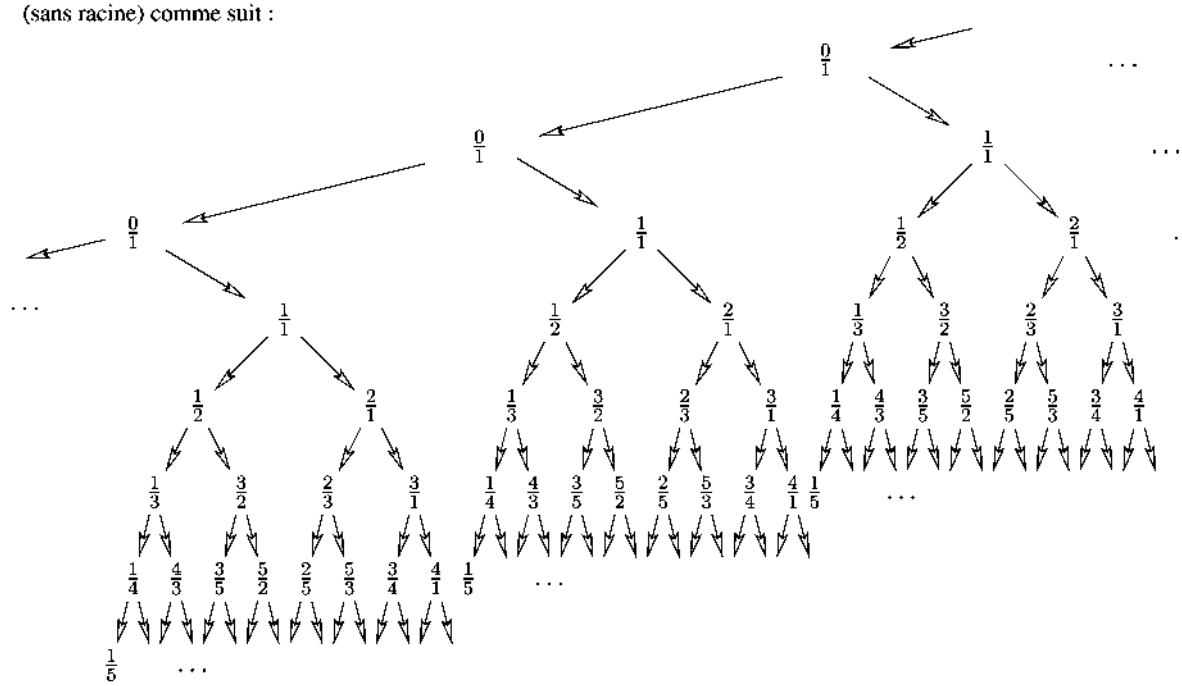
Incidemment nous avons prouvé un résultat surprenant : soit $\frac{r}{s}$ une fraction réduite, il existe un unique entier n tel que $r = h(n)$ et $s = h(n+1)$.

2. N.d.T. : l'informaticien dirait : « en effectuant un parcours en largeur » de l'arbre.

Tournons nous à présent vers la deuxième question. Dans l'arbre figure :



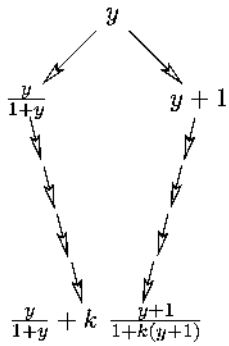
Nous utilisons ce schéma pour générer un arbre infini encore plus grand (sans racine) comme suit :



Dans cet arbre, toutes les lignes sont identiques et elles fournissent toutes le procédé de dénombrement des rationnels positifs de Calkin-Wilf (en partant de $\frac{0}{1}$).

Comment fait-on alors pour passer d'un rationnel à son successeur ? Pour répondre à cette question, remarquons d'abord que pour tout rationnel x, son fils droit est $x+1$, son petit-fils droit est $x+2$ et son descendant droit d'ordre k est $x+k$. De manière analogue, le fils gauche de x est $\frac{x}{1+x}$ dont le propre fils gauche est $\frac{x}{1+2x}$ et ainsi de suite. Le descendant gauche d'ordre k de x est $\frac{x}{1+kx}$.

À présent, pour trouver comment on passe de $\frac{r}{s} = x$ à son successeur $f(x)$ dans la liste, il nous faut analyser la situation représentée dans la marge. En fait, si l'on considère un rationnel x strictement positif quelconque dans l'arbre binaire infini, alors on voit que c'est le descendant droit d'ordre k du fils gauche d'un certain rationnel $y \geqslant 0$ (pour un certain $k \geqslant 0$) tandis que $f(x)$ s'obtient comme le descendant gauche d'ordre k du fils droit de



ce même y. Ainsi, à partir de la formule donnant la valeur des descendants d'ordre k on trouve :

$$x \;=\; \frac{y}{1+y} + k,$$

comme indiqué sur la figure ci-contre. Ici, $k = \lfloor x \rfloor$ est la partie entière de x tandis que $\frac{y}{1+y} = \{x\}$ est sa partie fractionnaire. On en déduit :

$$f(x) = \frac{y+1}{1+k(y+1)} = \frac{1}{\frac{1}{y+1}+k} = \frac{1}{k+1-\frac{y}{y+1}} = \frac{1}{\lfloor x \rfloor + 1 - \{x\}}.$$

Nous avons donc obtenu une magnifique formule pour le successeur $f(x)$ de x, récemment établie par Moshe Newman :

La fonction :

$$x \;\longmapsto\; f(x) \;=\; \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

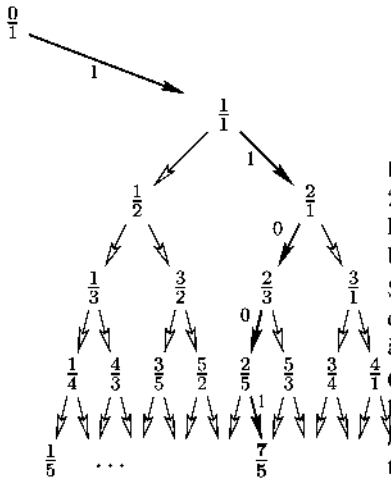
engendre la suite de Calkin-Wilf.

$$\tfrac{1}{1} \mapsto \tfrac{1}{2} \mapsto \tfrac{2}{1} \mapsto \tfrac{1}{3} \mapsto \tfrac{3}{2} \mapsto \tfrac{2}{3} \mapsto \tfrac{3}{1} \mapsto \tfrac{1}{4} \mapsto \tfrac{4}{3} \mapsto \ldots$$

dans laquelle figure exactement une fois tout rationnel positif.

Le procédé d'énumération de Calkin-Wilf-Newman présente d'autres propriétés remarquables. Par exemple, on peut se demander si l'on dispose d'un moyen rapide de calculer la n-ième fraction de la suite, disons, par exemple, pour $n = 10^6$. Le voici :

Pour trouver la n-ième fraction de la suite de Calkin-Wilf, il faut exprimer n sous sa forme binaire $n = (b_k b_{k-1} \ldots b_1 b_0)_2$ et suivre dans l'arbre de Calkin-Wilf le chemin défini par les chiffres b_i, en partant de $\frac{s}{t} = \frac{0}{1}$. L'égalité $b_i = 1$ signifie « choisir le fils droit », c'est-à-dire « ajouter le dénominateur au numérateur », tandis que $b_i = 0$ signifie « choisir le fils gauche », c'est-à-dire « ajouter le numérateur au dénominateur ».



La figure représentée ci-contre dans la marge montre le chemin pour $n = 25 = (11001)_2$. Ainsi le 25-ième terme de la suite de Calkin-Wilf est $\frac{7}{5}$. Le lecteur pourra aisément établir un procédé qui calcule la (représentation binaire de la) position n d'une fraction donnée $\frac{s}{t}$ dans la suite.

Signalons, pour en finir avec $\mathbb{Q}$, une autre façon, très élégante, de montrer que $\mathbb{Q}^+$ est dénombrable : elle consiste à observer que l'application de $\mathbb{Q}^+$ à valeurs dans $\mathbb{N}$ qui à p/q irréductible associe $2^p 3^q$ est injective.

Qu'en est-il de l'ensemble des nombres réels $\mathbb{R}$? Est-il lui-aussi dénombrable ? Il n'en est rien. La méthode employée pour le démontrer — la *méthode diagonale* de Cantor — n'a pas seulement une importance capitale pour la théorie des ensembles toute entière, elle appartient aussi à coup sûr au Grand Livre pour le trait de génie qu'elle constitue.

Théorème 2. *L'ensemble* $\mathbb{R}$ *des nombres réels n'est pas dénombrable.*

■ **Preuve.** Tout sous-ensemble N d'un ensemble dénombrable $M = \{m_1, m_2, m_3, \ldots\}$ est *au plus dénombrable* (c'est-à-dire fini ou dénombrable). En effet, il suffit de lister simplement les éléments de N tels qu'ils apparaissent dans M. Si donc on peut trouver un sous-ensemble de $\mathbb{R}$ qui n'est pas dénombrable, alors *a fortiori* $\mathbb{R}$ ne peut pas être dénombrable. Le sous-ensemble M de $\mathbb{R}$ que nous allons examiner est l'intervalle $]0, 1]$ de tous les nombres réels r tels que $0 < r \leqslant 1$. Supposons, au contraire, que M soit dénombrable et soit $M = \{r_1, r_2, r_3, \ldots\}$ une énumération des éléments de M. On écrit r_n sous la forme de son unique développement décimal *infini* (sans suite infinie de zéros à la fin [3]) :

$$r_n = 0.a_{n1}a_{n2}a_{n3}\ldots$$

où $a_{ni} \in \{0, 1, \ldots, 9\}$ pour tout n et pour tout i. Par exemple, $0.7 = 0.6999\ldots$ Considérons maintenant le tableau doublement infini :

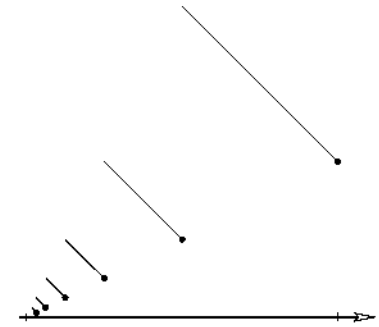
$$\begin{aligned} r_1 &= 0.a_{11}a_{12}a_{13}\ldots \\ r_2 &= 0.a_{21}a_{22}a_{23}\ldots \\ &\vdots \\ r_n &= 0.a_{n1}a_{n2}a_{n3}\ldots \\ &\vdots \end{aligned}$$

Pour tout n, soit b_n le plus petit élément de $\{1, 2\}$ différent de a_{nn}. Alors $b = 0.b_1b_2b_3\ldots b_n\ldots$ est un nombre réel appartenant à l'ensemble M qui doit donc être indexé sous la forme $b = r_k$. Cela est impossible puisque b_k est différent de a_{kk}. □

Attardons-nous un moment sur les nombres réels et remarquons que les quatre types d'intervalles $]0, 1[,]0, 1], [0, 1[$ et $[0, 1]$ ont le même cardinal. Nous pouvons notamment vérifier que $]0, 1]$ et $]0, 1[$ ont même cardinal. L'application f définie par $f :]0, 1] \longrightarrow]0, 1[, x \longmapsto y$ par :

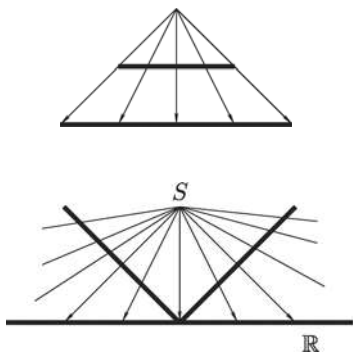
$$y := \begin{cases} \frac{3}{2} - x & \text{si} \quad \frac{1}{2} < x \leqslant 1, \\ \frac{3}{4} - x & \text{si} \quad \frac{1}{4} < x \leqslant \frac{1}{2}, \\ \frac{3}{8} - x & \text{si} \quad \frac{1}{8} < x \leqslant \frac{1}{4}, \\ \quad \vdots \end{cases}$$

convient. En effet, cette application est bijective, puisque y décrit l'intervalle $\frac{1}{2} \leqslant y < 1$ à la première ligne, $\frac{1}{4} \leqslant y < \frac{1}{2}$ à la deuxième ligne, $\frac{1}{8} \leqslant y < \frac{1}{4}$ à la troisième ligne et ainsi de suite.



$f :]0, 1] \longrightarrow]0, 1[$

3. N.d.T. : c'est-à-dire en faisant le choix (justifié par le raisonnement qui suit) de représenter, par exemple, $3/10$ par le développement $0,29999\ldots$ plutôt que par le développement $0,30000\ldots$



Nous constatons ensuite que *tous* les intervalles (de longueur finie strictement positive) ont même cardinal en considérant la projection centrale représentée sur la figure. Il y a même mieux : chaque intervalle (de longueur strictement positive) a le même cardinal que la droite réelle $\mathbb{R}$ entière. Pour s'en convaincre, il suffit de regarder l'intervalle ouvert plié $]0,1[$ et de le projeter sur $\mathbb{R}$ à partir du centre S.

En conclusion, tous les intervalles ouverts, semi-ouverts, fermés (finis ou infinis) de longueur strictement positive ont le même cardinal. On note c ce cardinal, c pour *continu*. On dit que ces ensembles de nombres ont la puissance du continu.

Le fait que des intervalles finis ou infinis aient le même cardinal peut apparaître comme intuitif après réflexion ; voici néanmoins un résultat qui va complètement à l'encontre de l'intuition.

Théorème 3. *L'ensemble $\mathbb{R}^2$ de tous les couples de nombres réels, (c'est-à-dire le plan réel) a le même cardinal que $\mathbb{R}$.*

Cantor proposa cet énoncé en 1878 avec l'idée de fusionner le développement décimal de deux réels pour en faire un seul. La variante de la méthode de Cantor présentée ici relève du Grand Livre. Abraham Fraenkel attribue à Julius König l'astuce qui fournit directement la bijection adéquate.

■ **Preuve.** Il suffit de montrer que l'ensemble de tous les couples (x, y), $0 < x, y \leqslant 1$, peut être envoyé de façon bijective sur $]0,1]$. Ici encore, la démonstration mérite de figurer dans le Grand Livre. Considérons le couple (x, y) et écrivons l'unique développement décimal infini de x et y comme dans l'exemple suivant :

$$\begin{array}{rcccccccc} x & = & 0.3 & & 01 & 2 & 007 & 08 & \ldots \\ y & = & 0.009 & 2 & 05 & 1 & 0008 & & \ldots \end{array}$$

Nous avons séparé les chiffres de x et y en groupes qui s'arrêtent dès qu'un chiffre non nul apparaît dans le développement. Nous associons ensuite à (x, y) le nombre $z \in]0,1]$ en écrivant le premier groupe de chiffres apparaissant dans l'écriture de x, puis le premier groupe issu de y, ensuite le deuxième groupe issu de x et ainsi de suite. Ainsi, avec l'exemple précédent, on obtient :

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0008\ \ldots$$

Comme ni x ni y ne sont composés que de zéros à partir d'un certain rang, l'expression de z est un développement décimal infini. Réciproquement, à partir du développement de z, nous pouvons immédiatement reconstituer son image réciproque (x, y), l'application est donc bijective. □

Comme $(x, y) \longmapsto x + iy$ est une bijection de $\mathbb{R}^2$ sur l'ensemble des nombres complexes $\mathbb{C}$, on obtient : $|\mathbb{C}| = |\mathbb{R}| = c$. Pourquoi le résultat $|\mathbb{R}^2| = |\mathbb{R}|$ est-il aussi inattendu ? Parce qu'il va à l'encontre de l'intuition qu'on peut avoir de la notion de *dimension*. Le résultat précédent dit que le plan $\mathbb{R}^2$ de dimension 2 (et plus généralement, par récurrence, l'espace

$\mathbb{R}^n$ de dimension n) peut être envoyé bijectivement sur la droite $\mathbb{R}$ qui est de dimension 1. Ainsi, la dimension n'est pas conservée en général par les applications bijectives. Cependant, si nous demandons à l'application et à son inverse d'être continues, alors la dimension est conservée, propriété que Luitzen Brouwer fut le premier à montrer.

Allons un peu plus loin. Jusqu'à présent, nous avons la notion d'égalité de cardinal. Quand pourra-t-on dire que M est au plus aussi grand que N ? Ce sont encore les applications qui apportent la clé. Nous dirons que le nombre cardinal $\mathfrak{m}$ est *inférieur ou égal à* $\mathfrak{n}$ si, étant donnés des ensembles M et N tels que $|M| = \mathfrak{m}$ et $|N| = \mathfrak{n}$, il existe une *injection* de M dans N. Il est clair que la relation $\mathfrak{m} \leqslant \mathfrak{n}$ est indépendante des représentants M et N choisis. Si les ensembles sont finis, cela correspond encore à l'intuition. Un m-ensemble est au plus aussi grand qu'un n-ensemble si et seulement si $m \leqslant n$.

On est maintenant confronté à un problème fondamental. Il serait évidemment souhaitable que les lois usuelles concernant les inégalités soient également vérifiées pour les nombres cardinaux (notamment infinis). En particulier, est-il vrai que $\mathfrak{m} \leqslant \mathfrak{n}$ et $\mathfrak{n} \leqslant \mathfrak{m}$ implique : $\mathfrak{m} = \mathfrak{n}$?

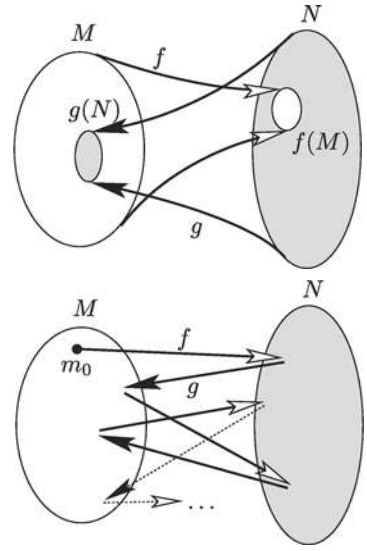
La réponse affirmative est fournie par le célèbrethéorème de Cantor-Bernstein que Cantor énonça en 1883. La première démonstration complète de ce résultat fut établie par Felix Bernstein bien des années plus tard dans le séminaire de Cantor. De nouvelles preuves ont été établies par Richard Dedekind, Ernst Zermelo et bien d'autres. La démonstration que nous en donnons ici est due à Julius König (1906).

Théorème 4. *Si chacun des deux ensembles M et N s'injecte dans l'autre, alors il existe une bijection de M sur N, c'est-à-dire $|M| = |N|$.*

■ **Preuve.** Nous pouvons supposer que M et N sont disjoints — si tel n'est pas le cas, on remplace N par une copie de N.

Soit f et g les applications qui transportent respectivement les éléments de M vers N et ceux de N vers M. Une manière d'éclaircir la situation consiste à aligner les éléments de $M \cup N$ en une chaîne. On va prendre un élément arbitraire m_0 de M ; on forme une chaîne à partir de cet élément en lui appliquant f, puis en appliquant g à son image, puis à nouveau f et ainsi de suite. La chaîne peut se refermer (cas 1) si l'on retombe sur m_0 au cours de l'itération de ce procédé ou, au contraire, être constituée d'une suite infinie d'éléments distincts (le premier élément qui se répéterait dans la chaîne ne pourrait être que m_0 par injectivité des applications considérées).

Si la chaîne est infinie, alors on va essayer de la parcourir en marche arrière, en passant de m_0 à $g^{-1}(m_0)$ si m_0 appartient à l'image de g, puis à $f^{-1}(g^{-1}(m_0))$ si $g^{-1}(m_0)$ appartient à l'image de f et ainsi de suite. Trois nouveaux cas peuvent alors se présenter. Soit le parcours rétrograde de la chaîne est infini (cas 2), soit le parcours s'interrompt en un élément de M ne figurant pas dans l'image de g (cas 3), soit le parcours s'interrompt en un élément de N ne figurant pas dans l'image de f (cas 4).



Ainsi, quatre cas peuvent se présenter pour les chaînes de $M \cup N$ et nous allons voir que dans chaque cas il est possible d'indexer les éléments de la chaîne de telle sorte que $F : m_i \longmapsto n_i$ soit une bijection.

Cas 1 : cycle fini constitué de $2k + 2$ éléments distincts ($k \geqslant 0$).

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} \cdots \xrightarrow{f} m_k \xrightarrow{f} n_k \xrightarrow{g} m_0$$

Cas 2 : chaîne infinie des deux côtés constituée d'éléments distincts.

$$\cdots \longrightarrow m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

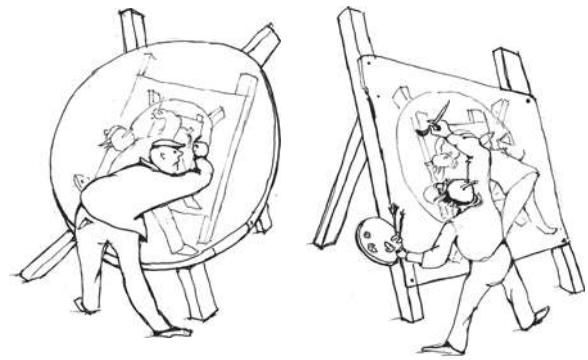
Cas 3 : chaîne infinie constituée d'éléments distincts commençant en $m_0 \in M \backslash g(N)$.

$$m_0 \xrightarrow{f} n_0 \xrightarrow{g} m_1 \xrightarrow{f} n_1 \xrightarrow{g} m_2 \xrightarrow{f} \cdots$$

Cas 4 : chaîne infinie constituée d'éléments distincts commençant en $n_0 \in N \backslash f(M)$.

$$n_0 \xrightarrow{g} m_0 \xrightarrow{f} n_1 \xrightarrow{g} m_1 \xrightarrow{f} \cdots$$

□



« Cantor et Bernstein en train de peindre ».

Qu'en est-il des autres relations gouvernant les inégalités ? Comme d'habitude, nous posons $\mathfrak{m} < \mathfrak{n}$ si $\mathfrak{m} \leqslant \mathfrak{n}$ et $\mathfrak{m} \neq \mathfrak{n}$. Nous venons de voir qu'étant donnés deux cardinaux $\mathfrak{m}$ et $\mathfrak{n}$ l'une au plus des trois possibilités :

$$\mathfrak{m} < \mathfrak{n},\ \mathfrak{m} = \mathfrak{n},\ \mathfrak{m} > \mathfrak{n}$$

peut se produire. Il découle de la théorie des cardinaux qu'en fait, une relation exactement est vraie (se reporter à l'appendice de ce chapitre, proposition 2).

En outre, le théorème de Schroeder-Bernstein nous dit que la relation $<$ est transitive, c'est-à-dire que $\mathfrak{m} < \mathfrak{n}$ et $\mathfrak{n} < \mathfrak{p}$ impliquent $\mathfrak{m} < \mathfrak{p}$. Ainsi,

les cardinaux sont placés dans un ordre linéaire qui commence avec les cardinaux finis $0, 1, 2, 3, \ldots$ En faisant appel au système axiomatique de Zermelo-Fraenkel (notamment à l'axiome du choix), on établit facilement qu'un ensemble infini M contient un sous-ensemble dénombrable. En effet, M contient un élément, soit m_1. L'ensemble $M \setminus \{m_1\}$ n'est pas vide (puisque M est infini) et il contient donc un élément m_2. De la même façon, $M \setminus \{m_1, m_2\}$ contient un élément m_3 et ainsi de suite. Ainsi, le cardinal d'un ensemble infini dénombrable est *le plus petit cardinal infini* habituellement noté $\aleph_0$ (prononcer « aleph zéro »).

Comme $\aleph_0 \leqslant \mathfrak{m}$ pour tout cardinal infini $\mathfrak{m}$, on obtient immédiatement le résultat de l'« hôtel de Hilbert » pour tout nombre cardinal infini $\mathfrak{m}$, c'est-à-dire qu'on a $|M \cup \{x\}| = |M|$ pour tout ensemble infini M. En effet, M contient un sous-ensemble $N = \{m_1, m_2, m_3, \ldots\}$. Maintenant, envoyons x sur m_1, m_1 sur m_2 et ainsi de suite, en laissant fixes les éléments de $M \setminus N$. Ce procédé fournit la bijection souhaitée.

On a montré par la même occasion un résultat annoncé un peu plus tôt : *Tout ensemble infini a le même cardinal que l'un de ses sous-ensembles propres.*

Une autre application du théorème de Cantor-Bernstein consiste à prouver que l'ensemble $\mathcal{P}(\mathbb{N})$ de tous les sous-ensembles de $\mathbb{N}$ est de cardinal c. Comme on l'a dit précédemment, il suffit de montrer que $|\mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}| = |]0, 1]|$. L'application f et g suivantes sont injectives et suffisent à prouver cette égalité :

$$\begin{aligned} f : \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\} &\longrightarrow]0, 1], \\ A &\longmapsto \sum_{i \in A} 10^{-i}, \end{aligned}$$

$$\begin{aligned} g :]0, 1] &\longrightarrow \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}, \\ 0.b_1 b_2 b_3 \ldots &\longmapsto \{b_i 10^i : i \in \mathbb{N}\} \end{aligned}$$

Jusqu'à présent, nous avons rencontré les cardinaux $0, 1, 2, \ldots, \aleph_0$; nous savons aussi que le cardinal c de $\mathbb{R}$ est plus grand que $\aleph_0$. Le passage de $\mathbb{Q}$ de cardinal $\aleph_0$ à $\mathbb{R}$ de cardinal c suggère immédiatement la question suivante :

Le cardinal infini $c = |\mathbb{R}|$ est-il celui qui suit immédiatement $\aleph_0$?

À présent nous sommes confrontés à la question de savoir s'il *existe* un nombre cardinal plus grand suivant $\aleph_0$ ou, en d'autres termes, s'il est pertinent d'introduire un nouveau cardinal $\aleph_1$. On peut répondre par l'affirmative et la preuve est esquissée dans l'appendice de ce chapitre.

L'énoncé $c = \aleph_1$ est connu sous le nom d'*hypothèse du continu*. La question de savoir si l'hypothèse du continu est vraie a constitué pendant plusieurs décennies l'un des plus grands défis de toutes les mathématiques. La réponse, finalement donnée par Kurt Gödel et Paul Cohen, nous mène aux

« Le plus petit cardinal infini ».

limites de la pensée logique. Ils ont montré que l'énoncé $c = \aleph_1$ est *indépendant* du système d'axiomes de Zermelo-Fraenkel, tout comme l'axiome de l'unique parallèle est indépendant des autres axiomes de la géométrie euclidienne. Il y a des modèles pour lesquels $c = \aleph_1$ et d'autres modèles de la théorie des ensembles pour lesquels $c \neq \aleph_1$.

À la lumière de ces remarques, il est intéressant de se demander s'il existe d'autres conditions (provenant par exemple de l'analyse) qui sont équivalentes à l'hypothèse du continu. Dans ce qui suit, nous voulons présenter un exemple de ce type ainsi que sa solution, très élégante et très simple, due à Paul Erdős. En 1962, Wetzel a posé la question suivante :

> *Soit $\{f_\alpha\}$ une famille de fonctions analytiques sur $\mathbb{C}$, deux à deux distinctes, telles que pour tout $z \in \mathbb{C}$ l'ensemble des valeurs $\{f_\alpha(z)\}$ soit dénombrable ; appelons (P_0) cette propriété.*
> *Peut-on en déduire que cette famille est elle-même dénombrable ?*

Très peu de temps après, Erdős a montré de façon surprenante que la réponse dépend de l'hypothèse du continu.

Théorème 5. *Si $c > \aleph_1$, alors toute famille $\{f_\alpha\}$ vérifiant (P_0) est dénombrable. Si, en revanche, $c = \aleph_1$, alors il existe une famille $\{f_\alpha\}$ de cardinal c vérifiant la propriété (P_0).*

La démonstration de ce théorème fait appel à certains résultats élémentaires sur les nombres cardinaux et ordinaux. Le lecteur qui ne serait pas familier avec ces notions est invité à se reporter à l'appendice où se trouvent réunis les résultats requis.

■ **Preuve du théorème 5.** Supposons d'abord $c > \aleph_1$. Nous allons montrer que pour toute famille $\{f_\alpha\}$ de fonctions analytiques de cardinal $\aleph_1$, il existe un nombre complexe z_0 tel que *toutes les* $\aleph_1$ valeurs $f_\alpha(z_0)$ soient distinctes. Par conséquent, si une famille de fonctions satisfait (P_0), alors elle doit être au plus dénombrable.

Pour s'en convaincre, il faut faire appel aux nombres ordinaux. On commence par bien ordonner la famille $\{f_\alpha\}$ relativement au nombre ordinal initial ω_1 de $\aleph_1$. Cela signifie, d'après la proposition 1 de l'appendice, que l'ensemble des indices parcourt tous les nombres ordinaux α qui sont plus petits que ω_1. Ensuite, on montre que l'ensemble des paires (α, β), $\alpha < \beta < \omega_1$, a $\aleph_1$ pour cardinal. Puisque tout $\beta < \omega_1$ est un ordinal dénombrable, l'ensemble des paires (α, β), $\alpha < \beta$, est au plus dénombrable pour tout β fixé. En prenant la réunion sur tous les β (au nombre de $\aleph_1$), on déduit de la proposition 6 de l'appendice que l'ensemble de toutes les paires (α, β), $\alpha < \beta$, a pour cardinal $\aleph_1$.

À présent, pour toute paire $\alpha < \beta$, considérons l'ensemble :

$$S(\alpha, \beta) = \{z \in \mathbb{C} : f_\alpha(z) = f_\beta(z)\}$$

Nous affirmons que chaque ensemble $S(\alpha, \beta)$ est au plus dénombrable. Pour le vérifier, considérons les disques C_k de rayon $k = 1, 2, 3, \ldots$ autour de l'origine du plan complexe. Si f_α et f_β coïncident en une infinité de points sur un certain C_k, alors f_α et f_β sont identiques selon un résultat bien connu sur les fonctions analytiques. Ainsi, f_α et f_β coïncident seulement sur un nombre fini de points sur chaque C_k, donc au plus sur un nombre dénombrable de points. Maintenant on pose $S = \bigcup_{\alpha<\beta} S(\alpha, \beta)$. Encore une fois, grâce à la proposition 6, on établit que S a pour cardinal $\aleph_1$ puisque chaque ensemble $S(\alpha, \beta)$ est au plus dénombrable. Le point clé apparaît ici : comme nous le savons, le cardinal de $\mathbb{C}$ est c et c est plus grand que $\aleph_1$ par hypothèse. Il existe donc un nombre complexe z_0 qui n'appartient pas à S ; pour un tel z_0 toutes les $\aleph_1$ valeurs $f_\alpha(z_0)$ sont distinctes.

Supposons maintenant que $c = \aleph_1$ et considérons l'ensemble $D \subseteq \mathbb{C}$ des nombres complexes $p + iq$ de parties réelle et imaginaire rationnelles. Puisque pour tout p l'ensemble $\{p + iq : q \in \mathbb{Q}\}$ est dénombrable, D est dénombrable. En outre, D est un ensemble *dense* dans $\mathbb{C}$ donc tout disque ouvert du plan complexe contient un point de D. Soit $\{z_\alpha : 0 \leqslant \alpha < \omega_1\}$ un bon ordre sur $\mathbb{C}$. Nous allons construire une famille $\{f_\beta : 0 \leqslant \beta < \omega_1\}$ de $\aleph_1$ fonctions analytiques telles que :

$$f_\beta(z_\alpha) \in D \text{ quand } \alpha < \beta \tag{1}$$

Une telle famille vérifie la condition (P_0). En effet, chaque point $z \in \mathbb{C}$ a un indice, disons $z = z_\alpha$. Pour tout $\beta > \alpha$, les valeurs $\{f_\beta(z_\alpha)\}$ appartiennent à l'ensemble *dénombrable* D. Puisque α est un nombre ordinal dénombrable, les fonctions f_β telles que $\beta \leqslant \alpha$ vont ajouter une quantité au plus dénombrable de valeurs supplémentaires $f_\beta(z_\alpha)$. Ainsi, l'ensemble de toutes les valeurs $\{f_\beta(z)\}$ est encore au plus dénombrable. Donc, si nous pouvons construire une famille $\{f_\beta\}$ satisfaisant (1), alors la seconde partie du théorème est démontrée.

La construction de $\{f_\beta\}$ utilise une récurrence transfinie. Pour f_0, nous pouvons prendre n'importe quelle fonction analytique, par exemple une fonction constante. Supposons que f_β ait déjà été construite pour tout $\beta < \gamma$. Puisque γ est un ordinal dénombrable, nous pouvons réordonner $\{f_\beta : 0 \leqslant \beta < \gamma\}$ en une suite $g_1, g_2, g_3, \ldots$ Le même ordonnancement de $\{z_\alpha : 0 \leqslant \alpha < \gamma\}$ donne une suite $w_1, w_2, w_3, \ldots$ Nous allons maintenant construire une fonction f_γ satisfaisant pour tout n les conditions :

$$f_\gamma(w_n) \in D \qquad \text{et} \qquad f_\gamma(w_n) \neq g_n(w_n) \tag{2}$$

La deuxième condition va permettre de s'assurer que toutes les fonctions f_γ $(0 \leqslant \gamma < \omega_1)$ sont distinctes ; la première condition est simplement la condition (1), ce qui implique (P_0) grâce à notre argument précédent. Notons que la condition $f_\gamma(w_n) \neq g_n(w_n)$ est une fois de plus un argument diagonal.

Pour construire f_γ, on écrit :

$$\begin{aligned} f_\gamma(z) \;:=\; & \varepsilon_0 + \varepsilon_1(z - w_1) + \varepsilon_2(z - w_1)(z - w_2) \\ & + \varepsilon_3(z - w_1)(z - w_2)(z - w_3) + \ldots . \end{aligned}$$

Si γ est un ordinal fini, alors f_γ est un polynôme ; elle est donc analytique et nous pouvons certainement choisir des nombres ε_i tels que (2) soit satisfaite. Supposons maintenant que γ soit un ordinal dénombrable ; alors :

$$f_\gamma(z) \;=\; \varepsilon_0 + \sum_{k=1}^{\infty} \varepsilon_k (z - w_1) \cdots (z - w_k) \tag{3}$$

Remarquons que les valeurs de ε_m $(m \geqslant n)$ n'ont pas d'influence sur la valeur $f_\gamma(w_n)$. Nous pouvons donc choisir les ε_n pas à pas. Si la suite (ε_n) converge vers 0 suffisamment rapidement, alors (3) définit une fonction analytique. En définitive, puisque D est un ensemble dense, nous pouvons choisir cette suite (ε_n) de sorte que f_γ satisfasse (2), ce qui termine la démonstration. □

Appendice - À propos des nombres cardinaux et ordinaux

Interrogeons-nous, tout d'abord, sur la question de l'existence d'un nombre cardinal supérieur à un nombre cardinal donné. Pour commencer, nous montrons que pour tout nombre cardinal $\mathfrak{m}$, il existe toujours un nombre cardinal $\mathfrak{n}$ plus grand que $\mathfrak{m}$. Pour ce faire, nous utilisons encore une fois une version de la méthode diagonale de Cantor.

Soit M un ensemble. Nous affirmons que l'ensemble $\mathcal{P}(M)$ *de tous les sous-ensembles* de M a un cardinal plus grand que M. En associant à $m \in M$ le sous-ensemble $\{m\} \in \mathcal{P}(M)$, on voit que M peut être envoyé bijectivement sur un sous-ensemble de $\mathcal{P}(M)$, ce qui implique $|M| \leqslant |\mathcal{P}(M)|$ par définition. Il reste à montrer que $\mathcal{P}(M)$ *ne peut pas* être envoyé bijectivement sur un sous-ensemble de M. Supposons qu'au contraire

$$\varphi : N \longrightarrow \mathcal{P}(M)$$

soit une bijection de $N \subseteq M$ sur $\mathcal{P}(M)$. Considérons le sous-ensemble $U \subseteq N$ constitué des éléments de N qui *ne sont pas* contenus dans leur image par φ, c'est-à-dire que $U = \{m \in N : m \notin \varphi(m)\}$. Puisque φ est une bijection, il existe $u \in N$ tel que $\varphi(u) = U$. On a donc soit $u \in U$, soit $u \notin U$, mais les deux sont impossibles ! En effet, si $u \in U$, alors $u \notin \varphi(u) = U$ par définition de U, et si $u \notin U = \varphi(u)$, alors $u \in U$, ce qui est contradictoire.

« Une légende raconte que saint Augustin, marchant le long de la plage et contemplant l'infini, vit un enfant qui essayait de vider l'océan avec un petit coquillage... »

Le lecteur connaît probablement déjà cet argument. C'est le vieux paradoxe du barbier : « un barbier est un homme qui rase les personnes qui ne se rasent pas elles-mêmes. Est-ce que le barbier se rase lui-même ? »

Pour poursuivre cette théorie, nous introduisons un autre concept important dû à Cantor : les *ensembles ordonnés* et les *nombres ordinaux*. Un ensemble M est *ordonné* par $<$ si la relation $<$ est transitive et si, pour tout couple d'éléments distincts a et b de M, on a soit $a < b$ soit $b < a$. On peut, par exemple, ordonner $\mathbb{N}^*$ de manière naturelle $\mathbb{N}^* = \{1, 2, 3, 4, \ldots\}$. On peut

aussi évidemment l'ordonner à l'envers $\mathbb{N} = \{\ldots, 4, 3, 2, 1\}$, ou encore en énumérant d'abord les nombres impairs, ensuite les nombres pairs $\mathbb{N}^* = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$.

Voici maintenant le concept fondamental. Un ensemble ordonné M est dit *bien ordonné* si chaque sous-ensemble non vide de M a un premier élément (ou plus petit élément). Ainsi, le premier et le troisième ordres associés à $\mathbb{N}^*$ ci-dessus sont de bons ordres mais ce n'est pas le cas du deuxième. Le *théorème fondamental du bon ordre*, déduit des axiomes, (incluant l'axiome du choix), affirme que *tout* ensemble M admet un bon ordre. À partir de maintenant, nous ne considérerons que des ensembles munis d'un bon ordre.

Les ensembles bien ordonnés :

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

et :

$$\mathbb{N}^* = \{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$$

ne sont pas similaires : le premier ordre n'a qu'un élément sans prédécesseur immédiat, tandis que le second en a deux.

On dit que deux ensembles bien ordonnés M et N sont *similaires* (ou *isomorphes*, ou encore de *même type d'ordre*) s'il existe une bijection φ de M sur N qui respecte l'ordre, c'est-à-dire telle que $m <_M n$ implique $\varphi(m) <_N \varphi(n)$. Remarquons que tout ensemble ordonné similaire à un ensemble bien ordonné est lui-même bien ordonné.

Il est clair que la similarité est une relation d'équivalence. Nous pouvons donc parler d'un *nombre ordinal* α appartenant à une classe d'ensembles similaires. En ce qui concerne les ensembles finis, deux ensembles ordonnés quelconques ont des bons ordres similaires ; nous utilisons à nouveau le nombre ordinal n pour désigner la classe des n-ensembles. Remarquons que, par définition, deux ensembles similaires ont le même cardinal. Ainsi, on peut donner un sens au *cardinal* $|\alpha|$ d'un nombre ordinal α. Notons encore que tout sous-ensemble d'un ensemble bien ordonné est aussi bien ordonné par l'ordre induit.

Comme nous l'avons fait pour les nombres cardinaux, nous pouvons comparer deux nombres ordinaux. Soit M un ensemble bien ordonné, $m \in M$, alors $M_m = \{x \in M : x < m\}$ est appelé le *segment* (*initial*) de M déterminé par m ; N est un segment de M si $N = M_m$ pour un certain m. Ainsi, en particulier, M_m est l'ensemble vide lorsque m est le premier élément de M. Soient, maintenant, μ et ν les nombres ordinaux des ensembles bien ordonnés M et N. Nous disons que μ est *plus petit* que ν, $\mu < \nu$, si M est similaire à un segment de N. Cette relation est à nouveau transitive, c'est-à-dire que $\mu < \nu$, $\nu < \pi$ impliquent $\mu < \pi$, puisqu'une application de similarité envoie un segment sur un segment.

Le nombre ordinal de $\{1, 2, 3, \ldots\}$ est plus petit que le nombre ordinal de $\{1, 3, 5, \ldots, 2, 4, 6, \ldots\}$.

Pour les ensembles finis, $m < n$ a le sens habituel. Notons ω le nombre ordinal de $\mathbb{N}^* = \{1, 2, 3, 4, \ldots\}$ naturellement ordonné. En considérant le segment $\mathbb{N}_{n+1}$, on trouve que $n < \omega$ pour tout n fini. Ensuite, on voit que $\omega \leqslant \alpha$ pour tout nombre ordinal infini α. Bien sûr, si l'ensemble infini et bien ordonné M a pour nombre ordinal α, alors M contient un premier élément m_1, l'ensemble $M \backslash \{m_1\}$ contient un premier élément m_2, $M \backslash \{m_1, m_2\}$ contient un premier élément m_3. En continuant de cette façon, on construit une suite $m_1 < m_2 < m_3 < \ldots$ de M. Si $M = \{m_1, m_2, m_3, \ldots\}$, alors M est similaire à $\mathbb{N}^*$, et ainsi $\alpha = \omega$. D'autre part, si $M \backslash \{m_1, m_2, \ldots\}$ est non vide, alors il contient un premier élément m donc $\mathbb{N}^*$ est semblable au segment M_m, c'est-à-dire $\omega < \alpha$ par définition.

Nous énonçons maintenant (sans développer les démonstrations qui ne présentent pas de difficulté) trois résultats fondamentaux sur les nombres ordinaux. Le premier affirme que tout nombre ordinal μ a un ensemble bien ordonné « standard » W_μ qui le représente.

Proposition 1. *Soit μ un nombre ordinal. Notons W_μ l'ensemble des nombres ordinaux plus petits que μ. Alors*
(i) *les éléments de W_μ sont deux à deux comparables.*
(ii) *si l'on ordonne W_μ naturellement, alors W_μ est bien ordonné et a pour nombre ordinal μ.*

Proposition 2. *Deux nombres ordinaux μ et ν vérifient exactement l'une des relations suivantes : $\mu < \nu$, $\mu = \nu$ ou $\mu > \nu$.*

Proposition 3. *Tout ensemble de nombres ordinaux (naturellement ordonnés) est bien ordonné.*

Après cette présentation des nombres ordinaux, revenons aux nombres cardinaux. Soit $\mathfrak{m}$ un nombre cardinal. Notons $O_\mathfrak{m}$ l'ensemble de tous les nombres ordinaux μ tels que $|\mu| = \mathfrak{m}$. En utilisant la proposition 3, nous savons qu'il existe un *plus petit* nombre ordinal $\omega_\mathfrak{m}$ dans $O_\mathfrak{m}$, qu'on appelle le *nombre ordinal initial* de $O_\mathfrak{m}$. Par exemple, ω est le nombre ordinal initial de $\aleph_0$.
Après ces préliminaires, nous pouvons démontrer un résultat fondamental de ce chapitre.

Proposition 4. *Tout nombre cardinal $\mathfrak{m}$ a un successeur.*

■ **Preuve.** Nous savons déjà qu'il existe au moins un nombre cardinal $\mathfrak{n}$ supérieur à $\mathfrak{m}$. Considérons maintenant l'ensemble $\mathcal{K}$ de tous les nombres cardinaux plus grands que $\mathfrak{m}$ et inférieurs ou égaux à $\mathfrak{n}$. Associons à chaque $\mathfrak{p} \in \mathcal{K}$ son nombre ordinal initial $\omega_\mathfrak{p}$. Parmi ces nombres initiaux, il en existe un plus petit (proposition 3) ; le nombre cardinal correspondant est alors le plus petit élément de $\mathcal{K}$. C'est donc le nombre cardinal successeur de $\mathfrak{m}$ que l'on cherchait. □

Proposition 5. *Soit M un ensemble infini de cardinal $\mathfrak{m}$. Supposons M bien ordonné relativement au nombre ordinal initial $\omega_\mathfrak{m}$. Alors M n'a pas de dernier élément.*

■ **Preuve.** En effet, si M avait un dernier élément m, alors le segment M_m aurait un nombre ordinal $\mu < \omega_\mathfrak{m}$ tel que $|\mu| = \mathfrak{m}$, contredisant la définition de $\omega_\mathfrak{m}$. □

Nous avons besoin d'une amélioration considérable du résultat qui affirme que la réunion d'une famille dénombrable d'ensembles dénombrables est encore dénombrable. Dans le résultat suivant, nous considérons des familles *arbitraires* d'ensembles dénombrables.

Proposition 6. *Supposons que $\{A_\alpha\}$ soit une famille de cardinal $\mathfrak{m}$ d'ensembles au plus dénombrables A_α, où $\mathfrak{m}$ est un cardinal infini. Alors la réunion $\bigcup_\alpha A_\alpha$ a un cardinal au plus égale à $\mathfrak{m}$.*

■ **Preuve.** On peut supposer que les ensembles A_α sont deux à deux disjoints et dénombrables, puisque cette hypothèse ne peut qu'augmenter la taille de la réunion. Soit M tel que $|M| = \mathfrak{m}$ soit l'ensemble des indices, bien ordonné selon le nombre ordinal initial $\omega_\mathfrak{m}$. Remplaçons chaque $\alpha \in M$ par un ensemble au plus dénombrable $B_\alpha = \{b_{\alpha 1} = \alpha, b_{\alpha 2}, b_{\alpha 3}, \ldots\}$, ordonné par ω, et appelons le nouvel ensemble $\widetilde{M}$. Alors $\widetilde{M}$ est encore bien ordonné en posant $b_{\alpha i} < b_{\beta j}$ si $\alpha < \beta$ et $b_{\alpha i} < b_{\alpha j}$ pour $i < j$. Soit $\widetilde{\mu}$ le nombre ordinal de $\widetilde{M}$. Puisque M est un sous-ensemble de $\widetilde{M}$, on a $\mu \leqslant \widetilde{\mu}$ par un argument précédemment développé. Si $\mu = \widetilde{\mu}$, alors M est similaire à $\widetilde{M}$, et si $\mu < \widetilde{\mu}$, alors M est similaire à un segment de $\widetilde{M}$. Maintenant, puisque l'ordre $\omega_\mathfrak{m}$ sur M n'a pas de dernier élément (proposition 5), on voit que, dans les deux cas, M est similaire à la réunion d'ensembles dénombrables B_β donc de même cardinalité.

Le reste est facile. Soit $\varphi : \bigcup B_\beta \longrightarrow M$ une bijection. Supposons que $\varphi(B_\beta) = \{\alpha_1, \alpha_2, \alpha_3, \ldots\}$. Remplaçons chaque α_i par A_{α_i} et considérons la réunion $\bigcup A_{\alpha_i}$. Puisque $\bigcup A_{\alpha_i}$ est la réunion *dénombrable* d'une famille d'ensembles dénombrables (il est donc dénombrable), on voit que B_β a le même cardinal que $\bigcup A_{\alpha_i}$. En d'autres termes, il existe une bijection de B_β sur $\bigcup A_{\alpha_i}$ pour tout β donc une bijection ψ de $\bigcup B_\beta$ sur $\bigcup A_\alpha$. Par conséquent, $\psi \circ \varphi^{-1}$ fournit la bijection désirée de M sur $\bigcup A_\alpha$. Ainsi, $|\bigcup A_\alpha| = \mathfrak{m}$. □

Bibliographie

[1] L. E. J. BROUWER : *Beweis der Invarianz der Dimensionszahl,* Math. Annalen **70** (1911), 161-165.

[2] N. CALKIN & H. WILF : *Recounting the rationals,* Amer. Math. Monthly **107** (2000), 360-363.

[3] G. CANTOR : *Ein Beitrag zur Mannigfaltigkeitslehre,* Journal für die reine und angewandte Mathematik **84** (1878), 242-258.

[4] P. COHEN : *Set Theory and the Continuum Hypothesis,* W. A. Benjamin, New York 1966.

[5] P. ERDŐS : *An interpolation problem associated with the continuum hypothesis,* Michigan Math. J. **11** (1964), 9-10.

[6] E. KAMKE : *Theory of Sets,* Dover Books 1950.

[7] M. A. STERN : *Ueber eine zahlentheoretische Funktion,* Journal für die reine und angewandte Mathematik **55** (1858), 193-220.