Cantor et l'hypothèse du continu

Das Wesen der Mathematik
liegt in ihrer Freiheit.
G. Cantor

Ce texte a été écrit à l'occasion d'une invitation à donner une conférence pour des étudiants de Licence à l'Université Gustave Eiffel de Champs-sur-Marne, dans le cadre d'un séminaire *Histoire et Philosophie des Sciences*. Le texte qui suit a rapidement débordé du volume tolérable pour une conférence dont la durée prévue est de deux heures. À côté de thèmes que j'avais déjà fréquentés, j'ai découvert, en préparant, de nombreux éléments que je ne connaissais pas. J'en remercie donc chaleureusement l'organisateur Marco Cannone qui m'a permis de sortir d'une léthargie confinée et d'une inactivité tranquille.

1. Dénombrable ou non dénombrable

1.1. *Contexte historique des premiers travaux de Cantor*

Georg Cantor est né en 1845 à Saint-Pétersbourg, d'un père de nationalité danoise et d'une mère autrichienne. Pour des raisons familiales (la santé du père), les Cantor s'installent en Allemagne en 1856. Après un court passage à l'ETH de Zürich (en français : École polytechnique fédérale), Georg a étudié à l'université de Berlin à partir de 1863 ; il y a suivi en particulier les fameux cours de Karl Weierstrass. En 1867 il présente sa *Dissertation* à Berlin et en latin, « De aequationibus secundi gradus indeterminatis ». Les curieux pourront voir dans le volume de ses œuvres [CaA] son CV de l'époque, en latin, un article de théorie des nombres de 1868 (étude de formes quadratiques à coefficients entiers), et encore deux articles en 1869 à propos de nombres, puis son *Habilitation*, toujours en latin. La même année, Cantor obtient un poste à l'université de Halle, assez près de Leipzig (30 km au NO) et quelque 150 kilomètres au sud-ouest de Berlin. Georg commence véritablement ses travaux mathématiques vers 1870, avec l'article *Über einen die trigonometrischen Reihen betreffenden Lehrsatz*, qui traite des séries trigonométriques.

En août 1870, la guerre éclate entre la France et une coalition allemande, menée par la Prusse du comte Bismarck et du roi Guillaume. En septembre, Napoléon III perd une bataille importante à Sedan contre les Prussiens ; il capitule le 2 septembre. À Paris, la République est proclamée le 4 septembre. Les Prussiens, accompagnés d'autres amis Allemands, des Bavarois, des gens de Baden et du Württemberg, entrent en France sans invitation. Rapidement, les Prussiens sont près de Marne-la-Vallée, entre autres endroits autour de Paris, dont ils font le siège. Le 18 septembre 1870, le comte de Bismarck et le roi de Prusse passent de Meaux à Ferrières ([Clar, p. 275]). Le 13 octobre, les troupes allemandes sont à Châtillon, à Bagneux. Fin octobre, (p. 322) Le Bourget est attaqué depuis Garges et le Blanc-Mesnil, (p. 407) Bonneuil, Noisy-le-Grand, Ormesson, Champigny, Villiers ; Aulnay, Gournay, Gagny, Livry ; en novembre les Prussiens s'installent sur les hauteurs de Bry, de Villiers, de Champigny. De violents combats y ont lieu le 30 novembre (p. 411). Il n'y a pas que les Prussiens : il y a aussi des Bavarois, des gens du Wurtemberg, etc. Des batteries d'artillerie allemandes situées au Raincy,

Gagny, Noisy-le-Grand, Gournay bombardent le fort de Rosny. Le roi de Prusse Guillaume 1er devient Empereur d'Allemagne à Versailles en janvier 1871.

Les Français résistent en de nombreux points : le général Bourbaki est dans l'Est de la France et en Suisse. L'italien Garibaldi se bat aux côtés des Français ; il passe à Dijon. Cependant la pression sur Paris, résultant du siège, devient intenable. La France prépare un projet de paix en janvier 1871, après sa défaite qui lui coûte l'Alsace et Lorraine.

La Commune de Paris se passe entre fin mars 71 et fin mai 71, pendant que Cantor s'occupe encore de séries trigonométriques. Pendant la Commune, on fait revivre le calendrier révolutionnaire dont la date origine est en 1792 : des décrets paraissent à Paris au mois de floréal, an 79. La Commune est écrasée par les Versaillais.

Cantor va rester à l'université de Halle ; à ses débuts, il y côtoie Eduard Heine, son aîné de 24 ans, qui vient de publier un article [HeiT] sur les séries trigonométriques, et qui a probablement attiré l'attention de Cantor vers ce sujet. Heine est l'auteur de l'article [Hein] de 1872 qui contient le « théorème de Heine » sur la continuité uniforme des fonctions continues sur un segment. Cantor espérera longtemps être recruté par l'université bien plus prestigieuse de Berlin, mais cela ne se produira jamais. On considère généralement que la raison en sera l'opposition de Leopold Kronecker, l'un des deux ou trois personnages importants de l'université de Berlin (avec Ernst Kummer et Weierstrass) ; Kronecker soutenait des positions « finitistes », qui devaient ramener les mathématiques aux propriétés des entiers, et les appuyer sur des constructions explicites. Ces conceptions de Kronecker sont sans doute à l'opposé des conceptions de Cantor sur « les infinis » (et même opposées à certaines vues de Weierstrass sur la théorie des fonctions continues). Il est incontestable qu'à partir d'un certain moment, vers 1880, Cantor a vu en Kronecker une personne qui lui était hostile : on peut le lire à plusieurs reprises dans le recueil [CaB] de ses lettres à divers amis ou collègues (voir la section *Die Kollegen*, p. 4 ; la lettre 48 en 1883 et les commentaires qui lui sont attachés ; les lettres 50, 60, 61 entre beaucoup d'autres). Kronecker meurt en 1891, Cantor n'a « que » 46 ans : il n'ira tout de même pas à Berlin ; il donnera ses derniers cours à Halle pendant le semestre d'hiver 1910/11 [PuIl, ch. *Die Antinomien*, p. 165] et prendra sa retaite en 1913.

1.2. *Nombres réels*

En 1870 on intuite depuis bien longtemps la droite réelle, le plan ou l'espace (ne serait-ce que dans les théories de physique mathématique, depuis Newton, puis Euler, d'Alembert, Lagrange et l'équation des cordes vibrantes par exemple), mais comme le mentionne Heine [Hein], on le fait en général par un recours à la géométrie et à l'idée de mouvement. Mais on a bien une idée de ce que peut être un nombre réel : dès les années 1620, Henry Briggs calcule avec 30 décimales les racines carrées successives de nombres entiers pour obtenir les valeurs de logarithmes ; on devait bien imaginer que le calcul des décimales pouvait (théoriquement) être poursuivi indéfiniment. Cependant, réduire les nombres réels à une suite d'une infinité de décimales n'est pas très efficace pour bâtir une théorie.

Dirichlet, dans ses cours des années 1850, a déjà introduit une notion de fonction qui s'approche de la nôtre. À un certain moment apparaît le besoin de fournir des « vraies » preuves, d'établir de vraies bases pour les propriétés des fonctions continues, qui étaient jusque là, soit jugées évidentes (comme le théorème des valeurs intermédiaires) soit encore peu utilisées (comme le fait que le maximum d'une fonction réelle continue sur un segment soit atteint). Une mise à plat s'avère nécessaire.

Les constructions des nombres réels qui nous sont connues datent des années 1870. Elles sont dues à Cantor, à Richard Dedekind et à Charles Méray en France. Heine publie

en 1872 un article qui est une mise au point des propriétés des fonctions continues. C'est en quelque sorte comme un chapitre d'un *Bourbaki* de l'époque, qui expose ce que toute une classe de personnes pense et sait (et accepte) à ce moment donné. Heine indique dans son introduction que presque tout ce qu'il écrit vient de l'enseignement de Weierstrass ; il précise aussi que sa présentation des nombres réels doit beaucoup à Cantor, son collègue à l'Université de Halle. Précisons aussi que Heine, en écrivant cet article, s'écarte de la ligne de ses recherches principales, consacrées notamment aux *fonctions spéciales*.

La mise à plat est en partie à la base de la construction de nouveaux objets tels que la fonction de Weierstrass, périodique continue mais nulle part dérivable, l'ensemble triadique de Cantor (dans les années 1880) et la fonction de Cantor ; cette fonction f ne pourrait pas être « dessinée » ; continue sur $[0,1]$, elle croît de 0 à 1 mais « en cachette » : pour tout $\varepsilon > 0$, il existe une suite finie de segments $\mathrm{F}_1, \ldots, \mathrm{F}_q$ dont la somme des longueurs est $< \varepsilon$, et telle que f soit dérivable avec $f'(x) = 0$ pour tout x extérieur à ces segments. On assiste aussi aux débuts des notions de « topologie générale » des espaces de dimension finie : les ouverts et les fermés, les points d'accumulation...

1.2.1. *Séries trigonométriques*

Cantor commence véritablement ses travaux mathématiques vers 1870 : l'article [CaT] *Über einen die trigonometrischen Reihen betreffenden Lehrsatz*, 1870, contient le *lemme de Cantor*, l'article est signé « Berlin, le 20 mars 1870 » ; dans le même fascicule de la revue, cet article est suivi de [CaE] « *Beweis, dass* ... », 6 avril 1870, qui démontre l'unicité des coefficients d'une série trigonométrique ; ensuite, « *Notiz* ... », 6 janvier 1871. Heine signe un article « Halle, en février 1870 » : les deux hommes sont collègues à l'université de Halle et travaillent sur le même sujet, et en même temps. Ils s'intéressent à la convergence des *séries trigonométriques*, qui sont les séries de fonctions de la forme

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos(nx) + b_n \sin(nx)), \qquad x \text{ variable réelle.}$$

Si la série converge pour un x donné, alors son terme général tend vers 0,

$$a_n \cos(nx) + b_n \sin(nx) \underset{n\to\infty}{\longrightarrow} 0. \tag{1}$$

Le lemme de Cantor affirme que : *si la convergence* (1) *a lieu pour tout x d'un intervalle ouvert non vide (α, β), alors les coefficients $(a_n), (b_n)$ tendent vers zéro.*

La preuve du lemme consiste en la construction abstraite d'un nombre réel Ω dans l'intervalle, par un procédé de suite de Cauchy : l'explicitation des propriétés de nombres réels y joue son rôle.

S'appuyant sur des résultats provenant du mémoire d'Habilitation de Riemann, publié en 1867 après la mort de ce dernier, et sur un résultat de son ami (d'alors) Hermann Schwarz, Cantor prouve un théorème d'unicité : si une fonction f est représentée par une série trigonométrique qui converge *en tout point*, alors ses coefficients sont uniquement déterminés. Par différence : si une série trigonométrique converge *en tout point* vers 0, tous ses coefficients a_n, b_n sont nuls, c'est la *série nulle*.

1.2.2. *Cantor manipule le dénombrable*

Cantor va, par étapes, généraliser son théorème d'unicité, en supposant que la série trigonométrique converge en tout point *à l'exception* d'un ensemble exceptionnel E : d'abord, E sera un ensemble fini ; puis une suite convergente. Cantor va petit à petit considérer des ensembles exceptionnels de plus en plus complexes : une suite de suites, puis une suite de suites de suites, etc... et développer la notion d'ensembles dérivés (voir par exemple [Hawk, sec. 3.3]). L'abstraction de l'ordre naturel de ces suites le conduit à la notion *d'ordinal*, qui deviendra en elle seule l'un des objets de ses recherches.

On peut visualiser le premier exemple d'ordinal infini en considérant la suite

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots, \frac{1}{2^n}, \ldots$$

à laquelle on adjoint sa limite 0 pour former un compact dénombrable K_1. Si on énumère cet ensemble de façon décroissante, y compris sa limite 0 qui vient après qu'on a « lu » l'infinité de termes > 0, on obtient une image de l'ordinal ω. On peut (en sautant des étapes que Cantor considère) construire un exemple plus complexe de la façon suivante : on peut écraser K_1 par un facteur multiplicatif 2^{-n}, puis translater de 2^{-n} l'ensemble écrasé pour obtenir un ensemble compact $\mathrm{K}_{1,n}$ situé dans $[2^{-n}, 2^{-n+1})$; si A est un sous-ensemble de $[0, 1)$ et si on définit l'ensemble

$$e_n(\mathrm{A}) = \{2^{-n}(1 + a) : a \in \mathrm{A}\} \subset [2^{-n}, 2^{-n+1}),$$

on voit que $\mathrm{K}_{1,n} = e_n(\mathrm{K}_1)$. La réunion des $\mathrm{K}_{1,n}$ et de $\{0\}$ fournit un compact K_2 plus complexe que K_1 : si on parcourt K_2, encore en décroissant, il faudra passer à la limite une infinité de fois. On peut reprendre avec des $\mathrm{K}_{2,n}$ pour avoir une image K_3 de ω^3, un ensemble encore plus complexe. Après avoir construit tous les K_n, il faut un argument un peu différent pour poursuivre : dans l'intervalle $[2^{-n}, 2^{-n+1})$ on place l'écrasé $e_n(\mathrm{K}_n)$ de K_n : ainsi une « copie » de chaque ensemble K_n déjà construit apparaît dans un nouveau compact dénombrable K_ω. Ça ne finit jamais.

Après cette vision géométrique, considérons une option numérique pour approcher les « petits » ordinaux. Commençons par rappeler la définition de *l'ordre lexicographique* sur les puissances d'un ensemble ordonné. Si X est un ensemble totalement ordonné et $k \geqslant 1$ un entier fixé, définissons un ordre sur les k-uplets $\mathbf{x} := (x_1, \ldots, x_k)$ d'éléments de X de la façon suivante : si $\mathbf{y} := (y_1, \ldots, y_k)$ est donné, on dit que $\mathbf{x} < \mathbf{y}$ si $\mathbf{x} \neq \mathbf{y}$ et si, pour le premier (le plus petit) indice j tel que $x_j \neq y_j$, on a $x_j < y_j$. Ainsi

$$(0, 9, 8) < (1, 0, 0)\,;\ \ (3, 1, 9) < (3, 2, 0)\,;\ \ (3, 6, 8) < (3, 6, 9).$$

On peut faire entrer dans ce schéma l'ordre usuel des entiers $\geqslant 0$, représentés en écriture décimale, si étant donné deux entiers m et n dont les écritures décimales sont de longueur différente, on commence par allonger « l'écriture » la plus courte avec des 0 en tête, pour qu'elle ait la même longueur que l'autre, on la considère ensuite comme une suite de chiffres, par exemple

$$m = 99 < n = 100\,;\ \ m \to (0, 9, 9),\ n \to (1, 0, 0),\ \ \text{et on a bien } (0, 9, 9) < (1, 0, 0)$$

en ordre lexicographique, avec $\mathrm{X} = \{0, 1, \ldots, 9\}$ ordonné par $0 < 1 < \ldots < 9$.

Si on remplace cet ensemble X à 10 éléments par $\mathbb{N}$, on obtient une nouvelle représentation de certains ordinaux comme suites finies d'entiers $\geqslant 0$ ordonnées lexicographiquement, avec la convention d'allongement qu'on vient de décrire pour égaliser les longueurs. On a d'abord la suite croissante

$$0, 1, 2, \ldots, n, \ldots$$

et le premier élément qui les dépasse tous est $(1, 0)$ (avec notre convention, $(0, 0)$ est une représentation impropre de 0, le plus petit élément) ; dans les notations de Cantor, il s'agit de ω. Ensuite viennent les $(1, n)$, suivis des $(2, n)$, des $(3, n)$; le premier qui les dépasse tous est $(1, 0, 0)$ qui correspond à ω^2. Cette vision par des suites finies est limitée : on pourra représenter ainsi par des suites $(1, 0, \ldots, 0)$ tous les ω^k, mais on n'aura pas ω^ω, qui est le premier qui dépasse tous les ω^k. Pour aller plus loin, on pourrait ajouter une nouvelle « place » en tête, séparée par un nouveau symbole, par exemple $(1\,;0)$ qui dépasserait les éléments précédents, récrits sous la forme $(0\,;0, 0, 5, 8)$ par exemple. On pourrait continuer avec les $(n\,;0)$, majorés par $(1, 0\,;0)$, puis les $(1, 0, \ldots, 0\,;0)$. Mais on se heurtera à une nouvelle limite.

Ce qu'on vient de faire se rattache à la description de l'ordinal noté ω^γ, où γ est un ordinal : désignons d'abord par $\mathrm{S}(\gamma)$ l'ensemble des ordinaux $< \gamma$, puis par $\mathcal{F}_0(\gamma, \omega)$ l'ensemble des applications f de $\mathrm{S}(\gamma)$ dans $\mathrm{S}(\omega) = \mathbb{N}$, qui ne prennent qu'un nombre fini de valeurs non nulles. On peut associer à f une suite finie d'entiers $(m_{\alpha_1}, \ldots, m_{\alpha_j})$ indexée par des ordinaux $\alpha_j < \ldots < \alpha_1 < \gamma$ où

$$\{\alpha_1, \ldots, \alpha_j\} = \{\alpha < \gamma \,:\, f(\alpha) \neq 0\} \quad \text{et } m_{\alpha_i} = f(\alpha_i) > 0,\ i = 1, \ldots, j.$$

Pour rappeler l'application f, on pourrait noter $\alpha_1 \mapsto m_1$ au lieu de m_{α_1}. Ainsi, l'élément de ω^8 qu'on a pu noter $(3, 0, 5, 0, 0, 4, 0, 9)$ serait désigné ici par

$$(3_7, 5_5, 4_2, 9_0) \ \text{ ou bien } (7 \mapsto 3,\ 5 \mapsto 5,\ 2 \mapsto 4,\ 0 \mapsto 9), \ \text{ avec } \mathrm{S}(8) = \{0, 1, \ldots, 7\}.$$

Il faut faire une exception pour l'application identiquement nulle, qui donnerait une suite *vide* d'indices i tels que $f(i) \neq 0$: on pourrait la représenter par $()$, ou plutôt par $0 \mapsto 0$ (le seul cas où l'entier au bout de la flèche est nul). Les entiers n de $\mathbb{N} = \mathrm{S}(\omega)$ sont représentés dans $\mathcal{F}_0(\gamma, \omega)$ par les « suites » d'un seul terme, de la forme $(0 \mapsto n)$.

L'ensemble $\mathcal{F}_0(\gamma, \omega)$ est ordonné ainsi : le plus petit élément est la suite vide (ou bien la fonction f identiquement nulle) ; ensuite on dira que

$$(\alpha_1 \mapsto m_1,\ \ldots,\ \alpha_j \mapsto m_j) < (\beta_1 \mapsto n_1,\ \ldots,\ \beta_k \mapsto n_k),$$

où $\gamma > \alpha_1 > \ldots > \alpha_j$ et $\gamma > \beta_1 > \ldots > \beta_k$, exactement dans les cas suivants :

si $\alpha_1 < \beta_1$ avec $n_1 > 0$,

ou si : $\alpha_1 = \beta_1$ et $m_1 < n_1$,

ou si : $\alpha_1 = \beta_1$ et $m_{\alpha_1} = n_{\beta_1}$ et $(\alpha_2 \mapsto m_2,\ \ldots,\ \alpha_j \mapsto m_j) < (\beta_2 \mapsto n_2,\ \ldots,\ \beta_k \mapsto n_k)$.

Le successeur de $(\alpha_1 \mapsto m_1,\ \ldots,\ \alpha_j \mapsto m_j)$ est $(\alpha_1 \mapsto m_1,\ \ldots,\ \alpha_j \mapsto m_j, 0 \mapsto 1)$ si $\alpha_j > 0$ et $(\alpha_1 \mapsto m_1,\ \ldots,\ \alpha_j \mapsto m_j + 1)$ si $\alpha_j = 0$. On peut voir que cet ordre est un bon ordre sur $\mathcal{F}_0(\gamma, \omega)$, l'ordinal ω^γ en est le « type d'ordre ».

Les ordinaux $< \omega^\omega$ peuvent être décrits par des suites $(k_1 \mapsto n_1, \ldots, k_p \mapsto n_p)$ où $k_1 > k_2 > \ldots > k_p$ sont des entiers. Les ordinaux $< \omega^{\omega^\omega}$ pourront être décrits par des suites $(\alpha_1 \mapsto m_1, \ldots, \alpha_k \mapsto m_q)$ où les α_i sont $< \omega^\omega$, ce qui pourrait s'écrire

$$\big((k_{1,1} \mapsto n_{1,1}, \ldots, k_{1,p_1} \mapsto n_{1,p_1}) \mapsto m_1,\ \ldots\ ,\ (k_{q,1} \mapsto n_{q,1}, \ldots, k_{q,p_q} \mapsto n_{q,p_q}) \mapsto m_q\big).$$

L'ensemble $\mathrm{S}(\omega^\omega)$, identifié à $\mathcal{F}_0(\omega,\omega)$, apparaît dans $\mathcal{F}_0(\omega^\omega,\omega)$ sous la forme des suites d'éléments $\alpha_i \mapsto m_i$, $i = 1,\dots,q$ avec α_i dans la partie de ω^ω qui représente $\mathrm{S}(\omega)$, c'est-à-dire les $\alpha_i = (0 \mapsto n_i)$; on obtient ainsi les éléments

$$\big((0\mapsto n_1)\mapsto m_1,\ \dots\ ,\ (0\mapsto n_q)\mapsto m_q\big).$$

On pourrait encore continuer sous forme d'arbre, mais avec une limite qu'on appellera ε_0 et qu'on expliquera plus bas.

Il existe de nombreux systèmes, qui deviennent rapidement très complexes, pour « décrire » des ordinaux dénombrables aussi grands que possible, en respectant la règle suivante : si le système de notation peut décrire un ordinal β, il doit aussi pouvoir décrire tous les ordinaux α plus petits que β. Le lecteur pourra s'amuser à consulter l'article *Grand ordinal dénombrable* de Wikipedia et les articles qui lui sont reliés. Chaque système de notation permet de décrire les ordinaux plus petits qu'une certaine limite, la limite pouvant justement être définie comme la limite des possibilités descriptives de ce système de notation ! Il existe par ailleurs un ordinal dénombrable β_0 à partir duquel on n'aura plus de système de notation possible pour décrire la totalité de la famille des ordinaux $\alpha < \beta_0$: cela n'empêchera pas de pouvoir *définir* β_0, ni de pouvoir « nommer » un certain nombre de successeurs de β_0, à commencer par $\beta_0 + 1$.

Cantor a donné un système de notation qui permet de décrire les ordinaux plus petits que l'un des termes de la suite

$$\omega,\ \omega^\omega,\ \omega^{\omega^\omega},\ \omega^{\omega^{\omega^\omega}},\ \dots$$

c'est-à-dire la suite $(\gamma_n)_{n\geqslant 0}$ où $\gamma_0 = \omega$ et où $\gamma_{n+1} = \omega^{\gamma_n}$, dont la limite est notée ε_0. Cette limite ε_0 vérifie la « propriété de point fixe » $\omega^{\varepsilon_0} = \varepsilon_0$.

1.2.3. *Non dénombrabilité*

En marge de ces développements sur les ordinaux, dans un article [Ca1] de 1874 (signé du 23 décembre 1873), Cantor énonce le résultat qui suit. Je vais essayer de traduire fidèlement et de garder les notations de Cantor.

Quand, par une loi quelconque, est donnée une suite infinie de nombres réels deux à deux distincts

(4.) $$\omega_1, \omega_2, \dots, \omega_\nu, \dots$$

alors, dans tout intervalle donné $(\alpha \dots \beta)$ *on peut trouver un nombre* η *(et par conséquent, une infinité de tels nombres) qui n'est pas dans la suite* (4.).

Il va de soi, même si Cantor ne l'écrit pas dans l'énoncé, que l'intervalle est supposé non vide : $\alpha < \beta$.

Preuve de Cantor, avec ses symboles et dans la mesure de mes facultés traductrices, avec ses propres mots

On désigne par α', β' les deux premiers nombres de la suite (4.) qui se trouvent dans l'intérieur de l'intervalle ouvert (α, β) et on suppose $\alpha' < \beta'$ [(†) : *voir NdT plus bas*] ; de même, on désigne par α'', β'' les deux premiers nombres dans notre suite qui se trouvent dans l'intérieur de $(\alpha' \dots \beta')$, on suppose $\alpha'' < \beta''$, puis par la même règle on construit un intervalle $(\alpha''' \dots \beta''')$ et ainsi de suite.

D'après la définition, $\alpha', \alpha'', \ldots$ sont des nombres de notre suite (4.), deux à deux distincts et dont les indices sont croissants, et de même pour les nombres $\beta', \beta'', \ldots$; de plus, les valeurs $\alpha', \alpha'', \ldots$ sont croissantes, les valeurs $\beta', \beta'', \ldots$ sont décroissantes ; chacun des intervalles $(\alpha \ldots \beta)$, $(\alpha' \ldots \beta')$, $(\alpha'' \ldots \beta'')$ contient les suivants. Il n'y a que deux cas possibles.

Ou bien le nombre des intervalles ainsi formés est fini ; soit $(\alpha_\nu \ldots \beta_\nu)$ le dernier d'entre eux ; comme il ne peut y avoir dans ce dernier intervalle qu'au plus un élément de la suite (4.), on peut trouver un nombre η dans cet intervalle qui n'est pas dans la suite (4.), et dans ce cas le résultat est obtenu. —

Ou le nombre des intervalles formés est infini ; alors les nombres $\alpha, \alpha', \alpha'', \ldots$, qui croissent sans tendre vers l'infini [*voir* (‡) *plus bas*], ont une limite α^∞ ; de même, les nombres $\beta, \beta', \beta'', \ldots$, décroissants, ont une limite β^∞ ; si $\alpha^\infty = \beta^\infty$ (un cas qui se produit quand la suite est la suite des nombres algébriques) on se rend compte facilement que le nombre $\eta = \alpha^\infty = \beta^\infty$ ne peut pas faire partie de notre suite*) ; si $\alpha^\infty < \beta^\infty$, tout nombre η à l'intérieur de l'intervalle $(\alpha^\infty \ldots \beta^\infty)$ ou aux extrémités a la propriété de ne pas être contenu dans la suite (4.). —

Note de Cantor, en bas de page :

*) Si le nombre η faisait partie de notre suite, on aurait $\eta = \omega_p$, où p serait un certain indice ; mais cela n'est pas possible, car ω_p ne se trouve pas à l'intérieur de l'intervalle $(\alpha^{(p)} \ldots \beta^{(p)})$, alors que le nombre η, d'après notre définition, est dans l'intérieur de cet intervalle.

Notes du Traducteur :

(†) Cantor envisage, sans le dire à l'endroit du renvoi, que ce couple de nombres peut ne pas exister —soit parce qu'aucun nombre de la suite ne se trouve dans l'intervalle ouvert (α, β), soit parce qu'*un seul* nombre de la suite se trouve dans l'intervalle et pas deux— ce qui est évidemment possible puisque la suite est quelconque. Dans ce cas le processus s'arrête, c'est envisagé dans la suite de la preuve de Cantor.

(‡) Les $\alpha, \alpha', \ldots$, sont majorés par β, par exemple.

Corollaire. *L'ensemble des nombres réels n'est pas dénombrable.*

Preuve. Plutôt que de simplement déduire, récrivons la preuve de façon plus algorithmique ; on donne une suite $(x_i)_{i \geqslant 0}$ de nombres réels qu'on suppose deux à deux distincts. On va construire par récurrence une suite de segments emboîtés $[a_n, b_n]$, telle que pour tout $n \geqslant 0$ on ait

$$[a_{n+2}, b_{n+2}] \subset (a_n, b_n)$$

et une suite $k(n)$ d'entiers, qui est strictement croissante et telle que : pour tout indice $i < k(n+1)$, on a $x_i \notin (a_n, b_n)$, et $x_{k(n+1)}$ est égal, soit à a_{n+1}, soit à b_{n+1}.

Au pas 0 de la procédure, on donne (pour fixer les idées) le segment $\mathrm{S}_0 = [0, 1]$, on pose $\mathrm{I}_0 = (0, 1)$, $a_0 = 0$, $b_0 = 1$. On désigne par $k(1)$ le plus petit entier i tel que $x_i \in \mathrm{I}_0$: les éléments de la suite dont l'indice est $< k(1)$ sont donc en dehors de I_0, mais $a_0 < x_{k(1)} < b_0$. On pose alors $a_1 = x_{k(1)}$, $b_1 = b_0$. On a $a_0 < a_1 < b_1 = b_0$, on pose $\mathrm{S}_1 = [a_1, b_1]$ et $\mathrm{I}_1 = (a_1, b_1)$.

On désigne par $k(2)$ le plus petit entier i tel que $x_i \in \mathrm{I}_1$, donc $a_1 < x_{k(2)} < b_1$; les éléments d'indice $< k(2)$ sont en dehors de I_1. On pose alors $a_2 = a_1$, $b_2 = x_{k(2)}$, $\mathrm{S}_2 = [a_2, b_2]$, $\mathrm{I}_2 = (a_2, b_2)$. On a maintenant $a_0 < a_1 = a_2 < b_2 < b_1 = b_0$, autrement dit

$$[a_2, b_2] \subset (a_0, b_0).$$

À l'instant $n \geqslant 1$ de la procédure, on a déjà lu les éléments de la suite jusqu'à un certain rang $k(n)$ inclus, on a singularisé un segment $\mathrm{S}_n = [a_n, b_n]$, avec $a_n < b_n$; on sait que tous les éléments de la suite dont l'indice est $< k(n)$ sont extérieurs à I_{n-1}, de plus $x_{k(n)}$ est égal, soit à a_n, soit à b_n, donc il n'est pas dans I_n.

On sait qu'en continuant la lecture de la suite pour les indices $i > k(n)$ on finira par trouver des éléments x_i de la suite, tels que $a_n < x_i < b_n$; si $k(n+1)$ est le plus petit indice i possible pour lequel $x_i \in \mathrm{I}_n$, on aura $a_n < x_{k(n+1)} < b_n$ et aucun élément de la suite strictement avant $k(n+1)$ ne sera dans $\mathrm{I}_n = (a_n, b_n)$.

Si n est impair, on pose $a_{n+1} = a_n$, $b_{n+1} = x_{k(n+1)} < b_n$, sinon on pose $a_{n+1} = x_{k(n+1)} > a_n$, $b_{n+1} = b_n$. On a ainsi pour tout entier $p \geqslant 0$

$$a_{2p} < a_{2p+1} < b_{2p+1} = a_{2p}, \quad a_{2p+1} = a_{2p+2} < b_{2p+2} < a_{2p+1},$$

de sorte que $a_{2p} < a_{2p+1} = a_{2p+2} < a_{2p+3}$, par conséquent $a_n < a_{n+2}$ pour tout $n \geqslant 0$, et de même $b_n < b_{n+2}$ pour tout $n \geqslant 0$. On a bien $\mathrm{S}_{n+2} \subset \mathrm{I}_n$ comme promis. Par la propriété des segments emboîtés, il existe un élément x qui est commun à tous les segments. Il s'agit de voir qu'il ne peut pas appartenir à la suite.

Supposons que $x = x_i$. La suite $k(n)$ est strictement croissante, elle dépasse tout entier donné, il existe donc un entier n tel que $i < k(n)$. Par construction, cela entraîne que $x_i \notin \mathrm{I}_n$ donc $x_i \notin \mathrm{S}_{n+2}$, contradiction. □

Cantor donnera plus tard, en 1891 une autre preuve de la non-dénombrabilité de $\mathbb{R}$, celle qu'on appelle l'*argument diagonal* de Cantor. On y reviendra.

Cantor établit les premiers résultats sur la dénombrabilité : par exemple, il montre que $\mathbb{N} \times \mathbb{N}$ peut être mis en bijection avec $\mathbb{N}$ par une bijection explicite dont vous avez sans doute aperçu le schéma : on parcourt successivement les *diagonales* $m + n = k$, on peut même écrire une bijection explicite

$$\varphi(m,n) = (0 + 1 + 2 + \cdots + (m+n)) + n,$$

$$= \frac{(m+n)(m+n+1)}{2} + n \;=\; \frac{m^2 + 2mn + n^2 + m + n + 2n}{2},$$

$$(0,0) \to 0, \quad (1,0) \to 1, \quad (0,1) \to 2, \quad (2,0) \to 3, \quad (1,1) \to 4, \quad \ldots.$$

Si (E_n) est une suite d'ensembles dénombrables, sa réunion $\mathrm{E} = \bigcup \mathrm{E}_n$ est dénombrable : si φ_n est une bijection de E_n sur $\mathbb{N}$, et $x \in \mathrm{E}$ et si n est le plus petit entier n tel que $x \in \mathrm{E}_n$, la formule $\varphi(x) = \varphi_n(x)$ définit une surjection de $\mathrm{E} = \bigcup \mathrm{E}_n$ sur $\mathbb{N} \times \mathbb{N}$, donc E est dénombrable. Il en résulte que l'ensemble des suites finies d'entiers est dénombrable.

1.3. *Nombres algébriques, nombres transcendants*

Un *nombre algébrique* θ est solution d'une équation polynomiale à coefficients entiers (à coefficients dans $\mathbb{Z}$, ou bien à coefficients rationnels : en « chassant » le dénominateur commun des coefficients rationnels, on se ramène au cas des coefficients entiers), de la forme

$$a_n\theta^n + \cdots + a_1\theta + a_0 = 0, \quad a_n \neq 0,$$

pour un certain entier $n \geqslant 2$ (le cas $n = 0$ n'a pas de sens, le cas $n = 1$ ne donne que des θ rationnels : $\theta = -a_0/a_1$). Un exemple de nombre algébrique est donné par $\theta = \sqrt{2}$, racine du polynôme $\mathrm{X}^2 - 2 \in \mathbb{Z}[\mathrm{X}]$. Un réel non algébrique est appelé *transcendant*. Il n'est pas

facile de montrer qu'un nombre tel que π est transcendant, mais on peut relativement facilement « fabriquer » un transcendant ; de plus, quand on en a un, appelons-le ξ, on a en beaucoup d'autres : tous les $\xi+r$ avec r rationnel sont transcendants aussi (développer les puissances $(\xi + r)^k$ dans une équation d'algébricité supposée de $\xi + r$ pour obtenir une équation polynomiale en ξ à coefficients rationnels).

Le fait que π soit transcendant a été prouvé en 1882 par Carl von Lindemann [Lind] ; incidemment, c'est Cantor qui a été chargé par Felix Klein, directeur de la revue *Mathematische Annalen*, de lire l'article avant sa publication [CaB, lettres 25, 26 et 27]. Bien avant, on avait déjà prouvé que π est irrationnel (Johann Heinrich Lambert, vers 1760), ça n'était déjà pas simple. La transcendance de π implique l'impossibilité de la *quadrature du cercle* : il est impossible de construire à la règle et au compas un segment de longueur π à partir d'un segment unité. Il n'est pas très difficile en effet de montrer que les quantités construites à la règle et au compas sont algébriques, et même, algébriques d'un type particulier.

Les polynômes à coefficients entiers correspondent aux suites finies d'entiers, ils forment un ensemble dénombrable, et chacun d'eux a un nombre fini de racines. L'ensemble des nombres algébriques est donc dénombrable. Cantor l'explique et conclut au résultat qui suit.

Corollaire. *Il y a vraiment beaucoup de nombres réels qui ne sont pas algébriques.*

1.3.1. *Nombres de Liouville*

Il est sans doute bien plus satisfaisant d'avoir des exemples explicites de nombres transcendants, comme celui qu'a mentionné Joseph Liouville en 1844 ([Lio1], puis [Lio2]) un exemple qui est défini par une série numérique (en marge de résultats plus généraux utilisant les *fractions continues*). On va essayer de donner une idée de preuve, abusivement longue mais très élémentaire, pour ces exemples de séries *a la Liouville*, en montrant comment construire un nombre réel x, somme d'une série « explicite », qui ne satisfait —pour une simple illustration— aucune équation polynomiale de degré 3 à coefficients entiers. Il est commode (mais pas indispensable) d'utiliser la numération binaire. Pour commencer d'expliquer les idées sur un exemple élémentaire, soit y la somme d'une série numérique de la forme

$$y = \frac{1}{2} + \frac{1}{16} + \frac{1}{256} + \frac{1}{512} + \frac{1}{4096} + \cdots$$

où tous les termes de la série sont de la forme 2^{-n}, distincts, et où on peut observer un « trou » entre $1/16$ et $1/256$. Alors l'expression de

$$16\,y = 8 + 1 + \frac{1}{16} + \frac{1}{32} + \frac{1}{256} + \cdots$$

commence par l'entier impair 9, le reste $16\,y - 9$ (non entier) vérifie

$$0 < \frac{1}{16} + \frac{1}{32} + \frac{1}{256} + \cdots < \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \frac{1}{128} + \frac{1}{256} + \frac{1}{512} + \cdots = \frac{1}{8},$$

donc $16\,y$ est plutôt proche d'un entier impair, en tout cas plus proche de 9 que de tout entier pair. Pour

$$32\,y = 16 + 2 + \frac{1}{8} + \frac{1}{16} + \frac{1}{128} + \cdots,$$

on est, à l'inverse, proche d'un entier pair. La preuve utilisera les évidences suivantes : la somme d'un impair et de plusieurs pairs est impaire ; un nombre impair n'est pas nul, un nombre réel suffisamment proche d'un impair n'est pas nul non plus !

Un nombre réel x étant donné, cet argument-massue sera, si possible, appliqué à un multiple $2^k\mathrm{A}$ convenable d'un nombre A de la forme

$$\mathrm{A} = a_3x^3 + a_2x^2 + a_1x + a_0, \quad a_0, a_1, a_2, a_3 \in \mathbb{Z},\ a_3 \neq 0,$$

pour en déduire que A lui-même n'est pas nul, et que x n'est pas racine de ce polynôme. Attention : si $z = i + \varepsilon$ est presque impair parce que i est un entier impair et ε un réel « petit », il ne faut pas se précipiter à dire que z^3 est presque impair ; en effet, le développement de z^3 contient $3i^2\varepsilon$, qui pose problème si i est grand et ε pas assez petit.

Maintenant allons-y ; considérons un sous-ensemble infini $\mathrm{L} \subset \mathbb{N}$, qui soit formé d'entiers $\geqslant 1$, dont on devra préciser plus loin certaines propriétés, et posons

$$x = \sum_{\ell\in\mathrm{L}} 2^{-\ell} \leqslant \sum_{k\geqslant 1} 2^{-k} = 1.$$

Pour $k \geqslant 0$ entier donné, cherchons si 2^kx est proche d'un entier ; découpons l'ensemble L en deux parties disjointes $\mathrm{L}_{\leqslant k}$ et $\mathrm{L}_{>k}$ définies par

$$\mathrm{L}_{\leqslant k} = \{\ell \in \mathrm{L} : \ell \leqslant k\}, \quad \mathrm{L}_{>k} = \{\ell \in \mathrm{L} : \ell > k\},$$

et écrivons

$$2^kx = \sum_{\ell\in\mathrm{L}} 2^{k-\ell} = \mathrm{S}_k + \mathrm{S}'_k, \quad \text{où } \mathrm{S}_k = \sum_{\ell\in\mathrm{L}_{\leqslant k}} 2^{k-\ell} \ \text{ et } \ \mathrm{S}'_k = \sum_{\ell\in\mathrm{L}_{>k}} 2^{k-\ell}.$$

L'ensemble $\mathrm{L}_{>k}$ est non vide pour tout entier $k \geqslant 1$, étant donné que L est supposé infini ; on a donc toujours $\mathrm{S}'_k > 0$ et par conséquent

$$(s) \qquad 0 \leqslant \mathrm{S}_k = 2^kx - \mathrm{S}'_k < 2^kx \leqslant 2^k.$$

L'ensemble $\mathrm{L}_{\leqslant k}$ des indices de la somme S_k peut être vide, si tous les éléments de L sont $> k$; dans ce cas, par convention, on pose $\mathrm{S}_k = 0$, qui est un entier. Dans le cas contraire où $\mathrm{L}_{\leqslant k}$ n'est pas vide, on a $k - \ell \geqslant 0$ pour tous les termes de la somme S_k, c'est une somme d'entiers donc S_k est un entier.

Supposons que l'ensemble L présente *un trou de largeur* $u \geqslant 1$ *à la place* $k + 1$, c'est-à-dire qu'aucun des entiers $k + 1, k + 2, \ldots, k + u$ n'appartienne à L. Dans ce cas tous les éléments de L qui vérifient $\ell > k$ vérifient aussi $\ell > k + u$, par conséquent

$$\mathrm{S}'_k = \sum_{\ell\in\mathrm{L}_{>k+u}} 2^{k-\ell} \leqslant \sum_{p>k+u} 2^{k-p} = \sum_{r>u} 2^{-r} = 2^{-u}$$

et donc, en rappelant aussi (s), on a en posant $\varepsilon = \mathrm{S}'_k$ les propriétés

$$(\mathrm{D}_1) \qquad 2^kx = \mathrm{S}_k + \varepsilon,\ \ \mathrm{S}_k \in \mathbb{N},\ \ \mathrm{S}_k \leqslant 2^k,\ \ \varepsilon \leqslant 2^{-u}.$$

Pour aller plus loin, demandons-nous si l'entier S_k, qui est très proche de $2^k x$ quand u est grand, est pair ou impair. Si $\mathrm{L}_{\leqslant k}$ est vide, $\mathrm{S}_k = 0$ est pair et $k \notin \mathrm{L}$; sinon, désignons par p le plus grand élément de $\mathrm{L}_{\leqslant k}$. Alors

$$\mathrm{S}_k = \sum_{\ell \in \mathrm{L},\, \ell < p} 2^{k-\ell} + 2^{k-p} =: s_k + 2^{k-p} ;$$

la première somme s_k est formée d'entiers pairs, la parité de S_k dépend donc du deuxième terme 2^{k-p}, où $k-p \geqslant 0$, et 2^{k-p} n'est impair que quand il vaut 1, autrement dit quand $k = p$, ce qui veut dire que $k \in \mathrm{L}$. En résumé,

(D_2) $\qquad \mathrm{S}_k$ est impair si $k \in \mathrm{L}$, $\quad \mathrm{S}_k$ est pair si $k \notin \mathrm{L}$.

Pour construire l'exemple il va falloir « faire des trous » ! On supposera qu'il existe un sous-ensemble infini $\mathrm{M} \subset \mathrm{L}$ et une suite $(v_m)_{m \in \mathrm{M}}$ d'entiers $\geqslant 1$ tendant vers l'infini quand $m \in \mathrm{M}$ devient grand, tels que :

—• pour tout $m \in \mathrm{M}$, l'ensemble L présente un trou de largeur $u'_m = 2m + v_m$ à la place $m+1$, c'est-à-dire que

$$\mathrm{L} \cap \{m+1, \ldots, 3m + v_m\} = \emptyset.$$

Il en résulte que L présente un trou de largeur $u''_m = m + v_m$ à la place $2m+1$, et que l'entier $2m$ n'est pas dans L.

Quand $m \in \mathrm{M} \subset \mathrm{L}$ devient grand, on sait d'après (D_1) et (D_2) que $2^m x$ est « presque impair », et plus précisément qu'il existe un entier impair $i_m \geqslant 1$ tel que

$$2^m x = i_m + \varepsilon'_m, \quad i_m \leqslant 2^m, \ 0 < \varepsilon'_m \leqslant 2^{-u'_m} = 2^{-2m-v_m}.$$

On développe

$$(2^m x)^3 = i_m^3 + 3\, i_m^2 \varepsilon'_m + 3\, i_m \varepsilon'^2_m + \varepsilon'^3_m$$

pour montrer que $(2^m x)^3$ est presque impair quand m est grand : en effet, l'entier i_m^3 est un entier impair, $3\, i_m^2 \varepsilon'_m \leqslant 3 \,.\, 2^{2m} 2^{-2m-v_m} = 3 \,.\, 2^{-v_m}$ tend vers 0, de même que $3\, i_m \varepsilon'^2_m$ (plus facile) et évidemment de même que ε'^3_m ; ainsi $2^{3m} x^3$ est presque impair quand m est grand.

Considérons

$$\mathrm{A} = a_3 x^3 + a_2 x^2 + a_1 x + a_0, \quad a_0, a_1, a_2, a_3 \in \mathbb{Z}, \ a_3 \neq 0.$$

Notre objectif est de montrer que A n'est jamais nul. Écrivons l'entier non nul a_3 sous la forme $a_3 = 2^q b$ avec b impair et q entier $\geqslant 0$. Pour tout $q \in \mathbb{N}$ fixé, dès que $m > q$, $2m - q > m$ est dans l'intervalle $[m+1, 3m + v_m]$ qui ne contient aucun élément de L ; on a donc $2m - q \notin \mathrm{L}$ et l'ensemble L présente un trou de largeur $u''_m + q$ à la place $2m - q + 1$; pour simplifier les écritures, on se contentera d'un trou de largeur plus petite u''_m à cette même place (on a $u''_m \leqslant u''_m + q$). On sait par conséquent d'après (D_1) et (D_2), appliqués à la place $k = 2m - q \notin \mathrm{L}$, qu'il existe un entier pair p_m tel que

$$2^{2m-q} x = p_m + \varepsilon''_m, \quad 0 < p_m \leqslant 2^{2m-q} \leqslant 2^{2m}, \ 0 < \varepsilon''_m \leqslant 2^{-u''_m} = 2^{-m-v_m}.$$

En conséquence, pour tout q fixé, les nombres réels $2^{2m-q}x$ sont presque pairs quand $m \in \mathrm{M}$ est grand.

Considérons la quantité $2^{3m-q}\mathrm{A}$ où $m \in \mathrm{M}$ restera « très grand » dans toute la suite de la preuve. D'abord, $2^{3m-q}a_3x^3 = b2^{3m}x^3$ est presque impair puisque b est impair et qu'on a vu que $2^{3m}x^3 = (2^m x)^3$ est presque impair. Ensuite

$$2^{3m-q}a_2x^2 = a_2(2^{2m-q}x)(2^m x) = a_2(p_m + \varepsilon''_m)(i_m + \varepsilon'_m)$$

$$= a_2 p_m i_m + a_2(p_m\varepsilon'_m + i_m\varepsilon''_m + \varepsilon''_m\varepsilon'_m)$$

est presque pair puisque l'entier $a_2p_mi_m$ est pair, que $p_m\varepsilon'_m \leqslant 2^{2m}2^{-2m-v_m} = 2^{-v_m}$ et $i_m\varepsilon''_m \leqslant 2^m 2^{-m-v_m} = 2^{-v_m}$ tendent vers 0, ainsi que $\varepsilon''_m\varepsilon'_m$ évidemment.

On continue avec $2^{3m-q}a_1x = a_1(2^{2m-q})(2^m x)$ qui est presque pair puisque $a_1 2^{2m-q}$ est pair et $2^m x$ presque entier. Enfin $2^{3m-q}a_0$ est pair et au total $2^{3m-q}\mathrm{A}$, somme de plusieurs presque pairs et d'un seul presque impair, est presque impair, donc non nul, et il en résulte que $\mathrm{A} \neq 0$: le nombre x ne peut pas satisfaire une équation polynomiale de degré 3. □

Le lecteur patient pourra deviner que

$$\xi = \sum_{n \geqslant 1} 2^{-n!}$$

est transcendant (c'est un cas particulier de l'exemple de Liouville, qui le donne plus généralement en remplaçant 2 par un entier $a \geqslant 2$ quelconque). On peut prendre ici

$$\mathrm{M} = \mathrm{L} = \{n! \ : \ n \geqslant 1\} \subset \mathbb{N}.$$

En effet, en posant $m = n!$ on voit qu'il existe dans L un très grand trou à la place $m+1$, de largeur $(n+1)! - n! - 1 = n.n! - 1$. Pour tout degré $p \geqslant 2$ fixé, ce trou dans L est de largeur $\geqslant (p-1)\,m + v_m$ pour $m = n!$ grand, on peut adapter au degré p la preuve précédente, sans aucune difficulté conceptuelle supplémentaire.

2. Le continu et les ensembles

2.1. *Cantor et les ensembles*

Cantor donne en 1891, dans une petite note qui tient sur trois pages [Ca3], une autre preuve de la non-dénombrabilité de $\mathbb{R}$, qui s'inscrit dans la preuve plus générale du fait que l'ensemble des parties d'un ensemble a un cardinal strictement plus grand que le cardinal de l'ensemble. Donnons d'abord la preuve dans un langage compréhensible par un lycéen. À chaque nombre réel x de $[0,1)$, associons son développement en base 10, son développement décimal *propre* (c'est-à-dire qu'il y a une infinité de décimales qui ne sont pas égales à 9)

$$\overline{0, a_1\, a_2 \ldots a_k \ldots}, \qquad a_j \in \{0, 1, \ldots, 9\},$$

qu'on peut récrire

$$x = \sum_{k=1}^{\infty} a_k 10^{-k}.$$

Si $[0,1)$ était dénombrable, on pourrait dresser une liste $(x^{(n)})_{n\geqslant 1}$ de tous les nombres de cet intervalle. Pour chaque $x^{(n)}$, on aurait une suite de décimales

$$\overline{0, a_1^{(n)}\, a_2^{(n)} \dots a_k^{(n)} \dots}.$$

L'objectif est de « fabriquer » un nombre y qui n'apparaisse pas dans la suite $(x^{(n)})_{n\geqslant 1}$, en travaillant sur la suite « double » $(a_k^{(n)})$. À proprement parler, la *suite diagonale* serait la suite $c_k = a_k^{(k)}$, mais il n'y aucune raison pour que le nombre z dont le développement est donné par cette suite (c_k) ne soit pas dans la suite, on pourrait très bien avoir $z = x^{(1)}$, c'est-à-dire

$$a_k^{(1)} = c_k = a_k^{(k)} \text{ pour tout } k \geqslant 1.$$

Il va falloir « contrarier » la suite $x^{(n)}$: pour être sûr que y soit différent de $x^{(n)}$, il suffit de savoir que la n-ème décimale de y est différente de celle de $x^{(n)}$, à savoir $c_n = a_n^{(n)}$. On a beaucoup de place pour le faire : c_n n'est qu'un des dix éléments de $\{0, \dots, 9\}$, il en reste neuf qui sont différents de lui. Pour être sûr de fabriquer un développement propre, on ne prendra pas 9 comme décimale. Posons par exemple

$$b_k = x_k^{(k)} + 1 \text{ si } x_k^{(k)} \leqslant 7,\ \ b_k = 0 \text{ si } x_k^{(k)} = 8, 9.$$

Le nombre

$$y = \overline{0, b_1\, b_2 \dots b_k \dots}$$

ne peut pas faire partie de la suite donnée.

Reprenons la question en base 2. Par le biais des développements binaires, on peut identifier $\mathbb{R}$, pour ce qui concerne sa cardinalité ou *puissance*, à l'ensemble des suites $(x_k)_{k\in\mathbb{N}} \subset \{0,1\}^{\mathbb{N}}$ formées de 0 et de 1. Étant donnée une famille dénombrable $(x^{(n)})_{n\in\mathbb{N}} \subset \mathcal{P}(\{0,1\}^{\mathbb{N}})$ de telles suites, une famille d'éléments de $\{0,1\}^{\mathbb{N}}$, il s'agit de voir que cette famille ne peut contenir toutes les éléments de $\{0,1\}^{\mathbb{N}}$; en effet, considérons la suite $y \in \{0,1\}^{\mathbb{N}}$ définie par

$$y_k = 1 \text{ si } x^{(k)}(k) = 0,\ \ y_k = 0 \text{ si } x^{(k)}(k) = 1, \quad k \in \mathbb{N},$$

c'est-à-dire $y_k = 1 - x^{(k)}(k)$, où la définition à chaque place k « contredit » la valeur à la même place du k-ème élément de la famille $x^{(k)}$: cette suite y ne peut faire partie de la famille dénombrable de suites qui a été donnée, l'ensemble $\mathcal{P}(\{0,1\}^{\mathbb{N}})$ n'est pas dénombrable.

L'argument général de Cantor fonctionne ainsi, pour tout ensemble M. Les sous-ensembles $\mathrm{N} \subset \mathrm{M}$ sont en bijection avec les éléments de l'ensemble $\mathrm{P} = \{0,1\}^{\mathrm{M}}$ des fonctions g sur M qui ne prennent que les valeurs $0, 1$: poser $g_{\mathrm{N}}(x) = 1$ si $x \in \mathrm{N}$, et 0 sinon.

S'il existait une surjection ψ de M sur $\mathrm{P} \simeq \mathcal{P}(\mathrm{M})$, on pourrait poser

$$g_0(x) = 1 - \psi(x)(x) \in \{0,1\}, \quad x \in \mathrm{M}.$$

Cet élément $g_0 \in \mathrm{P}$ ne peut pas être dans l'image de ψ : si $g_0 = \psi(x_0)$, alors on devrait avoir $g_0(x_0) = \psi(x_0)(x_0)$ alors que la définition de g_0 donne $g_0(x_0) = 1 - \psi(x_0)(x_0)$. On

aurait $1 = 0$, ce qu'on espère ne jamais pouvoir démontrer en mathématiques ! En fait on affirme carrément : c'est impossible, le résultat est prouvé, par l'absurde.

Déplaçons légèrement le langage. Une fonction f de M dans $\{0, 1\}$ n'est rien d'autre qu'un sous-ensemble de M, si on identifie cette fonction f au sous-ensemble des $x \in \mathrm{M}$ tels que $f(x) = 1$. Ainsi, $\Psi(x)$ est maintenant considéré comme un sous-ensemble de M et

$$x \in \mathrm{G}_0 \Leftrightarrow x \notin \Psi(x), \quad x \in \mathrm{M}.$$

Autrement dit

$$\mathrm{G}_0 = \{x \in \mathrm{X} : x \notin \Psi(x)\}. \tag{2}$$

On va voir que G_0 ne peut pas être dans l'image de Ψ. Si $\mathrm{G}_0 = \varphi(y)$, on cherche à placer y : si y est élément de G_0, il doit en vérifier la définition, à savoir $y \notin \varphi(y) = \mathrm{G}_0$, impossible. Mais si $y \notin \mathrm{G}_0 = \varphi(y)$, il vérifie la définition de l'ensemble Y, donc $y \in \mathrm{Y}$, contradiction !

Ernst Zermelo [Zer1] nomme ce résultat *théorème de Cantor*. C'est aussi une preuve un peu étrange de l'inégalité $n < 2^n$.

2.2. *Continus*

L'ensemble $\mathbb{R}^2$ n'a pas « plus » d'éléments que $\mathbb{R}$. Il suffit de voir que le carré $[0, 1]^2$ n'a pas plus de points que le segment $[0, 1]$. Voici l'idée en gros (elle n'est pas tout à fait correcte) : à chaque nombre x de $[0, 1)$ associons sa suite de décimales

$$d_1, d_2, \ldots, d_n, \ldots$$

et à partir de cette suite formons deux nombres dont les décimales sont, pour le premier, formées par les décimales *d'indice impair* de la suite donnée,

$$d_1, d_3, \ldots, d_{2n+1}, \ldots$$

et pour le second

$$d_2, d_4, \ldots, d_{2n}, \ldots.$$

Il y a comme souvent un problème avec les développements impropres, mais on peut le régler. Un développement impropre a des décimales qui sont toutes égales à 9 à partir d'un certain rang, comme

$$z = 0,99999\ldots = \sum_{n \geqslant 1} 9.10^{-n}$$

que des débutants en mathématiques refusent volontiers d'égaler à 1. Pourtant ils voudront bien voir que

$$z/3 = 0,33333\ldots$$

et voudront bien admettre que ce dernier développement infini est égal à $1/3$. Mais alors, si $z/3 = 1/3, \ldots$?

Pour un nombre y tel que $0 < y < 1$, un développement impropre est de la forme

$$y = \sum_{i=1}^{n} b_i 10^{-i} + \sum_{i>n} 9.10^{-i},$$

où les b_i sont dans $\{0,1,\dots,9\}$, $n \geqslant 1$ et $b_i < 9$. Le nombre réel y est égal à

$$y = \sum_{i=1}^{n} b_i 10^{-i} + 10^{-n},$$

c'est un décimal. L'ensemble des décimaux est un ensemble dénombrable D, l'ensemble des suites de décimales des développements impropres et des développements finis est un autre ensemble infini dénombrable E. L'application de $\{0,\dots,9\}^{\mathbb{N}} \setminus \mathrm{E}$ dans $[0,1]$ définie par

$$(a_i)_{i\geqslant 0} \to \sum a_i 10^{i+1}$$

est une bijection de $\{0,\dots,9\}^{\mathbb{N}} \setminus \mathrm{E}$ sur $[0,1] \setminus \mathrm{D}$.

On peut aussi se convaincre qu'il n'y a pas plus de points dans le carré en définissant une injection du carré dans le segment. Si (x,y) est dans le carré, si

$$x \underset{(10)}{=} \overline{0, a_1\, a_2 \dots a_n \dots}, \qquad y \underset{(10)}{=} \overline{0, b_1\, b_2 \dots b_n \dots},$$

on lui associe

$$z \underset{(10)}{=} = \overline{0, a_1\, b_1\, 0\, a_2\, b_2\, 0 \dots a_n\, b_n\, 0 \dots},$$

où les 0 ajoutés servent à éviter les développements impropres, donc à garantir l'unicité du développement d'où l'injectivité. Comme il est évident qu'on peut injecter le segment dans le carré, le théorème de Cantor–Bernstein fournit une bijection.

Il est plus commode de commencer par mettre $[0,1]$ en bijection avec $\Delta = \{0,1\}^{\mathbb{N}}$ en utilisant le développement dyadique. Un développement dyadique est impropre si les « décimales » sont constantes, toutes égales à 1 à partir d'un certain rang, par exemple

$$1 = \sum_{k\geqslant 1} 2^{-k} \underset{(2)}{=} \overline{0, 1\, 1 \dots 1 \dots}.$$

L'ensemble D des développements impropres est dénombrable, ainsi que l'ensemble E des sommes de ces développements, qui sont les nombres dyadiques de la forme $k/2^n$, $0 \leqslant k \leqslant 2^n$. L'application

$$(a_n)_{n\geqslant 0} \in \Delta \;\mapsto\; \sum_{n\geqslant 0} a_n 2^{-n-1}$$

définit une bijection de $\Delta \setminus \mathrm{D}$ sur $[0,1] \setminus \mathrm{E}$. On complète la bijection de Δ sur $[0,1]$ par une bijection de D sur E.

Il en résulte que $[0,1]^2$ est en bijection avec Δ^2. Pour mettre en bijection $[0,1]^2$ et $[0,1]$, il suffit donc d'établir une bijection entre Δ^2 et Δ, ce qui est facile.

On note que l'ensemble Δ correspond exactement à l'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$, en identifiant la suite au sous-ensemble

$$\mathrm{M} = \{n \in \mathbb{N} : a_n = 1\}.$$

Il est clair que c'est une bijection. Le « continu » correspond exactement à l'ensemble Δ des suites de 0 et de 1, ou encore, à l'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$.

Peu après la première approche de Cantor, qui doit gérer le problème des développements impropres, on arrive à s'en débarrasser au moyen d'une astuce (due à Julius König selon [PuIl, *Genesis der Mengenlehre*, p. 49]) qu'on pourrait rapprocher de techniques de codage moderne. Ce principe est plus agréable à décrire en base 2. Tout nombre réel x de l'intervalle semi-ouvert $[0,1)$ peut être décrit de façon unique par un développement propre

$$x \underset{(2)}{=} \overline{0,\, a_1\, a_2\, \ldots\, a_n\, \ldots}$$

correspondant à l'égalité

$$x = \sum_{n \geqslant 1} a_n 2^{-n},$$

où $a_i = 0, 1$ et où le « chiffre » 0 apparaît une infinité de fois (c'est le fait que le développement soit *propre*). On est donc sûr que toute suite finie de 1 dans le développement binaire de x sera suivie à un moment donné par un 0. On peut par conséquent décomposer la suite

$$a_1\ a_2\ a_3\ \ldots\ a_n\ \ldots$$

de zéros et de uns en « pièces de base » prises dans la suite

$$p_0 = 0,\ \ p_1 = 10,\ \ p_2 = 110,\ \ p_3 = 1110,\ \ p_4 = 11110,\ \ \ldots$$

Ainsi, le début du développement binaire

$$\overline{0,\ 0\,1\,1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\ \ldots}$$

pourra être codé par l'expression

$$[p_0\, p_2\, p_0\, p_1\, p_4\, p_0\, p_0\, p_1\ \ldots].$$

Considérons un couple quelconque $(x, y) \in [0,1)^2$, représenté au moyen de suites de « pièces de base »

$$x = [u_1\, u_2\, u_3\, \ldots\, u_n\, \ldots], \quad y = [v_1\, v_2\, v_3\, \ldots\, v_n\, \ldots],$$

où les u_i, v_i désignent des pièces de base p_k, pour un certain $k \geqslant 0$. Si on associe à ce couple (x, y) l'élément z de $[0,1)$ obtenu en intercalant les pièces de x et de y, c'est-à-dire le nombre z qui est défini par

$$z = [u_1\, v_1\, u_2\, v_2\, u_3\, v_3 \ldots\, u_n\, v_n\, \ldots],$$

on définit une bijection de $[0,1)^2$ sur $[0,1)$. On aurait pu remarquer que la décomposition en pièces fournit en fait une bijection entre $[0,1)$ et l'ensemble $\mathbb{N}^{\mathbb{N}}$ des suites d'entiers $\geqslant 0$, et conclure en notation symbolique que

$$[0,1)^2 = [0,1) \times [0,1) \simeq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \simeq \mathbb{N}^{\mathbb{N}\times\mathbb{N}} \simeq \mathbb{N}^{\mathbb{N}} \simeq [0,1).$$

2.2.1. *Construction d'ensembles continus*

On a fini par bien voir que le continu correspond exactement à l'ensemble Δ des suites de 0 et de 1, ou encore, à l'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$; ainsi, chaque fois qu'on pourra associer à chaque suite $u \in \{0,1\}^{\mathbb{N}}$ un point x_u différent dans un espace métrique complet fixé (X, d), on sera sûr que la puissance de X sera au moins le continu.

Supposons que cet espace X non vide n'ait pas de point isolé, c'est-à-dire qu'aucune boule $\mathrm{B}(x,r)$ de rayon $r > 0$ dans X ne soit réduite au seul centre x. Avec $x_0 \in \mathrm{X}$, centre de $\mathrm{B}(x_0,1)$ on aura déjà, avec cette hypothèse, un autre point $x_1 \neq x_0$. Posons $r_\emptyset = d(x_0,x_1)/3 < 1/3$, $r_\emptyset > 0$; on est sûr que les boules fermées $\mathrm{B}_f(x_0,r_\emptyset)$ et $\mathrm{B}_f(x_1,r_\emptyset)$ sont contenues dans $\mathrm{B}(x_0,1)$, et elles sont disjointes : tous les points qu'on pourra trouver dans l'une des deux boules seront distincts des points de l'autre boule.

Posons $x_{i,0} = x_i$; dans $\mathrm{B}(x_{0,0},r_\emptyset)$ on trouve un point $x_{0,1} \neq x_{0,0}$ et dans $\mathrm{B}(x_{1,0},r_\emptyset)$ on trouve un point $x_{1,1} \neq x_{1,0}$; on pose $r_i = d(x_{i,0},x_{i,1})/3 > 0$, $r_i < r_\emptyset/3 < 1/9$, et on continue le travail dans les quatre boules fermées disjointes.

Faisons encore un pas : posons $x_{i,j,0} = x_{i,j}$, trouvons dans $\mathrm{B}(x_{i,j,0},r_i)$ un point $x_{i,j,1} \neq x_{i,j,0}$, posons $r_{i,j} = d(x_{i,j,0},x_{i,j,1})/3$, etc... Pour chaque suite infinie $u_0,u_1,\ldots$ donnée, les points $x_{\mathbf{u},n} = x_{u_0,u_1,\ldots,u_n}$ forment une suite de Cauchy de limite $x_{\mathbf{u}}$, et les limites $x_{\mathbf{u}}$ sont deux à deux distinctes. L'ensemble triadique de Cantor est de cette nature. Ces exemples sont pleins de trous !

À côté de son étude du continu, Cantor a développé la notion d'ordinal, qui l'a conduit à l'idée du premier ordinal qui n'est plus dénombrable (le plus petit majorant des ordinaux de la seconde classe). Vers 1884 lui vient l'idée de rapprocher ces deux études : ce serait tellement satisfaisant de savoir que ce premier ordinal non dénombrable (on l'appelle aujourd'hui $\aleph_1$, aleph-un) est en bijection avec le continu !

À l'inverse, un sous-ensemble fermé K dénombrable de $[0,1]$ a nécessairement des points isolés. L'ensemble $\mathrm{K}' \subset \mathrm{K}$ des points de K qui ne sont pas isolés est un nouveau fermé, strictement plus petit. On peut poursuivre la définition des ensembles dérivés par récurrence ordinale,

$$\mathrm{K}'' = (\mathrm{K}')', \quad \mathrm{K}''' = (\mathrm{K}'')', \quad \mathrm{K}^{(\omega)} = \bigcap \mathrm{K}^{(n)}, \quad \mathrm{K}^{(\omega+1)} = (\mathrm{K}^{(\omega)})', \quad \ldots.$$

Comme K est dénombrable, il y aura un premier ordinal tel que le dérivé $\mathrm{K}^{(\beta)}$ soit vide. Cela ne peut pas se produire pour un ordinal limite (par compacité). On a par conséquent $\beta = \alpha + 1$, et le dérivé K^{α} est un ensemble fini non vide.

Revenons au théorème d'unicité de Cantor : supposons pour simplifier que $\mathrm{K}^{(\alpha)}$ soit réduit à un point x_0 ; si on considère un intervalle ouvert I autour de x_0 et si on enlève à K tous les points de l'intervalle I, l'ensemble $\mathrm{K}_1 = \mathrm{K} \setminus \mathrm{I}$ a une complexité strictement inférieure à celle de K : si une série trigonométrique (T) converge vers 0 sauf aux points de K_1, on sait que la fonction F de Riemann est affine sur K_1. Comme cela est vrai pour tout intervalle autour de x_0, il en résulte que F est affine sur $\mathrm{K} \setminus \{x_0\}$, donc affine par Riemann à nouveau.

2.2.2. *Bijection et continuité*

Le fait découvert par Cantor que $[0,1]$ et $[0,1]^2$ peuvent être mis en bijection, qu'ils soient donc *équipotents*, est devenu une banalité, et ne présente plus aucun caractère de difficulté de nos jours. Mais avec la continuité, la situation est différente : on peut trouver une surjection continue de $[0,1]$ sur le carré $[0,1]^2$, par exemple la *courbe de Peano*, mais il n'existe pas de bijection continue : ce point est encore très facile ; si f était une bijection continue de $[0,1]$ sur $\mathrm{K} = [0,1]^2$, et g la bijection réciproque, on raisonnerait ainsi : les trois points $f(0)$, $f(1/2)$ et $f(1)$ du carré K sont distincts, puisque f est bijective. Enlever le point $f(1/2)$ du carré K n'empêche pas de trouver un chemin continu γ dans K, qui va de $f(0)$ à $f(1)$ sans passer par $f(1/2)$. Mais alors $g \circ \gamma$ est un chemin continu dans $[0,1]$, qui va de 0 à 1 sans passer par $1/2$: c'est impossible en vertu du théorème des valeurs intermédiaires.

Cantor a « senti » le cas général (entre $[0,1]^m$ et $[0,1]^n$) et a essayé de le montrer, mais il n'a pas réussi. Jacob Lüroth [Lüro] a obtenu un résultat partiel, dans les années 1880–1900 : la bijection continue est impossible si $1 \leqslant m \leqslant 3$ et $m < n$; en 1907, à l'âge de 63 ans, n'étant pas parvenu au cas général qu'il a longtemps cherché, il se décide à publier les détails de sa preuve, dans un article plutôt difficile. Il a fallu attendre Luitzen Brouwer [Brou] pour une preuve générale de *l'invariance de la dimension* en 1911. Brouwer [Bro2] publie en 1912 (mais la signature à la fin de l'article est de juin 1910, à Amsterdam) son fameux théorème de point fixe : toute application continue de $[0,1]^n$ dans ui-même possède un point fixe. Brouwer fait découler ce théorème, à la dernière ligne de l'article, de résultats sur les points fixes d'applications continues d'une n-sphère dans elle-même, fondés sur la notion de *degré topologique*.

2.3. *Logique classique*

Incidemment, le mathématicien Brouwer dont on a parlé à propos de topologie est à l'origine d'une autre logique, la *logique intuitionniste* qui en gros, refuse les constructions qui ne sont pas explicites, notamment le principe du tiers-exclu. Voici un exemple d'argument, tout à fait valable en logique classique, mais qui serait rejeté par Brouwer.

Théorème. *Toute suite de nombres réels admet une sous-suite monotone au sens large.*

Preuve. Soit $(x_n)_{n\geqslant 0} \subset \mathbb{R}$ une suite donnée, et supposons qu'on veuille d'abord trouver une sous-suite strictement croissante, en sélectionnant pas à pas des indices croissants $n_0 < n_1 < \ldots < n_k$ pour former la sous-suite voulue ; on sera « bloqué » dans la construction si on a choisi pour être dans la sous-suite un indice n_k tel que pour tout $n > n_k$ on ait

$$x_{n_k} \geqslant x_n, \quad \text{c'est-à-dire} \quad x_{n_k} = \max\{x_n : n \geqslant n_k\} ;$$

il sera alors impossible de trouver $n_{k+1} > n_k$ tel que $x_{n_{k+1}} > x_{n_k}$, donc impossible de poursuivre la construction d'une sous-suite strictement croissante. Disons dans ce cas (c'est le mauvais cas, dans notre optique actuelle de recherche de suite croissante) que n_k est un *point d'arrêt*.

De deux choses l'une : ou bien l'ensemble A des points d'arrêt est fini, ou bien il constitue une liste infinie $(a_j)_{j\geqslant 0}$ strictement croissante de points d'arrêt : dans ce second cas on voit que la sous-suite $(x_{a_j})_{j\geqslant 0}$ est décroissante au sens large, par définition des points d'arrêt : puisque a_j est un point d'arrêt, $a_{j+1} > a_j$ implique $x_{a_{j+1}} \leqslant x_{a_j}$. Dans le

cas contraire, il n'y a plus de points d'arrêt si on va assez loin : on peut construire une sous-suite strictement croissante, pourvu qu'on la commence assez loin. □

David Hilbert appréciait peu le point de vue de Brouwer : il estimait que les principes intuitionnistes de Brouwer amenaient à jeter par dessus bord un bon nombre des résultats qui font la richesse et la beauté des mathématiques. En 1928, Hilbert a contribué à évincer Brouwer du comité de rédaction de la célèbre revue allemande *Mathematische Annalen* ; il se dit que Hilbert craignait de voir grandir après sa mort l'influence du courant intuitionniste. De fait, la grande majorité des mathématiciens a continué à raisonner dans le cadre de la logique classique ; le point de vue intuitionniste n'a pas disparu, mais il ne s'est pas imposé.

Cependant, l'avènement de l'informatique et des aspects théoriques qui l'accompagnent ont sensiblement changé la donne. Si on pense, non plus en termes de « vérité », mais en termes de *résultat effectivement calculable*, par exemple calculable par une machine, on voit bien qu'on ne peut pas en général, sans information particulière sur la suite (x_n) de la preuve précédente, déterminer « par machine » si une valeur donnée m est un point d'arrêt : il faudrait vérifier l'infinité des valeurs $(x_n)_{n>m}$, ce qui n'est pas envisageable dans l'état actuel de la technique… C'est une première raison de réfuter la preuve précédente. L'autre est l'application qu'on a faite du principe du *tiers exclu* de la logique classique : entre une chose et son contraire, il faut bien que l'une des deux soit vraie. Mais on ne peut pas dire qu'entre une chose et son contraire, il faut bien que l'une des deux soit *vérifiable par une machine* : il est bien possible que ni l'une, ni l'autre ne soit calculable ; on pourra essayer de sentir la différence subtile entre les deux affirmations suivantes : d'abord la « calculabilité » de A, *j'ai un programme qui me fournit le résultat* A, puis celle de NON(NON A) : *j'ai un programme qui me prouve que je n'aurai pas de programme qui prouverait que* A *est fausse*.

Voici un autre exemple d'argument généralement admis chez les mathématiciens normaux, dans des raisonnements par dichotomie, par exemple dans une des preuves du théorème de Bolzano–Weierstrass. Considérons un arbre de racine r et où chaque nœud possède un nombre fini de descendants directs, et dont toutes les branches sont finies : un théorème dit alors que l'arbre est fini.

En effet, si l'arbre est infini, et puisque la racine r n'a qu'un nombre fini de « fils », l'un d'entre eux au moins, disons r_1, doit avoir une infinité de descendants : mais une machine ne pourrait pas trouver quel fils choisir. Raisonnant ainsi, on trouvera une branche infinie, contrairement à l'hypothèse.

Autre preuve par « premier qui » : une version simplifiée du théorème de recouvrement de Borel. Si une suite (I_j) d'intervalles ouverts recouvre $[0,1]$, il existe déjà un nombre fini qui recouvre $[0,1]$.

On pose $b_0 = 0$, et $k(1)$ est le premier indice j tel que $b_0 \in \mathrm{I}_j$; on désigne par b_1 l'extrémité droite de l'intervalle ouvert $\mathrm{I}_{k(1)} = (a_1, b_1)$ qui contient b_0 ; on a donc $b_0 < b_1$ et pour tout $j < k(1)$, b_0 est en dehors de I_j. Puis $k(2)$ est le premier $j > k(1)$ tel que $b_1 \in \mathrm{I}_j$, et on continue. On voit que pour tout entier $n \geqslant 0$ on a l'inclusion

$$[0, b_n] \subset \mathrm{I}_{k(1)} \cup \mathrm{I}_{k(2)} \cup \ldots \cup \mathrm{I}_{k(n+1)}.$$

La suite (b_n) est croissante. S'il existe un entier n tel que $b_n > 1$, on a obtenu le résultat annoncé. Sinon, la suite converge vers $\ell \leqslant 1$, $\ell \in [0,1]$. Il existe un premier j tel que $\ell \in \mathrm{I}_j$; mais alors I_j contient tous les points b_k tels que $k \geqslant k_0$. Il existe $n \geqslant k_0$ tel que $j < k(n)$, ce qui implique que b_n n'est pas dans I_j, contradiction.

2.4. *Le langage des ensembles*

Pour parler des ensembles, Cantor est vague, forcément vague… Il écrit dans les premières lignes d'un article [Ca4] qui développe les notions de cardinalité :

> « Unter einer "Menge" verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unsrer Anschauung oder unseres Denkens (welche die "Elemente" von M genannt werden) zu einem Ganzem. »

Tentative de traduction :
Par le mot « ensemble », nous entendons le rassemblement en un tout, que nous désignons par M*, de certains objets bien différenciés* m *(qu'on appellera les « éléments » de* M*), objets provenant de notre intuition ou de notre pensée.*

Après cette entrée en matière, Cantor définit la réunion de plusieurs ensembles qui n'ont pas d'élément commun, définit les *parties* d'un ensemble, c'est-à-dire les sous-ensembles. Il embraye immédiatement en présentant la *cardinalité* d'un ensemble M, qu'il introduit comme une chose « qui a une existence dans notre esprit en tant qu'image intellectuelle ou en tant que projection de l'ensemble donné ». Viennent les ensembles *équivalents* (qui peuvent être mis en bijection), les comparaisons de cardinaux, puis les opérations sur les cardinaux : addition, produit, exponentiation. Tous ces développements sont devenus le contenu usuel des manuels traitant de théorie naïve des ensembles.

Si les mathématiciens de 1880 sont acquis au principe de récurrence usuel, il n'en va pas de même avec un nouveau principe de raisonnement qui est promu par Cantor : la *récurrence transfinie*. On considère maintenant une propriété $\mathrm{P}(\alpha)$ dépendant d'un ordinal α quelconque ; pour qu'elle soit vraie *pour tout ordinal*, il suffit de savoir selon Cantor que : la propriété $\mathrm{P}(0)$ est vraie, et chaque fois qu'un ordinal β est donné et que $\mathrm{P}(\alpha)$ est vraie pour tous les ordinaux $\alpha < \beta$, alors $\mathrm{P}(\beta)$ est vraie aussi.

Ces conceptions très permissives des « ensembles » vont laisser des esprits vicieux profiter de leur liberté de langage mathématique pour parvenir à l'absurde : c'est l'arrivée des paradoxes. En nécessaire réaction, il ne sera bientôt plus possible d'autoriser qu'une phrase absolument quelconque puisse définir un *ensemble* : il faudra passer par les axiomes qui seront introduits peu après 1900.

Puisqu'elles conduisent à des absurdités, faut-il rejeter les notions introduites par Cantor ? Les ordinaux de Cantor, définis par une notion bien floue de *type d'ordre*, sont-ils des objets mathématiques légitimes ? Et qui permet donc à Cantor d'instituer ce nouveau type de récurrence, la récurrence tranfinie ? Peut-on vraiment admettre poursuivre un raisonnement sur une quantité peut-être non dénombrable de pas ?

Les réactions aux travaux de Cantor des mathématiciens français des années 1890 ont été diverses. Émile Borel et Henri Lebesgue ont mentionné les ordinaux de Cantor ; dans un de ses premiers travaux [Bore], Borel accepte un argument de cardinalité venu de Cantor, pour prouver une version du *théorème de recouvrement* dit de Borel–Lebesgue (il a alors 25 ans, il rédige sa « Thèse d'État ») ; il écrit une ligne qui montre qu'il connaît les ordinaux ; il envisage une famille de points d'un segment AB (segment qu'il appelle une « droite ») : « Je dis que nous atteindrons nécessairement l'extrémité B de la droite, car, si on ne l'atteignait pas, on définirait une série d'intervalles ayant pour extrémités

$$\mathrm{B}_{i_1},\ \mathrm{B}_{i_2},\ \ldots,\ \mathrm{B}_{i_\omega},\ \mathrm{B}_{i_{2\omega}},\ \ldots,\ \mathrm{B}_{i_{\omega^2}},\ \ldots,\ \mathrm{B}_{i_{\omega\omega}},\ \ldots,$$

les indices étant *tous* les nombres de la seconde classe de nombres (définis par M. Cantor). Mais ces indices sont aussi dans un certain ordre, les nombres naturels, en tout ou en

partie. C'est là une contradiction puisque la seconde classe de nombres constitue un ensemble de seconde puissance. »

Cependant Borel s'est écarté assez rapidement des conceptions de Cantor. Lebesgue a donné une preuve voisine du même théorème de recouvrement, par récurrence ordinale également, au moyen de la notion de *chaîne d'intervalles* : il s'agit d'une famille strictement croissante (x_α) de points de $[0,1]$, indexée par les ordinaux $\alpha \leqslant \alpha_0$ pour un certain α_0, et qui est telle que $x_0 = 0$ et $x_{\alpha_0} = 1$.

Étant donnée une famille d'ouverts $(\mathrm{U}_i)_{i\in\mathrm{I}}$ qui recouvre $[0,1]$, il s'agit de trouver une sous-famille finie qui suffit à couvrir $[0,1]$. Lebesgue construit par récurrence ordinale une chaîne (x_α) telle que pour tout α, le segment $[0, x_\alpha]$ puisse être couvert par une sous-famille finie des U_i. Si les (x_α) sont construits pour tout $\alpha < \beta$, il s'agit de trouver un x_β admissible pour continuer la chaîne ; l'ensemble $\mathrm{B} \subset [0,1]$ des $(x_\alpha)_{\alpha<\beta}$, qui est non vide et majoré par 1, admet une borne supérieure $y \in [0,1]$; par l'hypothèse de recouvrement, l'un des ouverts donnés, disons U_j, contient cette borne y ; il existe $\varepsilon > 0$ tel que $\mathrm{I} = (y-\varepsilon, y+\varepsilon) \subset \mathrm{U}_j$. Mais alors I contient aussi des points de B, sinon la borne ne serait pas la borne ! Si x_α est dans I, on pourra couvrir $[0, x_\alpha]$ par un nombre fini d'ouverts, par l'hypothèse de récurrence sur la chaîne, et avec le seul ouvert supplémentaire U_j on couvrira jusqu'à y : on peut poser $x_\beta = y$. Si $y = x_\beta = 1$, on a achevé la construction, la récurrence s'arrête avec $\alpha_0 = \beta$.

Il s'agit de voir qu'on arrivera jusqu'à $x_\beta = 1$; c'est là qu'on emprunte à Cantor : si cela ne se produisait jamais, on continuerait l'adjonction de nouveaux points jusqu'à une cardinalité plus grande que celle de $[0,1]$: c'est impossible, on atteint donc le point 1 avec la chaîne d'intervalles et le résultat est établi par récurrence ordinale.

On peut raffiner un peu le dernier argument : chaque fois qu'on passe de x_α à $x_{\alpha+1}$, on enferme un nouveau nombre rationnel dans l'intervalle non vide $(x_\alpha, x_{\alpha+1})$; d'après Cantor à nouveau, la famille de tous les ordinaux dénombrables n'est *pas dénombrable* ; il est impossible par conséquent que la récurrence se soit poursuivie jusqu'au *premier ordinal non dénombrable*. La *chaîne d'intervalles* arrive donc à 1 pour un ordinal α_0 dénombrable.

Quand on arrive à 1, le théorème de recouvrement de Borel–Lebesgue est démontré : par construction, on sait que le segment $[0,1] = [0, x_{\alpha_0}]$ peut être recouvert par une sous-famille finie d'ouverts.

3. L'axiomatique à ses débuts

3.1. *Le paradoxe de Russell et les débuts de la logique mathématique*

Cantor ne pouvait introduire la notion d'ensemble que par des considérations plutôt intuitives et naïves, qui ont bien vite conduit à des paradoxes. Bertrand Russell dans ses Principes [Russ] de 1903 propose un paradoxe qui fait penser à la preuve de Cantor qui a tourné autour de l'équation (2). Avec Alfred Whitehead, Russell construira un peu plus tard dans les *Principia Mathematica* [R-W] un système très lourd pour fonder les mathématiques : selon les mauvaises langues, il y faut 50 pages avant de pouvoir enfin démontrer que $1 + 1 = 2$!

Voici le fameux paradoxe : considérons l'ensemble E formé précisément de tous les ensembles F qui ne se contiennent pas comme élément, en symboles : $\mathrm{F} \notin \mathrm{F}$. Alors, si E

est élément de E, par la définition même de cet ensemble, on doit conclure que $E \notin E$, ce qui est contradictoire ; mais si E n'est pas élément de E, on a $E \in E$ par la définition de E à nouveau, ce qui est contradictoire aussi. Que faire ?

Il est bien probable que ce paradoxe n'ait pas été l'invention de Russell. Plusieurs témoignages laissent penser qu'il était connu de Zermelo avant la publication par Russell (voir [Ebbi, sec. 2.4.3, *The Zermelo-Russell Paradox*]). Je ne choisirai pas le témoignage le plus sérieux : le site allemand de Wikipedia attribue à Zermelo la plaisanterie suivante, formulée devant ses étudiants de l'Université de Göttingen, où Felix Klein jouait un rôle très important : « les mathématiciens de Göttingen se classent en deux catégories : ceux qui font ce qui plaît à Felix Klein, mais cela ne leur plaît pas ; et ceux qui font ce qui leur plaît, mais cela ne plaît pas à Klein. Dans quelle catégorie doit-on classer Felix Klein lui-même ? » Après un temps de suspens, la réponse de Zermelo : « Il faut en conclure que Felix Klein n'est pas un mathématicien ! » C'est bien la seule réponse possible au paradoxe de Russell : il faut élaborer un système où la famille formée par tous les ensembles *ne soit pas un ensemble*. En 1897, Burali-Forti publie un autre paradoxe, concernant cette fois « l'ensemble » des ordinaux de Cantor ; de nos jours, on dit clairement que la « classe des ordinaux n'est pas un ensemble » (Cantor n'a pas été trop troublé par le paradoxe de Burali-Forti : il était déjà au courant, comme l'indique une lettre qu'il écrit à Hilbert en 1897 [PuIl, p. 150 et documents 43, 44 p. 225–226]).

Si vous connaissez l'obsession de Wikipedia à propos des « sources », vous vous doutez qu'il doit y avoir une source pour la plaisanterie attribuée ci-dessus à Zermelo : ce serait le fameux physicien autrichien Wolfgang Pauli qui l'aurait rapportée, d'après un article de 1999 d'Engelbert Schücking ([Schü, p. 28] ; d'origine allemande, ce dernier a été professeur de Physique à la New York University à partir de 1967 ; Pauli était passé par Göttingen en 1921–22, l'université de Zermelo autour de 1900). Selon le même article, Pauli conclut ainsi son histoire : « Zermelo n'a pas été promu au grade de professeur à Göttingen ! » De fait, Zermelo enseignait à Göttingen, mais il n'avait pas un *vrai* poste : il avait depuis 1905 un *titre* de professeur, mais il était en réalité « Privatdozent » depuis 1902, recevant une bourse annuelle modeste ; les efforts des uns et des autres (Hilbert en particulier) pour qu'il obtienne une poste permanent à Göttingen échouèrent (voir [Ebbi, sec. 2.11]).

Même si elle tombe un peu « comme un cheveu dans la soupe », dans cet article de Schücking consacré principalement au rôle du physicien Pascual Jordan dans la physique du 20^{e} siècle, l'anectode est amusante ; elle sous-entend que Felix Klein était à cette époque le dictateur du département de mathématiques de Göttingen ; elle est aussi instructive par rapport au paradoxe de Russell, mais il faut peut-être nuancer un peu son caractère véridique : Zermelo quitte Göttingen pour Zürich vers 1910 ; Pauli a alors 10 ans ! Il rapporte donc une « légende de Göttingen », qu'il a entendue environ dix ans plus tard, et il la rappelle bien plus tard, au début des années 1950, lors un dîner avec Jordan et Schücking — élève de Jordan — dans un restaurant chic de Hamburg : *se non è vero, è molto ben trovato*.

Face à cette crise des paradoxes, on décide de s'occuper des *fondations* : il faut que tout l'édifice mathématique repose sur des bases clairement énoncées, des *axiomes*. Cette démarche n'est évidemment pas une invention de la fin du 19^{e} siècle : la géométrie antique, celle d'Euclide, entend tirer toutes les propriétés géométriques d'un certain nombre de *postulats*, un autre mot pour « axiome ». Giuseppe Peano est l'un de ceux

qui font un gros travail dans les années avant 1900 pour fonder les mathématiques sur des axiomes : on a certainement entendu parler de ses axiomes pour les entiers. Mais son texte *Arithmetices principia, nova methodo exposita*, écrit en latin en 1889, est difficile à lire. Il présente un des premiers exemples de tentative d'écriture suivant des principes de logique mathématique, d'axiomatisation des mathématiques (il faut aussi mentionner Dedekind [Dede] en 1888, en particulier art. 71 et Th. 126). Ce premier texte de Peano a été suivi de plusieurs autres sur des principes de logique mathématique, puis le *Formulaire de mathématiques*, en plusieurs volumes. Gottlob Frege est un nom important pour les débuts de la logique mathématique (né en 1848 à Wismar, Mecklembourg-Poméranie occidentale ; études à Iéna, passage à Göttingen, retour à Iéna ; il publie un court livre en 1879 ; signé à Jena, 1878) ; Frege tente d'établir les principes qui sont à la base du raisonnement mathématique lui-même, d'énoncer les règles de déduction. Il introduit les règles pour la quantification : il est le créateur du *calcul des prédicats*. Le titre du livre : *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*, Halle 1879.

Concernant la géométrie, Hilbert publie en 1899 un ouvrage où il présente une axiométisation de la géométrie plane et spatiale ([Hilb], dont une traduction française paraît dès 1900). Il semble plus que probable que cette préoccupation axiomatique de Hilbert va infléchir les centres d'intérêt de Zermelo. Zermelo est sans contexte l'un des personnages importants pour la théorie des ensembles. Il contribue à la clarification de l'axiome du choix, et il contribue à mettre en place le point de vue de la théorie des modèles. L'axiome du choix intervient naturellement dans la situation suivante : si f est une surjection de X sur Y, une façon naturelle d'obtenir une injection de Y dans X est de « choisir » dans chaque image inverse $f^{-1}(y)$, $y \in \mathrm{Y}$, non vide à cause de la surjectivité, un élément $g(y) \in f^{-1}(y) \subset \mathrm{X}$. C'est cette forme qui est retenue par Zermelo pour formuler l'axiome du choix en 1908 dans son article fondateur : si Z est un ensemble dont les éléments sont des ensembles A tous non vides, il existe un ensemble Z_1 dont l'intersection avec chaque élément A de Z est un singleton, $\mathrm{A} \cap \mathrm{Z} = \{a\}$: l'ensemble Z_1 « choisit » un élément a dans chaque $\mathrm{A} \in \mathrm{Z}$.

À mon humble avis d'amateur incompétent, Zermelo [Zer1] a effectué en 1908 une avancée considérable en direction de la notion de *modèle* qu'on développera plus bas. Zermelo envisage un *domaine* $\mathfrak{B}$, qui est une collection de « choses », « d'objets ». Le domaine représente l'univers des objets mathématiques. Entre deux de ces objets a, b du domaine $\mathfrak{B}$ peut exister une relation notée $a \varepsilon b$ par Zermelo, cette relation se lit : *a est élément de b*. Zermelo appelle « ensembles » les objets b du domaine tels qu'il existe un autre objet a du domaine qui satisfait la relation $a \varepsilon b$, à une unique exception près, un « ensemble vide » qui n'a pas d'élément. Zermelo énonce des axiomes qui sont étonnamment proches de ceux qui sont encore en vigueur ; il en résulte en particulier qu'il n'existe aucun objet b tel que tous les objets a de $\mathfrak{B}$ soient éléments de b.

3.2. *À Göttingen*

À l'initiative des autorités prussiennes (notamment celle du ministre des cultes Friedrich Althoff), Göttingen devient autour de 1900 un centre d'excellence : pour les mathématiques, ce serait même « le centre du monde mathématique » selon certains, et pour les autres sciences, un repaire de nombreux Prix Nobel (une vingtaine entre 1905 et 1930). Le recrutement de Felix Klein (1886, précédemment à Leipzig) est important ; ce dernier contribue avec Althoff au recrutement d'autres personnalités éminentes ; Hilbert (1895),

puis Hermann Minkowski ; Constantin Cararathéodory (d'origine grecque, mais né à Berlin en 1873 d'un père diplomate ; travaux en calcul des variations) y étudie à partir de 1902, docteur en 1904 sous la direction de Minkowski, divers postes ailleurs puis y est nommé de 1913 à 1918. Hermann Weyl, Emmy Noether ; Klein privilégie aussi les applications des mathématiques et la formation d'ingénieurs. En 1926/27 John von Neumann vient à Göttingen travailler avec Hilbert.

Hilbert, né en 1862, originaire de Königsberg (Kaliningrad depuis 1946, enclave russe au bord de la Baltique) où il a étudié, était professeur à Göttingen depuis 1895. Il y fait venir son ami Hermann Minkowski (qui meurt prématurément en 1909, un coup dur pour Hilbert). Parmi les nombreux domaines où Hilbert a eu une grande influence, il faut noter la logique mathématique, avec le *programme de Hilbert* (vers 1920), dont l'espoir était de justifier les fondements des mathématiques par une mécanique finie à partir d'un système fini d'axiomes dont on puisse prouver la non-contradiction.

Ernst Zermelo naît en 1871 à Berlin, fils d'un professeur de lycée. Études secondaires à Berlin, puis universitaires à Berlin, avec un semestre à Halle (où il suit un cours de Cantor, mais sur la théorie des nombres), un semestre à Freiburg im Breisgau ; il passe ensuite un doctorat à Berlin sur le calcul des variations, sous la direction de Hermann Amandus Schwarz (qui fut un ami de Cantor à l'époque de leurs études à Berlin), soutenu en 1894 ; intérêt en hydrodynamique (assistant de Max Planck), Habilitationsschrift (toujours en hydrodynamique) à Göttingen en 1899. Cette même année 1899, Hibert publie *Grundlagen der Geometrie* [Hilb], où il propose une série d'axiomes pour la géométrie, ramène leur non-contradiction à la non-contradiction de l'arithmétique, et prouve l'indépendance des axiomes proposés en fournissant des exemples de *géométries* où les axiomes, sauf un, sont satisfaits. Les preuves données pour l'indépendance démontrent un des caractères de la méthode axiomatique : Hilbert introduit des objets mathématiques dont certains ont peu à voir avec la géométrie d'Euclide, il réinterprète dans leur cas les notions de points et de droites, et prouve que l'objet « géométrique » ainsi défini satisfait les axiomes, sauf un axiome particulier : cet axiome particulier n'est donc pas conséquence des autres axiomes. Zermelo s'associe rapidement aux recherches de Hilbert sur les fondements.

Göttingen était le centre mondial des maths à l'époque. En 1900, dans un congrès international à Paris, Hilbert place le problème de l'hypothèse du continu en tête de sa fameuse liste des *23 problèmes de Hilbert*. En 1904, Zermelo publie son théorème sur le bon ordre. Sa santé n'est pas bonne : il souffre de tuberculose et doit se reposer sous un meilleur climat. Il obtient le titre de professeur en 1905 à Göttingen (mais sans poste permanent), puis un vrai poste à Zürich en 1910, il s'intéresse à la théorie des jeux. De santé fragile, il s'installe à Freiburg en 1926.

3.3. *Non contradiction et théorèmes de Gödel*

Dès les débuts de la méthode axiomatique, on se pose la question bien naturelle de la non-contradiction du système d'axiomes qu'on veut introduire, c'est-à-dire : va-t-on pouvoir déduire de ces axiomes que $0 \neq 0$? Zermelo indique en 1908 dans son article fondateur [Zer1] *qu'il n'a pas été en mesure* de démontrer la non-contradiction de son système d'axiomes, ce qui veut évidemment dire qu'il s'est posé la question.

La question sera posée avec force par Hilbert, qui propose autour des années 1920 un « programme » qui conduirait à réduire les déductions mathématiques à des considérations pour ainsi dire purement mécaniques. On pourrait alors espérer prouver

mécaniquement que l'affirmation $0 \neq 0$ n'est pas conséquence des axiomes d'une théorie donnée, l'arithmétique par exemple. Certains problèmes simples peuvent être résolus de cette manière : considérons le groupe G des isométries directes d'un solide antique que j'aime beaucoup, l'icosaèdre régulier $\mathfrak{I}$, solide convexe à vingt faces triangulaires et douze sommets ; ce groupe a 60 éléments (le groupe G est aussi, « par dualité », le groupe des isométries directes du dodécaèdre régulier, solide convexe à douze faces pentagonales et 20 sommets, qu'on obtient simplement comme solide dont les sommets sont les 20 barycentres des faces triangulaires de l'icosaèdre). Supposons choisi un ensemble S de *générateurs* pour le groupe G, c'est-à-dire un sous-ensemble S de G tel que tout élément du groupe puisse s'exprimer comme un produit d'éléments pris dans l'ensemble S ; évidemment, S = G conviendrait, mais on cherche S aussi petit que possible. Ici, deux générateurs g_0, g_1 suffisent, on peut prendre deux rotations d'un cinquième de tour autour de deux sommets voisins dans l'icosaèdre : si M est un sommet de $\mathfrak{I}$, le point opposé $-$M est un autre sommet, et la rotation d'un cinquième de tour autour de l'axe passant par M et $-$M laisse le solide invariant.

On cherche ensuite un ensemble E, aussi petit que possible également, formé de relations d'égalités vraies dans G, de la forme

$$h_1 h_2 \dots h_k = h'_1 h'_2 \dots h'_\ell$$

où tous les h_i, h'_j sont égaux à g_0 ou à g_1, qui soit suffisant pour simplifier (compte-tenu des règles de calcul dans un groupe) tout produit $h_0 \dots h_j$ de la forme précédente jusqu'à son expression « la plus petite », au sens de l'ordre de type lexicographique suivant,

$$\mathbf{1} < g_0 < g_1 < g_0 g_0 < g_0 g_1 < g_1 g_0 < g_1 g_1 < g_0 g_0 g_0 < g_0 g_0 g_1 < \dots$$

(où $\mathbf{1}$ désigne l'élément neutre de G, considéré comme étant le produit d'une suite *vide* de générateurs). Donnons un exemple de simplification : puisque g_0 et g_1 sont des cinquièmes de tour, les deux relations $g_0^5 = \mathbf{1}$ et $g_1^5 = \mathbf{1}$ sont satisfaites dans G ; chaque fois qu'une chaîne $A = h_1 \dots h_k$ de générateurs contient une sous-chaîne $B = g_0 g_0 g_0 g_0 g_0$, on peut simplifier l'expression A en y éliminant B, sans changer la valeur du produit dans G. Mais il est clair que ces deux relations ne suffisent pas à caractériser le groupe G : elles seraient vraies aussi pour $g_0 = (1, 0)$, $g_1 = (0, 1)$ dans le groupe $\mathbb{Z}/(5\mathbb{Z}) \times \mathbb{Z}/(5\mathbb{Z})$, qui n'est pas isomorphe à G (il n'a même pas le bon nombre d'éléments).

À partir des axiomes de groupe et des seules relations de l'ensemble E, on pourra alors décider si deux produits finis h et h' quelconques des générateurs g_0 et g_1 sont égaux ou pas. L'ensemble E joue le rôle d'un système d'axiomes, on pourrait dire ici que E fournit des *axiomes pour le groupe* ; et l'ordinateur peut résoudre ce petit problème de mécanique de groupe. Il donne par exemple un système E formé des quatre relations

$$g_1 g_0 g_1 = g_0 g_1 g_0,\ g_0 g_1 g_1 g_0 = g_1 g_1 g_1,\ g_1 g_0 g_0 g_1 = g_0 g_0 g_0,\ g_0 g_0 g_0 g_0 g_0 = \mathbf{1},$$

qui suffisent à caractériser le groupe G.

Mais il en va différemment si le monde à étudier est plus riche, en particulier s'il contient le monde des nombres entiers et de leur arithmétique. Kurt Gödel [Göde] va invalider le programme de Hilbert en 1931. Un système d'axiomes est *consistant* s'il ne permet pas de déduire *en même temps* un énoncé A et l'énoncé contraire NON A : c'est bien la moindre des choses à demander, sinon, dans le cas inconsistant, les axiomes

impliquent *n'importe quel énoncé* ! Gödel montre que dans tout système consistant contenant l'arithmétique, il y aura des énoncés A tels que ni A, ni NON A ne résulte des axiomes : l'énoncé A est *indécidable* dans le système d'axiomes considéré. C'est le premier théorème d'incomplétude ; le deuxième théorème d'incomplétude, qui l'accompagne, affirme — en gros — qu'on ne peut pas démontrer la non-contradiction d'un tel « monde logique », suffisamment riche, à l'intérieur de ce monde lui-même.

Pour donner une idée abusivement simpliste de la preuve, il faut commencer par rappeler *le paradoxe du menteur* : vous savez que Pseftis est un menteur pathologique ; il n'ouvre la bouche que pour proférer des mensonges. Alors, le jour où Pseftis déclare : « je suis un menteur », vous ne savez pas quoi penser... Dans une théorie logique T suffisamment riche, on pourra formaliser cette déclaration de Pseftis, et on ne pourra, ni en trouver une preuve, ni une preuve du contraire. Si la théorie possède les outils de l'arithmétique, on pourra avec Gödel coder par des entiers tous les énoncés de la logique, et faire des mots de Pseftis une affirmation arithmétique qu'on ne pourra ni démontrer, ni infirmer au sein de T.

Pour réaliser le programme, on commence par « arithmétiser » les énoncés de la théorie T en question, c'est-à-dire par coder chaque énoncé par un entier, ce qui au fond n'est pas bien surprenant. Le langage de la théorie contient les entiers eux-mêmes ; il contient par ailleurs les symboles logiques ET, OU, NON, les quantificateurs $\exists$ et $\forall$, les parenthèses ouvrante et fermante, tous codables par un nombre fini d'entiers ; on a aussi besoin de « variables libres » $x, y, \ldots$ qui sont aussi codées par des entiers (par exemple des nombres premiers, $x \to 11$, $y \to 13, \ldots$). Un énoncé $\mathrm{A}(x)$ à une variable libre est une suite finie de symboles qui se ramène à une suite finie de codes, que Gödel remplace par un code unique en utilisant la suite des nombres premiers,

$$(n_1, n_2, n_3, \ldots, n_k) \;\to\; 2^{n_1} 3^{n_2} 5^{n_3} \ldots p_k^{n_k}.$$

Mais il faut aussi, et c'est bien plus délicat, définir avec les seuls moyens de cette théorie T, pour chaque règle ρ de déduction (qui peut être une loi logique générale, ou bien l'application de l'un des axiomes de la théorie T), une fonction f_ρ sur les entiers telle que l'égalité $n = f_\rho(m)$ traduise le fait que l'énoncé ϕ_n codé par l'entier n est conséquence directe de l'énoncé ϕ_m par l'application de cette règle de déduction ρ. Gödel tient aussi à utiliser pour ce faire des fonctions f qui soient *calculables* dans un sens bien précis, les *fonctions récursives*.

De cette façon, Gödel peut définir une fonction $\mathrm{Dem}(n)$ qui vaut 1 exactement quand la formule ϕ_n résulte des axiomes de T. Supposons établie (toujours en se restreignant aux moyens du système) une liste (R_n) des énoncés $\mathrm{A}(x)$ à une variable libre x ; désignons de plus par $[\mathrm{R}_n : m]$ l'énoncé clos obtenu en remplaçant la variable libre x de R_n par la valeur entière m (un *énoncé clos* ne contient pas de variable libre : il est susceptible d'être vrai ou faux). L'ensemble « diagonal » d'entiers K défini par

$$\mathrm{K} := \{n : \mathrm{Dem}[\mathrm{R}_n : n] \neq 1\}$$

va servir à formaliser le paradoxe du menteur : on peut former un énoncé $\mathrm{S}(x)$ à une variable libre tel que

$$n \in \mathrm{K} \;\Leftrightarrow\; \mathrm{S}(n)\,;$$

l'énoncé $\mathrm{S}(x)$ fait partie de la liste (R_n) d'énoncés, il est donc égal à un certain R_q. Alors l'énoncé clos $\mathrm{S}(q)$ est indécidable : en effet, si $\mathrm{S}(q)$ est démontrable, alors $\mathrm{S}(q)$ est vraie et $q \in \mathrm{K}$, donc

$$\mathrm{Dem}[\mathrm{R}_q : q] \neq 1 \equiv \mathrm{Dem}[\mathrm{S}(x) : q] \neq 1 \equiv \mathrm{Dem}(\mathrm{S}(q)) \neq 1,$$

c'est-à-dire que $\mathrm{S}(q)$ n'est pas démontrable, contradiction ; d'un autre côté, si NON $\mathrm{S}(q)$ est démontrable, alors $q \notin \mathrm{K}$ et $\mathrm{Dem}(\mathrm{S}(q)) = 1$, ce qui veut dire que $\mathrm{S}(q)$ est démontrable aussi : on aurait démontré à la fois $\mathrm{S}(q)$ et son contraire, ce qui n'est pas possible si la théorie T est consistante.

Ainsi, l'hypothèse $\mathrm{Cons}(\mathrm{T})$ de la consistance de T entraîne que $\mathrm{Dem}(\mathrm{S}(q)) \neq 1$, sinon $\mathrm{Dem}(\mathrm{S}(q)) = 1$ entraînerait que $\mathrm{S}(q)$ soit vraie, donc $q \in \mathrm{K}$ et $\mathrm{Dem}(\mathrm{S}(q)) \neq 1$, ce qui est impossible par consistance. Mais on a dit que T n'entraîne pas $\mathrm{Dem}(\mathrm{S}(q)) \neq 1$, qui est indécidable : il en résulte que les axiomes de T ne peuvent pas impliquer $\mathrm{Cons}(\mathrm{T})$, la consistance de T ne peut pas être prouvée dans T. C'est une explication, par trop approximative, du *second théorème d'incomplétude* de Gödel.

Je suis tombé par hasard, dans une bibliothèque municipale du 93, sur le livre [$\mathrm{N}^2\mathrm{G}^2$] qui contient une traduction en français de l'article de Gödel, ainsi que des commentaires d'éminents logiciens qui peuvent aider à mieux le cerner. Les premières pages de l'article de Gödel sont plutôt lisibles et surtout très instructives, c'est leur contenu que j'ai essayé de restituer plus haut. Le pourquoi de la présence d'un tel livre, entre le rayon des mangas japonais et celui des livres de cuisine, restera pour moi une question indécidable...

4. *Les temps modernes*

On va maintenant quitter les considérations historiques pour entrer dans une étude un peu plus technique, de la théorie axiomatique des ensembles. On s'attachera à sa version la plus courante, la théorie de Zermelo–Fraenkel.

4.1. *Modèles de* Z *ou de* ZF

Le contenu scientifique de cette section a été servilement copié chez Jean-Louis Krivine, dans [Kri1] ou [Kri2]. N'étant pas logicien, il m'a fallu du temps pour saisir le point de vue de l'auteur. J'ai ajouté des mots qui j'espère, pourront aider le mathématicien ordinaire à parcourir plus rapidement le chemin que je n'ai su faire que lentement.

La forme modernisée du système d'axiomes pour la théorie des ensembles proposé par Zermelo est désignée de nos jours par Z, l'initiale de son nom. Mais ces axiomes, même sous leur forme modernisée, ont été reconnus insuffisants pour formaliser, par exemple, les mathématiques de Cantor. Le système de Zermelo a été notablement modifié, notamment à l'initiative d'Abraham Fraenkel, à partir de 1922, et on est arrivé au système moderne d'axiomes qu'on désigne par ZF pour Zermelo–Fraenkel. De très nombreux mathématiciens devraient aussi être mentionnés, notamment von Neumann, voir [Kan], [Kan2].

On peut voir un *modèle* de Z ou de ZF comme un graphe orienté, dont les sommets forment un ensemble $\mathcal{U}$ *non vide* qu'on appellera *univers*, et dont les arcs (a, b), pour $a, b \in \mathcal{U}$, seront représentés ici par la notation $a \sqsubseteq b$ (remarquer que ce n'est *pas* le signe usuel $\in$ d'appartenance) ; on pourrait figurer la situation en plaçant deux points a et b, puis une flèche de a vers b. L'idée est que les éléments $a \in \mathcal{U}$ vont « coder » les ensembles utilisés en mathématiques, et la relation $a \sqsubseteq b$ codera la notion d'appartenance de la

théorie « naïve » des ensembles, qui constitue le langage des mathématiques. De cette façon on pourra traduire, « formaliser » dans ce graphe les relations entre ensembles et les constructions d'ensembles. Je me garderai soigneusement, de peur de ne plus rien comprendre à ce que je raconte, d'appeler *ensembles* les éléments a, b de l'ensemble $\mathcal{U}$, je dirai toujours *objets de* $\mathcal{U}$, et je n'emploierai pas la notation d'appartenance ordinaire pour désigner les arcs du graphe, mais le symbole *ad hoc* $\sqsubseteq$; je dirai que a est un $\sqsubseteq$-élément de b lorsque $a \sqsubseteq b$, c'est-à-dire que (a, b) est un arc dont a est la *source* et b la *cible* ou extrémité.

Le graphe $(\mathcal{U}, \sqsubseteq)$ est supposé vérifier les *axiomes* de la théorie des ensembles qu'on va présenter plus loin. Ces axiomes imposent à l'ensemble $\mathcal{U}$ de contenir certains objets particuliers dotés de propriétés caractéristiques, tout comme la théorie des groupes impose qu'un groupe G contienne un élément neutre e pour la loi du groupe. Par exemple, il résulte des axiomes de la théorie Z de Zermelo que l'univers $\mathcal{U}$ doive contenir un objet distingué qu'on notera ici $\mathbf{0}$, qui correspond à l'ensemble vide des mathématiciens ; du point de vue du graphe, c'est un objet $a \in \mathcal{U}$ qui n'est l'extrémité d'aucun arc, il n'y a aucun $b \in \mathcal{U}$ tel que $b \sqsubseteq a$: en d'autres termes, $\mathbf{0}$ n'a aucun $\sqsubseteq$-élément. L'objet $\mathbf{0}$ est une *constante* de la théorie.

Le développement de la théorie va produire une famille distinguée de sous-ensembles de $\mathcal{U}$, qu'on appellera *collections* ; ce seront essentiellement les seuls sous-ensembles de $\mathcal{U}$ qui interviendront. On peut donner tout de suite deux premiers exemples : si $a \in \mathcal{U}$, le sous-ensemble

$$a_{\sqsubseteq} = \mathrm{C}(a) := \{b \in \mathcal{U} : b \sqsubseteq a\} \subset \mathcal{U}$$

est une collection, ainsi que le singleton $\{a\} \subset \mathcal{U}$. Par ailleurs, l'univers entier $\mathcal{U}$ est une collection. Les axiomes garantiront l'existence d'objets de $\mathcal{U}$ vérifiant certaines propriétés : il s'agira souvent de voir qu'étant donnée une certaine collection C, il existe (ou pas) un objet $a \in \mathcal{U}$ tel que $\mathrm{C} = \mathrm{C}(a)$.

La théorie axiomatique des ensembles ne parle pas comme les « gens normaux » ; tout y est « ensemble » : un entier est un ensemble, un nombre réel est un ensemble au même titre qu'une partie de $\mathbb{R}$, etc... Une fonction est un ensemble ! D'autre part, nous avons tous un jour dessiné une « patate » pour figurer un ensemble A, puis une plus grosse patate « contenant » la première pour figurer un autre ensemble B contenant A : le point de vue du graphe $(\mathcal{U}, \sqsubseteq)$ est un peu déroutant : les deux patates peuvent être deux collections $\mathrm{C}(a)$ et $\mathrm{C}(b)$, qui peuvent encore être contenue l'une dans l'autre, mais les « points » a et b eux-mêmes, objets de $\mathcal{U}$ qui « représentent » ces patates, sont « ailleurs » dans l'univers $\mathcal{U}$, aux bouts des flèches du graphe orienté... Les choses apparaissent en quelque sorte en deux versions : la « patate », collection $a_{\sqsubseteq} = \mathrm{C}(a)$ qui correspond à notre habitude de se représenter et de manipuler une famille d'objets, et l'objet $a \in \mathcal{U}$, qui est une espèce « d'étiquette ». Mais si on « change de niveau », en envisageant une collection $(\mathrm{C}(a_i))_{i\in \mathrm{I}}$ de parties de $\mathcal{U}$, c'est à la collection des étiquettes $(a_i)_{i\in \mathrm{I}}$ qu'on fera référence pour ne pas trop s'éloigner de la représentation par l'ensemble $\mathcal{U}$: cette nouvelle collection pourra (ou pas) être la collection $\mathrm{C}(b)$ d'un nouvel objet $b \in \mathcal{U}$,

$$\mathrm{C}(b) = \{a_i : i \in \mathrm{I}\} \subset \mathcal{U}.$$

En fait, les mathématiciens ordinaires se soucient en général assez peu de la « théorie axiomatique des ensembles », ils continuent, comme Cantor a commencé de le faire,

d'effectuer les opérations qui leur semblent raisonnables sur les collections d'objets qu'ils manipulent, comme « l'ensemble des nombres réels algébriques » ; ils ne leur viendrait pas à l'esprit de devoir demander la permission d'introduire cette notion. Tout au plus certains se sentent-ils à l'abri du parapluie de ZF, ou prétendent l'être : pour tenter une comparaison provocatrice et absurde, ils sont à l'abri comme ceux des Français qui se sentent sous la protection de « leur » force nucléaire stratégique, mais qu'ils n'utilisent jamais (jusqu'à présent) dans la vie courante...

4.2. *Énoncés*

Avant d'introduire les axiomes, il faut revenir sur la notion *d'énoncé* et sur ce qui s'y rattache. Les énoncés sont formés au moyen d'un petit nombre de signes, d'autant de lettres de variables $x, y, \ldots$ qu'on veut, d'autant de lettres $a, b, \ldots$ représentant des objets de $\mathcal{U}$ qu'on veut (les *paramètres*), et au moyen d'un (très) petit nombre de règles de formation :

• $x = y$, $x \sqsubseteq y$ sont des énoncés ; ces deux énoncés contiennent les *variables libres* x et y.

Si a est un objet de $\mathcal{U}$ (tel que l'objet « vide » $\mathbf{0}$, dont on a anticipé l'existence) et si b est un autre objet de $\mathcal{U}$, on peut évaluer la valeur *vrai* ou *faux* des énoncés précédents quand on y remplace x par a et y par b : l'énoncé $a = b$ est vrai si et seulement si a et b sont le même objet de $\mathcal{U}$, l'énoncé $a \sqsubseteq b$ est vrai si et seulement si le couple (a, b) est un arc du graphe orienté $(\mathcal{U}, \sqsubseteq)$. De plus, $x \sqsubseteq b$ devient un nouvel énoncé, à une seule variable libre x et à un *paramètre* b, ou bien, de manière analogue, l'énoncé $a \sqsubseteq y$ possède une variable libre y et un paramètre b ; un énoncé sans variable libre tel que $a \sqsubseteq b$ est appelé *énoncé clos* ; on a ainsi un premier aperçu du remplacement dans un énoncé $\mathrm{E}(x, y)$ d'une ou plusieurs variables libres par des objets de $\mathcal{U}$: par exemple $\mathrm{E}(a, y)$, $\mathrm{E}(x, b)$ ou l'énoncé clos $\mathrm{E}(a, b)$. Cela s'applique bien sûr aussi aux énoncés contenant moins ou plus de variables libres, tels que $\mathrm{E}(x)$, ou $\mathrm{E}(x, y, z)$, $\mathrm{E}(x, y, z, t), \ldots$

• Si $\mathrm{E}(x, y, z)$ est un énoncé comportant (ce n'est qu'un exemple) trois variables libres, alors $\mathrm{E}(x, x, z)$ est un énoncé, à deux variables libres : ainsi, $x \sqsubseteq x$, $x = x$ sont des énoncés.

• Si E, E_1 et E_2 sont des énoncés, alors « NON(E) », « (E_1) OU (E_2) » sont des énoncés ; on peut enlever un couple de parenthèses « (...) » correctement associées, quand le sens reste clair, non ambigu (c'est ce qu'on fait en général dans les langages de programmation).

Si E, E_1, et E_2 sont des énoncés clos, la valeur de vérité de l'énoncé NON(E) ou de l'énoncé (E_1) OU (E_2) est évaluée en suivant les règles usuelles de la logique.

• Si $\mathrm{E}(x)$ est un énoncé contenant la variable libre x, alors $\exists x\, \mathrm{E}(x)$ est un énoncé, dans lequel la variable x n'est plus libre, elle est devenue *variable liée* et l'énoncé $\exists x\, \mathrm{E}(x)$ est un énoncé clos. On pourrait aussi bien l'écrire $\exists y\, \mathrm{E}(y)$, $\exists z\, \mathrm{E}(z)\ldots$ (comme on fait dans une intégrale avec le « nom » de la variable d'intégration) à condition bien sûr que y ou z ne soit pas une autre variable libre de l'énoncé E, qu'on aurait oubliée en écrivant $\mathrm{E}(x)$ au lieu de $\mathrm{E}(x, y)$, $\mathrm{E}(x, y, z)$.

Un énoncé clos $\exists x\, \mathrm{E}(x)$ est *vrai dans* $\mathcal{U}$ si et seulement s'il existe $a \in \mathcal{U}$ tel que $\mathrm{E}(a)$ soit vrai dans $\mathcal{U}$.

Pour donner un exemple de l'application des règles précédentes, construisons les énoncés successifs

$$y \sqsubseteq x, \quad \exists y\, (y \sqsubseteq x), \quad \text{NON}\, \exists y\, (y \sqsubseteq x)\,;$$

l'énoncé $\mathrm{A}(x,y) := y \sqsubseteq x$ a deux *variables libres* x et y ; dans les énoncés

$$\exists y\,(y \sqsubseteq x), \quad \text{NON}\,\exists y\,(y \sqsubseteq x),$$

le quantificateur en y rend la variable y *liée* ; ces deux énoncés contiennent la seule variable libre x. Maintenant l'énoncé

$$\mathrm{E} := \exists x\ \text{NON}\,\exists y\,(y \sqsubseteq x)$$

n'a plus de variable libre, c'est un *énoncé clos*. Les axiomes Z de Zermelo impliquent que cet énoncé clos E doit être vrai dans $\mathcal{U}$; son interprétation est l'existence d'un objet $a \in \mathcal{U}$ qui n'a aucun $\sqsubseteq$-élément b. L'axiome d'extensionnalité qu'on verra plus loin implique que cet objet sans $\sqsubseteq$-élément est unique, c'est le représentant dans $\mathcal{U}$ de « l'ensemble vide », pour lequel on introduit un *symbole de constante* qui désigne cet objet de l'univers, en général $\emptyset$, pour nous ce sera $\mathbf{0}$ pour éviter toute confusion (on a déjà évoqué cet objet $\mathbf{0}$). On peut bâtir de nouveaux énoncés qui utilisent des constantes, par exemple

$$\text{NON}(x = \mathbf{0}),\ \ \exists x\ \text{NON}(x = \mathbf{0}).$$

Le premier est un énoncé à un paramètre et une variable libre x, le deuxième est un énoncé clos (à paramètre) qui est vrai en théorie des ensembles : il existe un ensemble non vide.

Certains des axiomes de la théorie sont assez abscons, leur lecture serait totalement insupportable sans quelques « macro-énoncés » qui les rendent plus concis, et qui peuvent ensuite être utilisés « en cascade ». On emploiera la notation M := E pour indiquer que le macro-énoncé M peut remplacer l'énoncé plus long E, où E peut déjà contenir d'autres macros déjà définies. À partir d'un macro-énoncé on pourrait, en éliminant pas à pas toutes les « macros », arriver à un énoncé n'utilisant strictement que les éléments primitifs du langage : $\sqsubseteq$, $=$, NON, OU, $\exists$, variables $x, y, \ldots$, constantes $a, b, \ldots \in \mathcal{U}$ et quelques parenthèses...

Dressons une liste de macro-énoncés de base, en commençant par le macro-énoncé logique « ET » qui sera défini (on pense en logique classique, où $\text{NON}(\text{NON}\ \mathrm{A}) \equiv \mathrm{A}$) par

$$\mathrm{A}\ \text{ET}\ \mathrm{B} := \text{NON}((\text{NON}\,\mathrm{A})\ \text{OU}\ (\text{NON}\,\mathrm{B})).$$

Cette macro s'appliquera à deux énoncés quelconques représentés ici par A et B. Pour obtenir un « véritable » énoncé qui n'emploie que les symboles de base du langage, il faudra *remplacer littéralement* les lettres A et B par leur « valeur énoncé », par exemple $\mathrm{A} := x \sqsubseteq y$ et $\mathrm{B} := \text{NON}(x = y)$, en les entourant de parenthèses si nécessaire. Les lettres 'A' et 'B' qui apparaissent ci-dessus sont en quelque sorte des « variables », mais elles ne sont pas de même nature que les « variables libres » $x, y, \ldots$ qui font *vraiment partie* du *langage* des énoncés. Pour ce qui concerne cette première « macro » ET, elles participent simplement à la facilitation de la description des énoncés ; on pourrait ne pas introduire ET : les énoncés seraient beaucoup plus longs mais surtout, ils deviendraient rapidement incompréhensibles. On dira (entre nous) que 'A', 'B' sont des *variables de macro* ou *macro-variables*. On aura plus loin des exemples où ces macro-variables ne seront pas seulement commodes, mais indispensables, tout au moins si on reste dans le système qu'on est en train de décrire. Continuons avec

$$\mathrm{A} \Rightarrow \mathrm{B} := (\text{NON}\,\mathrm{A})\ \text{OU}\ \mathrm{B}\,; \quad \mathrm{A} \Leftrightarrow \mathrm{B} := (\mathrm{A} \Rightarrow \mathrm{B})\ \text{ET}\ (\mathrm{B} \Rightarrow \mathrm{A}),$$

$$\forall x\, \mathrm{E}(x) := \mathrm{NON}(\exists x\ \mathrm{NON}\, \mathrm{E}(x)),$$

où on vient d'utiliser la macro-variable E, macro-variable d'énoncé à une variable libre x. Enfin, donnons un macro-énoncé à deux variables libres x, y pour « l'$\sqsubseteq$-inclusion »,

$$x \sqsubset y := \forall z\, (z \sqsubseteq x \Rightarrow z \sqsubseteq y).$$

Bien entendu, on ne se privera pas d'introduire les macro-énoncés $x \neq y := \mathrm{NON}(x = y)$ et $x \not\sqsubseteq y := \mathrm{NON}(x \sqsubseteq y)$, ou bien, quand les axiomes nous auront fourni la paire $\{a, b\}$, objet de $\mathcal{U}$ dont les deux seuls $\sqsubseteq$-éléments sont a et b, une macro $\langle x, y\rangle$ pour la *paire ordonnée* ou *couple*, habituellement définie par

$$\langle x, y\rangle := \{\{x\}, \{x, y\}\}.$$

4.3. *Axiomes de la théorie*

On a appelé *collection* un sous-ensemble de $\mathcal{U}$ défini à partir d'un énoncé $\mathrm{E}(x)$ à une variable libre par la définition naïvement ensembliste

$$(c) \qquad \mathrm{C}_{\mathrm{E}} = \{a \in \mathcal{U} : \mathrm{E}(a) \text{ est vrai dans } \mathcal{U}\}.$$

Par exemple, la collection associée à l'énoncé $x = x$ est $\mathcal{U}$ tout entier. À l'opposé, si a est un objet de $\mathcal{U}$, l'énoncé $\mathrm{E}_a(y) := (y \sqsubseteq a)$ introduit la « petite » collection $\mathrm{C}_{\mathrm{E}_a}$ des $\sqsubseteq$-éléments de a, qu'on a déjà notée $a_{\sqsubseteq} = \mathrm{C}(a) = \{b \in \mathcal{U} : b \sqsubseteq a\}$, et qu'on appellera à l'occasion une « collection élémentaire », puisqu'elle provient d'un objet a de $\mathcal{U}$.

La liste des axiomes de la théorie des ensembles est plutôt courte : Zermelo [Zer1] en 1908 propose une liste de 7 axiomes, qui inclut l'axiome du choix (ce n'est plus le cas pour la version moderne de Z) ; pour ZF, Krivine n'en compte que 5, le cinquième étant l'axiome de l'infini, dont on a absolument besoin si on veut représenter les « mathématiques de tout le monde ».

L'axiome du choix est laissé de côté dans ZF, il reste à part ; on parle de ZFC ou ZF+AC si on ajoute l'axiome du choix (en réalité, on a aussi besoin d'une forme minimale d'axiome du choix pour faire des mathématiques). Chaque axiome est un énoncé clos qui doit être vrai dans $\mathcal{U}$ pour que $\mathcal{U}$ puisse prétendre être un *modèle de la théorie des ensembles*. Sur cinq axiomes de ZF, quatre garantissent l'existence de certains objets de l'univers $\mathcal{U}$, *l'axiome d'extensionnalité* pour sa part donne une propriété caractéristique des objets de $\mathcal{U}$: il exprime le fait que tout objet a de $\mathcal{U}$ est complètement déterminé par la famille $\mathrm{C}(a)$ des $b \in \mathcal{U}$ tels que $b \sqsubseteq a$; pour tous $a_1, a_2 \in \mathcal{U}$, on a

$$\mathrm{C}(a_1) = \mathrm{C}(a_2) \Rightarrow a_1 = a_2.$$

Le véritable *énoncé* de l'axiome est le suivant :

$$\forall x \forall y\, ([\forall z(z \sqsubseteq x) \Leftrightarrow (z \sqsubseteq y)] \Rightarrow x = y).$$

On en tire un procédé pour la *définition* d'ensembles : si $\mathrm{E}(y)$ est un énoncé à une variable libre, si on pose

$$(f) \qquad \mathrm{F}(x) := \forall y(y \sqsubseteq x \Leftrightarrow \mathrm{E}(y))$$

et s'il existe un objet $a \in \mathcal{U}$ tel que $\mathrm{F}(a)$ soit vrai dans $\mathcal{U}$, alors cet objet a est unique, puisque la véracité de $\mathrm{F}(a)$ caractérise complètement la famille $\mathrm{C}(a)$ des $\sqsubseteq$-éléments b de a, à savoir $\mathrm{C}(a) = \mathrm{C_E}$, où $\mathrm{C_E}$ est définie en (c).

Mais il est tout à fait possible qu'une collection $\mathrm{C_E} \subset \mathcal{U}$, définie par un énoncé $\mathrm{E}(x)$, ne soit la famille $\mathrm{C}(a)$ d'aucun objet $a \in \mathcal{U}$; un exemple classique dans cette direction se rattache à la preuve qu'on a vue pour $2^n > n$, ou au *paradoxe de Russell* : soit l'énoncé

$$\mathrm{E_0}(x) := x \not\sqsubseteq x. \tag{1}$$

Cet énoncé ne peut définir un objet a de $\mathcal{U}$ par le procédé (f), à savoir ici

$$\forall y\,(y \sqsubseteq a \Leftrightarrow \mathrm{E_0}(y)). \tag{2}$$

En effet, on ne pourrait avoir ni $\mathrm{E_0}(a)$, ni $\text{NON}\,\mathrm{E_0}(a)$, ce qui est impossible en logique classique : par la définition (2) de a, l'affirmation de $\mathrm{E_0}(a)$ serait équivalente à $a \sqsubseteq a$, alors que la définition (1) de $\mathrm{E_0}(a)$ est $a \not\sqsubseteq a$! Zermelo utilise $\mathrm{E_0}$ pour montrer, à l'aide l'axiome de compréhension ci-dessous, que pour tout $a \in \mathcal{U}$, il existe $b \sqsubset a$ tel que $b \not\sqsubseteq a$, où

$$(y \sqsubseteq b) \Leftrightarrow (y \sqsubseteq a)\ \text{ET}\ \mathrm{E_0}(x).$$

En particulier, l'univers entier $\mathcal{U}$ ne peut pas être un $\mathrm{C}(a)$, sinon on aurait $b \sqsubseteq a$ pour tout $b \in \mathcal{U}$, en contradiction avec ce qui précède.

Le système Z des axiomes de la théorie des ensembles de Zermelo, introduit en 1908, modifié ou précisé depuis, contient *l'axiome de compréhension*. C'est l'axiome qu'on utilise tous les jours en mathématiques : étant donné un ensemble A et une propriété $\mathrm{P}(a)$ des objets a de A, on considère le sous-ensemble B de A formé de tous les $a \in \mathrm{A}$ tels que $\mathrm{P}(a)$ soit vraie. Dans la liste des axiomes de la théorie ZF, apparue dans les années 1920–30, l'axiome de compréhension est remplacé par un axiome plus fort, le schéma de remplacement (voir plus loin). Voici l'axiome de compréhension : pour tout énoncé $\mathrm{E}(x)$ à une variable libre, l'énoncé suivant est vrai dans $\mathcal{U}$:

$$\forall x\,\exists y\,(z \sqsubseteq y \Leftrightarrow ((z \sqsubseteq x)\ \text{ET}\ \mathrm{E}(z)).$$

L'axiome dit qu'étant donné $a \in \mathcal{U}$, il existe un objet $b \in \mathcal{U}$ dont les $\sqsubseteq$-éléments sont exactement les $\sqsubseteq$-éléments c de a tels que $\mathrm{E}(c)$ soit vrai dans $\mathcal{U}$,

$$\mathrm{C}(b) = \{c \in \mathrm{C}(a) : \mathrm{E}(c) \text{ est vrai}\} = \mathrm{C}(a) \cap \mathrm{C_E}.$$

Cet axiome est en fait une liste d'axiomes, correspondant à la liste (infinie) qu'on peut établir des énoncés $\mathrm{E}(x)$ à une variable libre. De ce fait, on dit plutôt qu'il s'agit du *schéma d'axiomes* de compréhension. On pourrait dire qu'il s'agit d'un « macro-axiome », dans la mesure où il contient une macro-variable E désignant un énoncé arbitraire à une variable libre, qu'il faudrait successivement remplacer littéralement par tous les énoncés strictement écrits avec les symboles de base, et obtenir ainsi une liste infinie d'axiomes.

C'est ici que la macro-variable d'énoncé E semble indispensable. Il existe une autre approche, qui n'est pas majoritairement retenue cependant dans la pratique actuelle. Un énoncé $\mathrm{E}(x)$ détermine une partie de l'univers $\mathcal{U}$, qu'on a appelée collection et qu'on appelle aussi *classe*. On pourrait décider d'ajouter au langage des *variables de classe* X, et de pouvoir « quantifier » sur ces classes ; il faudrait des axiomes concernant les classes,

pour ne pas en revenir au *n'importe quoi* d'avant 1900. Un tel système a été proposé par Gödel et Bernays : le système GB ne comporte qu'un nombre fini d'axiomes, il contient des axiomes qui portent sur les ensembles et sur les classes (voir [Cohe], Ch. II, § 6). On a pu prouver que les théorèmes obtenus dans ce système, mais qui ne mentionnent pas la notion de classe, peuvent aussi être démontrés dans ZF ([Cohe], même section, Theorem p. 77). Le schéma d'axiome de compréhension deviendrait dans GB l'axiome unique

$$\forall \mathrm{X} \forall x \exists y \forall z \, (z \sqsubseteq y \Leftrightarrow ((z \sqsubseteq x) \text{ ET } (z \in \mathrm{X}))),$$

où X est une *variable de classe*, qui remplace l'énoncé $\mathrm{E}(x)$. Comme on pense que X représente un sous-ensemble de $\mathcal{U}$, on a écrit $z \in \mathrm{X}$ avec le signe d'appartenance ordinaire. Les règles qu'on a imposées pour la formation des énoncés deviennent des axiomes concernant l'existence des classes. Par exemple, le fait que $x \sqsubseteq y$ soit un énoncé pourra se traduire par l'axiome suivant,

$$\exists \mathrm{X} \forall x \, (x \in \mathrm{X} \Leftrightarrow \exists y \exists z \, (x = \langle y, z \rangle \text{ ET } y \sqsubseteq z))$$

qui garantit l'existence d'une classe $\Gamma \subset \mathcal{U}$ formée de tous les couples $\langle a, b \rangle$ tels que $a \sqsubseteq b$.

Revenons au système Z et mentionnons une conséquence de l'axiome de compréhension : on a supposé $\mathcal{U}$ non vide ; en appliquant le schéma de compréhension à l'énoncé $\mathrm{E}(x) := x \neq x$, toujours faux dans $\mathcal{U}$, et à un objet a quelconque de $\mathcal{U}$, on déduit qu'il existe un objet $b \in \mathcal{U}$ dont les $\sqsubseteq$-éléments $c \sqsubseteq a$ sont ceux qui vérifient $\mathrm{E}(c)$: comme il n'y en a aucun, l'objet b est l'objet $\mathbf{0}$, la $\sqsubseteq$-traduction dont on a déjà parlé de « l'ensemble vide » ; mais on a maintenant la justification de son existence à partir des axiomes de Zermelo.

L'axiome de compréhension permet de définir l'intersection de deux objets a et b de $\mathcal{U}$, intersection qu'on peut voir comme l'objet $a \sqcap b \in \mathcal{U}$ construit *par compréhension* à partir de a et de l'énoncé $\mathrm{E}(y) := y \sqsubseteq b$; on a l'énoncé suivant, vrai dans $\mathcal{U}$:

$$\forall x \forall y \exists z \forall t \, (t \sqsubseteq z \Leftrightarrow (t \sqsubseteq x) \text{ ET } (t \sqsubseteq y)),$$

dont la traduction intuitive est $\mathrm{C}(a \sqcap b) = \mathrm{C}(a) \cap \mathrm{C}(b)$. On a ici un exemple de *relation fonctionnelle* (voir plus loin) à deux variables x, y, qu'on peut noter $z = x \sqcap y$. La définition de la *réunion* demande *l'axiome de la somme* dont nous zapperons l'énoncé strict : il dit que pour tout $a \in \mathcal{U}$, il existe $b \in \mathcal{U}$ dont les $\sqsubseteq$-éléments sont les $\sqsubseteq$-éléments des $\sqsubseteq$-éléments de a,

$$\mathrm{C}(b) = \bigcup_{c \in \mathrm{C}(a)} \mathrm{C}(c).$$

La réunion usuelle de a_1 et a_2 est obtenue en appliquant l'axiome à la paire $\dashv a_1, a_2 \vdash$, objet de $\mathcal{U}$ dont les seuls $\sqsubseteq$-éléments sont a_1 et a_2. L'existence de la paire est un axiome de Z, mais résulte des axiomes de ZF :

$$\forall x \forall y \exists z \forall t \, \big(t \sqsubseteq z \Leftrightarrow [(t = x) \text{ OU } (t = y)]\big).$$

À la base du *problème du continu* se trouve la formation de l'ensemble des parties d'un ensemble donné. Un axiome lui est consacré :

$$\forall x \exists y \forall z \, (z \sqsubseteq y \Leftrightarrow z \sqsubset x) \, ;$$

étant donné $a \in \mathcal{U}$, il existe $b \in \mathcal{U}$ tel que $\mathrm{C}(b)$ soit précisément formé de tous les $c \in \mathcal{U}$ tels que $c \sqsubset a$, c'est-à-dire tels que $\mathrm{C}(c) \subset \mathrm{C}(a)$. Par extensionnalité, l'objet $b \in \mathcal{U}$ associé à $a \in \mathcal{U}$ par cet axiome est unique, on peut le noter $b = \mathcal{P}(a)$, encore une *relation fonctionnelle*.

Si $b \in \mathcal{U}$ et $b \sqsubset \mathbf{0}$, on voit que $b = \mathbf{0}$: l'axiome de l'ensemble des parties fournit un objet $\mathcal{P}(\mathbf{0})$ de $\mathcal{U}$ qui n'a donc qu'un seul $\sqsubseteq$-élément, à savoir $\mathbf{0}$; on note $\{\mathbf{0}\} = \mathcal{P}(\mathbf{0})$. Ensuite, on voit que l'objet $\mathcal{P}(\{\mathbf{0}\}) \in \mathcal{U}$ ne possède que deux $\sqsubseteq$-éléments, $\mathbf{0}$ et $\{\mathbf{0}\}$, on note $\{\mathbf{0}, \{\mathbf{0}\}\} = \mathcal{P}(\{\mathbf{0}\})$. On peut continuer...

4.4. *Fraenkel*

On a utilisé plus tard en logique mathématique un système plus puissant que le système d'axiomes de Zermelo, le système ZF pour *Zermelo–Fraenkel*. Abraham Fraenkel est né en 1891 à Munich ; enfant, il apprend l'hébreu, jeune homme les mathématiques à Munich, Berlin, Breslau ; homme jeune il fait la guerre de 14–18, sur le front français mais du côté allemand évidemment. Dès 1919 il publie une première version du livre « Einleitung in die Mengenlehre », « Introduction à la théorie des ensembles » ; dans la préface de 1919 il mentionne ses camarades de guerre, non-mathématiciens :

« Das vorliegende Büchlein ist im Feld entstanden und aus dem Feld in Druck gegeben worden ; die Anregung zu ihm verdanke ich Unterhaltungen, in denen ich Kriegskameraden (Nichtmathematikern) gelegentlich öde Stunde durch Einführung in Gedankengänge der Mengenlehre verkürzen konnte. »

La troisième version [Fra2], en 1928, devient un gros livre de plus de 400 pages qui développe, au début, toute la théorie « naïve » des ensembles. Fraenkel publie son livre en employant son deuxième prénom, Adolf Fraenkel (c'est encore en tant qu'Adolf qu'il écrit sur la vie de Cantor en 1932 dans le volume [CaA] qui rassemble les œuvres de ce dernier). Entre-temps, il a publié un court article [Fra1] de huit pages (paru en 1922, signé du 10 juillet 1921) qui pointe certaines insuffisances du système d'axiomes de Zermelo, et proposé un axiome plus fort que la compréhension, destiné à réparer ces faiblesses, *l'axiome de remplacement* (Ersetzungsaxiom). Je n'ai pas trouvé la version de 1919 du livre, mais j'ai vu proposée la version de 1928 à 59,25 euros chez Amazon.fr ; le même jour je l'ai téléchargée gratuitement sur un site officiel d'une société savante allemande ! J'en donne l'adresse,

https ://gdz.sub.uni-goettingen.de/id/PPN373206852

En plus de ce livre, on peut trouver à cette adresse une grande quantité d'articles anciens, en particulier pour ce qui nous concerne, ceux de Cantor et de Zermelo.

On trouve donc dans [Fra1] un axiome plus fort que le schéma de compréhension : il ne s'agit plus seulement de définir les sous-ensembles qui vérifient une certaine propriété, mais de pouvoir définir un nouvel ensemble b comme « image » d'un ensemble quelconque a par une « relation fonctionnelle » F, $b = \mathrm{F}(a)$. C'est le *schéma de remplacement*.

Dans le cas plus simple de relation fonctionnelle d'une seule variable, un énoncé $\mathrm{R}(x, y)$ est une *relation fonctionnelle* quand pour tout x, il ne peut pas y avoir deux valeurs différentes $y = y_1$ et $y = y_2$ telles que $\mathrm{R}(x, y)$ soit vraie (mais il peut n'y en avoir aucune). Le fait que la relation soit fonctionnelle ou pas n'est pas purement syntactique, il dépend des axiomes de la théorie. Par exemple, la relation

$$\mathrm{R}(x, y) := \forall t((t \in x) \Leftrightarrow (t \in y))$$

est une relation fonctionnelle par l'axiome d'extensionnalité : c'est la relation d'égalité $y = x$.

Si $\mathrm{R}(x, y)$ est un énoncé à deux variables libres, on peut écrire un macro-énoncé clos (mais contenant la macro-variable R) qui signifie que R est une relation fonctionnelle,

$$\mathrm{rf}(\mathrm{R}) := \forall x \forall y \forall y' ((\mathrm{R}(x, y) \text{ ET } \mathrm{R}(x, y')) \Rightarrow y = y').$$

Cet énoncé ne prescrit pas qu'étant donné un $a \in \mathcal{U}$ quelconque, il existe au moins un $b \in \mathcal{U}$ pour lequel on ait $\mathrm{R}(a, b)$. La collection des a qui ont une « image » b est définie par l'énoncé

$$\mathrm{dom}(\mathrm{R})(x) := \exists y \mathrm{R}(x, y).$$

On peut considérer R comme le graphe d'une fonction $\mathrm{F_R}$ définie sur une partie de $\mathcal{U}$ (une collection) et à valeurs dans $\mathcal{U}$: elle est définie sur la collection $\mathrm{C}_{\mathrm{dom(R)}} \subset \mathcal{U}$ associée à l'énoncé dom(R) ; on peut écrire de façon plus parlante $y = \mathrm{F_R}(x)$ au lieu de $\mathrm{R}(x, y)$. On voit qu'une relation fonctionnelle revient tout simplement à une fonction F définie sur une partie de $\mathcal{U}$, mais pas n'importe quelle fonction : elle doit être définie par un *énoncé*, au sens précis qui a été donné.

Pour donner un exemple de domaine, revenons à l'axiome de l'ensemble des parties, en considérant la relation

$$\mathrm{R}(x, y) := \forall z (z \sqsubseteq y \Leftrightarrow z \sqsubset x).$$

Par extensionnalité, il s'agit d'une relation fonctionnelle $y = \mathcal{P}(x)$, qui est définie sur l'univers $\mathcal{U}$ tout entier par l'axiome de l'ensemble des parties.

Les relations fonctionnelles sont à la base du schéma de remplacement, qui distingue le système ZF du système Z. À nouveau, cet axiome est en fait une liste d'axiomes, correspondant à la liste (infinie) qu'on peut établir de toutes les relations fonctionnelles $y = \mathrm{F_R}(x)$: pour chaque relation fonctionnelle R et pour chaque objet $a \in \mathcal{U}$, il existe un objet $b \in \mathcal{U}$ qui est « l'image » de a par $\mathrm{F_R}$, au sens que la famille des d tels que $d \sqsubseteq b$ est formée des $d = \mathrm{F_R}(c)$ pour c variant dans la famille des $\sqsubseteq$-éléments de a,

$$\mathrm{C}(b) = \{\mathrm{F_R}(c) : c \in \mathrm{C}(a)\} = \mathrm{F_R}(\mathrm{C}(a)),$$

avec la notation usuelle pour les images d'ensembles. Le remplacement est encore un « macro-axiome », où il faut remplacer le symbole $\mathrm{F_R}$, qui renvoie à une relation fonctionnelle arbitraire R, par son énoncé. Donnons-en un énoncé un peu édulcoré (l'énoncé complet contient une quantité arbitraire de variables susceptibles d'être remplacées par des paramètres pris dans $\mathcal{U}$) :

$$\mathrm{rf}(\mathrm{R}) \Rightarrow \forall t \exists u \forall z ((z \sqsubseteq u) \Leftrightarrow \exists w ((w \sqsubseteq t) \text{ ET } (z = \mathrm{F}(w)))).$$

4.5. *Modèles, derrière le rideau*

On peut imaginer une espèce de jeu vidéo : le joueur veut (on ne demandera pas pourquoi) jouer à faire des mathématiques, « axiomatiquement justifiées », par l'intermédiaire d'un logiciel qui a été programmé par des spécialistes « derrière le rideau », des « mathémagiciens » (j'ai appris ce jeu de mot d'un collègue américain, Steven Bellenot de la FSU ;

le mot « mathemagician » était apparemment déjà connu en 1933). Les sources du programme ne sont pas connues, il faut simplement que le logiciel soit capable de fournir tous les ensembles qui sont permis par les axiomes de la théorie, les axiomes de ZF, et en respectant ces axiomes.

Voici un exemple des magouilles qui peuvent avoir lieu derrière ce fameux rideau. C'est le théorème de Löwenheim–Skolem ; j'essaie d'en donner une idée simpliste : l'utilisateur du logiciel ne peut avoir qu'une quantité dénombrable de requêtes à formuler : en effet, chacune d'elles est une suite finie de signes d'un alphabet fini, ou au pire dénombrable. Il suffit d'avoir dans le « modèle » les objets correspondant à ces requêtes : à partir d'un modèle $\mathcal{U}$, on pourra déterminer une suite d'objets $(a_n) \subset \mathcal{U}$ qui permettront de répondre aux requêtes ; il faut bien voir que les choix successifs de $a_0, \ldots, a_n$ introduisent la possibilité de formuler de nouvelles requêtes où les a_j déjà choisis peuvent être paramètres, mais tout cela peut entrer dans une liste. De cette façon, à partir d'un modèle déjà existant, on pourra bricoler un modèle M dénombrable pour ZF ; on pourra même faire en sorte que M « soit un ensemble » dans $\mathcal{U}$, c'est à dire qu'il existe $m \in \mathcal{U}$ tel que $\mathrm{M} = \mathrm{C}(m)$.

Et on avait dit que $\mathbb{R}$ n'est pas dénombrable ! Y a un truc. C'est le *paradoxe de Skolem* : devant le rideau, vous venez de démontrer, à l'aide du logiciel qui peut formaliser la preuve de Cantor, que $\mathbb{R}$ est non-dénombrable, pourtant le modèle $\mathcal{U}$ derrière le rideau, bien plus gros que la seule collection $\mathrm{C}(\mathbb{R})$ des $\sqsubseteq$-éléments de l'ensemble $\mathbb{R}$, est dénombrable ! La raison est la suivante : pour l'opérateur, le modèle est dénombrable parce qu'il a à sa disposition une bijection de $\mathcal{U}$ avec les entiers, une bijection *qu'il vous cache*. Plus précisément : le modèle doit contenir un représentant de l'ensemble $\mathbb{N}$ des entiers, et il peut y avoir un sous-ensemble $\mathrm{X} \subset \mathcal{U}$ qui soit le graphe d'une bijection f entre cet ensemble $\mathbb{N}$ et l'univers $\mathcal{U}$; mais le sous-ensemble X ne provient pas d'un objet $a \in \mathcal{U}$, il n'est pas de la forme $\mathrm{X} = \mathrm{C}(a)$. Par ailleurs, l'ensemble X ne peut pas non plus être une collection telle qu'on les a définies, sinon cette collection-graphe définirait une relation fonctionnelle F et l'axiome de remplacement devrait faire de l'univers $\mathcal{U}$ tout entier, image de $\mathbb{N}$ par F, un sous-ensemble de $\mathcal{U}$ de la forme $\mathrm{C}(b)$, ce qui est impossible comme on a vu.

En bref, un modéle n'est certainement pas une représentation des « mathématiques réelles », *whatever that means*, mais en tout cas une *image pour ce qu'on peut démontrer*. Si le modèle est dénombrable, on conçoit que certaines propriétés ou notions difficilement concevables, telles que l'axiome du choix ou la notion d'ultrafiltre, soient manipulées derrière le rideau où elles deviennent bien simples, mais apparaissent ahurissantes devant, comme dans un tour de magie.

Le mathémagicien ne peut rien contre vous tant que vous lui posez des questions telles que « est-ce que 143 est un nombre premier ? » Mais les ennuis peuvent commencer si vous entamez une question par « soit n un entier ». Le magicien après avoir préparé derrière le rideau va sortir un entier de son chapeau, vous ne verrez pas qu'il s'agit peut-être en fait d'un objet d'une complexité inouïe, comme un entier non standard, une classe d'équivalence d'entiers modulo une relation définie par un ultrafiltre, en tout cas un objet bien différent de ce que vous pouvez imaginer. Mais vous n'y verrez que du feu : toutes les propriétés et axiomes que vous connaissez seront respectées.

4.6. *Consistance, indépendance*

Les logiciens savent nous convaincre que la théorie des ensembles, sous la forme d'un système d'axiomes ou d'un autre, Z, ZF, ZF+AC, est non-contradictoire si et seulement

si on peut fournir un modèle $\mathcal{U}$ pour ce système d'axiomes. Par ailleurs, les théorèmes *d'incomplétude* de Gödel indiquent qu'on ne peut pas prouver que ZF (ou la plupart des systèmes suffisamment riches) est non-contradictoire à partir des propres axiomes de ZF. L'existence d'un modèle est donc un acte de foi, fondé sur l'expérience : depuis le temps qu'on fait des maths, si on pouvait prouver que $0 \neq 0$, on le saurait !

Cela étant, on peut se poser la question suivante : en supposant qu'il existe un modèle pour ZF, peut-on ajouter un axiome supplémentaire $\mathcal{A}$ et trouver un nouveau modèle qui satisfasse aussi cet axiome supplémentaire ? Dans l'affirmative, on dit qu'on a obtenu la *consistance relative* de ce nouvel axiome $\mathcal{A}$. On a ainsi montré que si ZF admet un modèle, on peut construire des modèles qui satisfont en plus l'axiome du choix AC. On pourra trouver dans [Kri2] un grand nombre de tels résultats de consistance relative.

À partir des années 1925, la notion d'ordinal, revisitée par von Neumann, va jouer un rôle important dans la construction de modèles. Pour von Neumann, les ordinaux sont des ensembles particuliers : les ordinaux commencent avec

$$\mathbf{0},\ \ \{\mathbf{0}\},\ \ \{\mathbf{0},\{\mathbf{0}\}\},$$

L'ordinal suivant contient le précédent, et plus précisément

$$\alpha + 1 := \alpha \sqcup \{\alpha\},$$

les $\sqsubseteq$-élément de $\alpha + 1$ sont α et les $\sqsubseteq$-éléments de α. Il est possible de dire quand un objet b de $\mathcal{U}$ est un ordinal : d'une part, la relation $\sqsubseteq$ est un bon ordre sur b, c'est-à-dire que pour tout $c \sqsubset b$, $c \neq \mathbf{0}$, il existe $d_0 \sqsubseteq c$ qui est « le plus petit » $\sqsubseteq$-élément de c (si $d_1 \sqsubseteq c$, alors $d_1 = d_0$ ou $d_0 \sqsubseteq d_1$) ; d'autre part, $d \sqsubseteq b$ entraîne $d \sqsubset b$.

Avec l'axiome de remplacement et les ordinaux, von Neumann introduit la très puissante méthode de définition par induction sur la collection des ordinaux. L'axiome de fondation n'a pas grand sens pour les mathématiciens, mais il permet à l'opérateur d'opérer : cet axiome suppose que l'univers $\mathcal{U}$ est obtenu à partir de l'objet vide $\mathbf{0}$, en itérant de façon ordinale la prise de l'ensemble des parties, $\mathrm{V}_{\alpha+1} = \mathcal{P}(\mathrm{V}_\alpha)$ ou plus généralement

$$\mathrm{C}(\mathrm{V}_\beta) = \mathrm{V}_{\beta\sqsubseteq} = \bigcup_{\alpha<\beta} \mathrm{V}_{\alpha\sqsubseteq}.$$

Ainsi tous les objets de $\mathcal{U}$ sont classés dans une hiérarchie. Si on veut bricoler le modèle $\mathcal{U}$, on aura la possibilité de le faire « pas à pas », en commençant avec $\mathbf{0}$ et en montant dans la collection des ordinaux.

Gödel a montré que l'hypothèse du continu CH est « relativement consistante » : si on a un modèle de ZF, on peut fabriquer un modèle de ZF qui vérifie en plus CH.

Un axiome $\mathcal{A}$ est *indépendant* de ZF si on peut aussi bien supposer qu'il soit vrai ou qu'il soit faux, sans casser la machine si elle marchait avant. C'est ce que Paul Cohen a montré pour l'hypothèse du continu CH, complétant le travail de Gödel en construisant des modèles de ZF où CH est fausse : il y a dedans des tas d'ensembles dont la cardinalité est entre le dénombrable et le continu. La méthode de Cohen s'appelle le *forcing* ; il est totalement hors de question que je vous en donne une idée, pour la simple raison que je suis assez loin de l'avoir vraiment comprise.

Références bibliographiques

[Bore] Émile Borel, Sur quelques points de la théorie des fonctions, Ann. Sci. École Norm. Sup. (3), 12, p. 9–55 (1895).

[Brou] Luitzen E. J. Brouwer, Beweis der Invarianz der Dimensionenzahl. Math. Annalen **70**, 161–165 (1911).

[Bro2] Luitzen E. J. Brouwer, Über Abbildung von Mannigfaltigkeiten, Math. Annalen **71**, 97–115 (1912).

[CaT] Georg Cantor, Ueber einen die trigonometrische Reihen betreffenden Lehrsatz, Journal für die reine und angew. Math. **72**, 130–138 (1870).

[CaE] G. Cantor, Beweis, dass eine für jeden reellen Werth von x durch eine trigonometrische Reihe gegebene Function $f(x)$ sich nur auf eine einzige Weise in dieser Form darstellen lässt, Journal für die reine und angew. Math. **72**, 139–142 (1870).

[Ca1] G. Cantor, Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen, Journal für die reine und angewandte Mathematik **77**, 258–262 (1874).

[Ca1*] G. Cantor, Sur une propriété du système de tous les nombres algébriques réels, Acta Mathematica **2**, 305–310 (1883).

[Ca2] G. Cantor, Ein Beitrag zur Mannigfaltigkeitslehre. Journal f. reine und angew. Math. **84**, 242–258 (1878).

[CaF] G. Cantor, Fondements d'une théorie générale des ensembles, Acta Math. **2**, 381–408 (1883).

[CaP] G. Cantor, De la puissance des ensembles parfaits de points, Acta Math. **4**, 381–392 (1884).

[Ca3] G. Cantor, Ueber eine elementare Frage der Mannigfaltigkeitslehre, Jahresbericht der Deutschen Mathematiker-Vereinigung, 1, 75–78 (1891).

[Ca4] G. Cantor, Beiträge zur Begründung der transfiniten Mengenlehre, Math. Annalen **46**, 481–512 (1895).

[CaA] Georg Cantor, Gesammelte Abhandlungen mathematischen und philosophischen Inhalts, éd. par Ernst Zermelo, 1932.

[CaB] Georg Cantor Briefe, Herausgegeben von Herbert Meschkowski und Winfried Nilson, Springer-Verlag, Berlin-Heidelberg, 1991.

[Clar] Jules Claretie, Histoire de la révolution de 1870–71, nouvelle édition, 1877.

[Coh1] Paul J. Cohen, The independence of the continuum hypothesis. Proc. Nat. Acad. Sci. U.S.A. **50**, 1143–1148 (1963).

[Coh2] Paul J. Cohen, The independence of the continuum hypothesis. II. Proc. Nat. Acad. Sci. U.S.A. **51**, 105–110 (1964).

[Cohe] Paul J. Cohen, Set Theory and the Continuum Hypothesis, Benjamin, 1966.

[C–L] René Cori et Daniel Lascar, Cours de logique mathématique, Masson, 1993.

[Dede] Richard Dedekind, Was sind und was sollen die Zahlen ? Vieweg : Braunschweig 1888 ; repris dans les Œuvres de Dedekind, 335–391 (1932).

[Ebbi] Heinz-Dieter Ebbinghaus, in cooperation with Volker Peckhaus, Ernst Zermelo. An Approach to His Life and Work. Second Edition. Springer, 2015.

[Fra1] Abraham Fraenkel, Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre, Mathematische Annalen **86**, 230–237 (1922).

[Fra2] Abraham Fraenkel, Einleitung in die Mengenlehre, Grundlehren der mathematischen Wissenschaften IX, Springer, Berlin (1928).

[Göde] Kurt Gödel, Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatshefte für Mathematik und Physik **38**, 173–198 (1931).

[Hawk] Thomas Hawkins, Lebesgues Theory of Integration ; its Origins and Development, Madison (Wis.) : The University of Wisconsin Press, 1970 ; reprint New York : Chelsea Publ. Co, 1975.

[HeiT] Eduard Heine, Ueber trigonometrische Reihen, J. reine angew. Math. **71**, 353–365 (1870).

[Hein] E. Heine, Die Elemente der Functionenlehre, Journal für die reine und angewandte Mathematik **74**, 172–188 (1872).

[Hilb] David Hilbert, Grundlagen der Geometrie, B.G. Teubner : Leipzig, 1899.
Les principes fondamentaux de la géométrie, Gauthier-Villars : Paris, 1900 (traduction par Léonce Laugel).

[Kan] Akihiro Kanamori, The Mathematical Development of Set Theory from Cantor to Cohen, The Bulletin of Symbolic Logic **2**, 1–71 (1996).

[Kan2] Akihiro Kanamori, Set Theory from Cantor to Cohen, Philosophy of mathematics, 395–459, Handb. Philos. Sci., 4, Elsevier/North-Holland, Amsterdam, 2009.

[Kan3] Akihiro Kanamori, In praise of replacement. Bull. Symbolic Logic **18**, 46–90 (2012).

[Kri1] Jean-Louis Krivine, Théorie axiomatique des ensembles, Presses Universitaires de France, 1972.

[Kri2] Jean-Louis Krivine, Théorie des ensembles, Cassini, 1998.

[Lind] Ferdinand Lindemann, Über die Zahl π, Math. Annalen **20**, 213–225 (1882).

[Lio1] Joseph Liouville, Compte Rendu des Séances de l'Académie des Sciences, vol. 18, séance du 13 mai 1844.

[Lio2] Joseph Liouville, Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques, J. Math. Pures Appl., 1re série, **16**, 133–142 (1851).

[Lüro] Jacob Lüroth, Über Abbildung von Mannigfaltigkeiten, Math. Annalen **63**, 222–238 (1907).

[Mer] Charles Méray, Nouveau précis d'analyse infinitésimale. Paris 1872.

[N^2G^2] Ernest Nagel, James R. Newman, Kurt Gödel, Jean-Yves Girard, Le théorème de Gödel. Collection Sources du Savoir, 1989 ; réédition : Collection Points Sciences, S122, 1997. Éditions du Seuil.

[PuIl] Walter Purkert et Hans Joachim Ilgauds, Georg Cantor : 1845–1918, Vita Mathematica 1, Birkhäuser Verlag, 1987.

[Russ] Bertrand Russell, The Principles of Mathematics, Cambridge 1903.

[R-W] Bertrand Russell et Alfred N. Whitehead, Principia Mathematica, Cambridge 1910, 1912, 1913.

[Schü] Engelbert Schücking, Jordan, Pauli, Politics, Brecht, and a Variable Gravitational Constant, Physics Today **52**, 26–31 (1999).

[Zer1] Ernst Zermelo, Untersuchungen über die Grundlagen der Mengenlehre. I. Math. Annalen **65**, 261–281 (1908).

[Zer2] Ernst Zermelo, Über Grenzzahlen und Mengenbereiche, Neue Untersuchungen über die Grundlagen der Mengenlehre. Fundamenta Math. **16**, 29–47 (1930).