Chapitre 1 : Les nombres

Ce chapitre est une divagation autour des ensembles de nombres. Ce sera l'occasion de discuter de leur construction formelle et de s'intéresser à la notion de cardinalité. Bien que certains points seront utiles pour la suite du cours, ce chapitre doit surtout être considéré pour la culture mathématique. Nous ne prétendons pas ici être complet sur les sujets abordés ni avoir toute la rigueur exigible.

1 Une rapide histoire des nombres

L'idée de nombre s'est construite avec les civilisations et l'écriture, c'est-à-dire très récemment à l'échelle de l'histoire de l'humanité.

- $\mathbb{N}^*$ et $\mathbb{Q}_+^*$: les entiers naturels et les fractions positives sont utilisés depuis le début des temps historiques (premiers écrits). Toutes les cultures du monde ont des noms pour les premiers nombres entiers et des façons de les représenter. Les écritures des nombres ont été très diverses et plus ou moins pratiques. Il faut noter qu'il existe encore des peuples de chasseurs-cueilleurs qui n'ont pas de mot (et donc de représentation mentale) pour les nombres au-dessus de quelques unités (les Pirahãs comptent « un, deux, beaucoup »). Les grands nombres et le calcul sont donc des affaires de civilisations.

- $(\mathbb{R} \setminus \mathbb{Q})_+$: on sait que $\sqrt{2}$ est irrationnel depuis les pythagoriciens (vers 500 avant J.C). Les grecs de l'Antiquité avaient la vision des nombres comme des longueurs et donc se plaçant sur une ligne droite. Dans ce sens, on peut dire qu'ils voyaient les nombres positifs comme un continuum et donc incluaient les irrationnels.

- $\mathbb{Z}^*$ et $\mathbb{Q}_-^*$: les nombres négatifs sont utilisés en Chine et en Inde deux siècles avant notre ère. Cela consiste à noter avec des couleurs différentes les dettes et de connaître les règles d'opération sur les signes. Ils ne seront utilisés que bien plus tard chez les arabes et en occident.

- L'écriture décimale et le chiffre zéro apparaissent en Inde vers le Vème siècle avant d'être adoptés par la civilisation arabe. D'ailleurs, ceux que nous appelons « chiffres arabes » étaient qualifiés d'« indiens » par al-Khwārizmī (IXème siècle, Perse). Ce dernier rédige un manuel d'utilisation de l'écriture décimale qui sera traduit et participera à l'essor de cette écriture en occident pendant la renaissance. Ceci explique que « chiffre » se dit « algarismo » en portugais (une autre partie de l'œuvre d'al-Khwārizmī fera que son nom donnera aussi le mot « algorithme » et le titre d'un de ces livres notre mot « algèbre »).

- 0 : le nombre zéro n'apparaît que vers 500 en Inde. Il ne faut pas le confondre avec le chiffre zéro qui ne sert qu'à indiquer une position vide dans une écriture positionnelle (parfois un espace blanc ou un dessin ont joué le même rôle que le chiffre zéro).

- $\mathbb{C}$: pendant la renaissance italienne, Tartaglia, Cardan et Ferrari développent la résolution des équations de degré 3 et 4. Leurs formules peuvent conduire à des calculs du type $\sqrt{-1} - \sqrt{-1}$. A priori, cela n'a pas de sens, mais si on admet $\sqrt{-1}$ comme un nombre « imaginaire », alors le calcul donne 0 et on obtient la solution qu'on sait exister. Il s'agit donc au début d'une astuce pour faire aboutir une méthode de calcul mais pas de nombres en tant que tels. C'est Raphaël Bombelli (1526-1572, Italie) puis Leonhard Euler (1707-1783, Suisse) qui feront de ces nombres de vrais nombres, bien que « complexes ».

2 Un aperçu de la construction des nombres

2.1 Entiers et fractions

Lors de la refondation des mathématiques, les mathématiciens ont cherché à recréer toutes les théories en partant du minimum de bagages : quelques axiomes fondant la théorie des ensembles. Comment créer les nombres entiers avec le moins de choses possibles ? Une façon très simple est due à John von Neumann (1903-1957, Hongrie et USA), un des pères de l'informatique. Il suffit de poser 0 comme l'ensemble vide $\emptyset$, puis 1 comme le singleton $\{0\} = \{\emptyset\}$, 2 est l'ensemble $\{0,1\} = \{\emptyset,\{\emptyset\}\}$ etc. On construit donc par récurrence l'entier n comme l'ensemble contenant tous les nombres précédents. Cela fournit naturellement l'opération « $+1$ ». Il faut ensuite expliquer comment retrouver les opérations standards. Par exemple, l'addition $n+2$ est définie par $(n+1)+1$ et ainsi de suite : l'addition générale $n+m$ est définie comme étant $(n+(m-1))+1$. Retrouver toutes les propriétés des entiers naturels devient juste un jeu de patience et de rigueur. Coder les nombres négatifs est simple puisqu'il suffit de rajouter un *bit* devant le nombre entier.

Une fraction est juste un couple d'entiers. Mais si on définit $\mathbb{Q}$ comme $\mathbb{Z} \times \mathbb{N}^*$, on a deux couples différents (1,2) et (2,4) alors qu'il s'agit de la même fraction 1/2. Donc on va définir $\mathbb{Q}$ comme étant $\mathbb{Z} \times \mathbb{N}^*$ quotienté par la relation d'équivalence $(p,q) \equiv (p',q')$ si $pq' = p'q$. Notez bien que le test d'égalité reste dans les entiers puisqu'on ne sait pas ce qu'est une fraction (c'est tout le sel du jeu). On peut alors définir la somme de deux fractions par $(p,q) + (p',q') = (pq' + p'q, qq')$ et continuer avec la multiplication, l'inverse etc.

2.2 L'écriture décimale

L'écriture décimale est une écriture positionnelle en base 10. Un nombre décimal est un nombre que l'on peut écrire exactement avec un nombre fini de chiffres.

Définition 1.1

Un nombre **décimal** est un nombre rationnel du type $p/10^k$ avec p et k dans $\mathbb{Z}$.

Proposition 1.2

Le nombre r est décimal si et seulement s'il existe un couple $n > m$ dans $\mathbb{Z}$ et une suite de chiffres $a_n, \ldots a_m \in \{0,1,2,\ldots,9\}$ telle qu'on peut l'écrire sous la forme

$$a_n a_{n-1} \ldots a_1 a_0 \, , a_{-1} \ldots a_m := \sum_{i=n}^{m} a_i 10^i$$

avec $a_n \neq 0$ et $a_m \neq 0$. Par ailleurs, si elle existe, cette écriture est unique.

On voit que des fractions comme $1/3$ ou $1/7$ ne sont pas des décimaux. On peut alors imaginer les coder et même créer tous les nombres réels en poursuivant l'écriture décimale avec un nombre infini de chiffres après la virgule. On a bien alors

$$0{,}333333\ldots \;=\; \sum_{k=1}^{+\infty} 3.10^{-k} \;=\; 3\frac{10^{-1}}{1-10^{-1}} \;=\; \frac{3}{9} \;=\; \frac{1}{3}\;.$$

Formellement, on est en train de construire les réels comme limite des décimaux. C'est certainement la façon dont on les envisage dans la vie courante. Mais on rencontre un problème :

$$0{,}99999\ldots \;=\; \sum_{k=1}^{+\infty} 9.10^{-k} \;=\; 9\frac{10^{-1}}{1-10^{-1}} \;=\; 1$$

ce qui veut dire qu'il existe deux écritures pour le même nombre 1. On introduit donc la définition suivante.

Définition 1.3

Un développement décimal infini $a_n a_{n-1} \ldots a_1 a_0{,}a_{-1} a_{-2} \ldots$ est dit **impropre** s'il existe i_0 tel que $a_i = 9$ pour tout $i \leq i_0$.

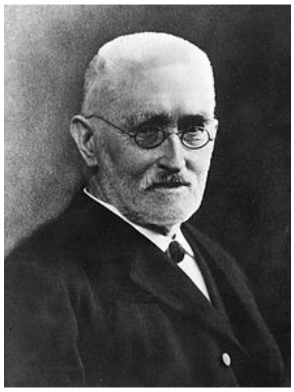
Pour ne plus avoir de doublon dans la représentation décimale des réels, on n'autorise que les développements décimaux propres. Si on a réglé le principal problème, il reste encore définir les règles d'addition et multiplication sur ces nombres décimaux pour retrouver les structures des réels. Or ceci est très pénible, en particulier à cause des écritures impropres : $0{,}444\ldots + 0{,}555\ldots$ n'est pas égal à $0{,}999\ldots$! C'est pour cela qu'une construction par les nombres décimaux n'est pas jugée pratique. Par ailleurs, elle dépend fortement de la base choisie, ce que n'aiment pas trop les mathématiciens : un nombre existe indépendamment de la base dans laquelle on l'écrit.

2.3 Autres constructions des réels

Imaginons que nous avons construits les nombres rationnels. Nous voulons représenter tous les nombres réels et les opérations liées d'une façon qui n'utilise que des nombres rationnels. Cela permettra de s'assurer que les réels ne sont pas une invention absurde qui pourrait aboutir à une contradiction logique, mais bien une structure découlant des axiomes de base des mathématiques. Il a été proposé plusieurs approches pour ce faire, dont les deux principales sont les suivantes. Il faut évidemment avoir en tête que ces constructions ont été faites a posteriori, alors que les nombres réels étaient utilisés depuis longtemps.

Les coupures de Dedekind
L'idée de Dedekind est de représenter un nombre par une coupure (A,B) de $\mathbb{Q}$, i.e. deux ensembles complémentaires non vides A et B tels que pour tout $a \in A$ et $b \in B$, $a \leq b$. Il faut vraiment voir la coupure comme un trait coupant $\mathbb{Q}$ en deux parties : A à gauche et B à droite. Ces coupures peuvent déjà représenter les rationnels en posant qu'un rationnel $q \in \mathbb{Q}$ est représenté par

$$A_q = \{r \in \mathbb{Q},\, r < q\} \text{ et } B_q = \{r \in \mathbb{Q},\, q \leq r\} \ .$$



Richard Dedekind
1831-1916
Allemagne

On a le choix de mettre q dans A ou B. Il faut une convention et c'est celle que l'ensemble A ne doit pas avoir de plus grand élément. On a donc $q = \min B_q$ pour les rationnels. Mais on peut aussi regarder la coupure

$$A = \{r \in \mathbb{Q},\, r^2 < 2 \text{ ou } r \leq 0\} \text{ et } B = \{r \in \mathbb{Q},\, 2 < r^2 \text{ et } 0 \leq r\}$$

qui est une coupure admise, entièrement décrite par des rationnels, mais qui n'est pas de la forme (A_q,B_q) avec $q \in \mathbb{Q}$ puisque B n'a pas de minimum dans $\mathbb{Q}$. C'est donc un nouveau nombre, qui va correspondre à $\sqrt{2}$. Pour vraiment construire la théorie, il faut retrouver toutes les propriétés de $\mathbb{R}$, bien définir ce qu'est la somme de deux coupures, leur produit etc. Par exemple, $(A,B) \leq (A',B')$ peut être défini par $A \subset A'$. De même, on peut définir l'addition de coupures par $(A,B) + (A',B') = (A+A',B+B')$. On montre ainsi qu'on obtient une bonne représentation de ce qu'on appelle « nombre réel ».

Les suites de Cauchy
Louis Augustin Cauchy a eu lui l'idée d'introduire une notion de suite qui assurerait la convergence sans pour autant introduire la limite elle-même. Une suite $(u_n) \subset \mathbb{Q}$ est dite « de Cauchy » si

$$\forall \varepsilon \in \mathbb{Q}_+^* \ , \ \exists n_0 \in \mathbb{N} \ , \ \forall n,m \geq n_0 \ , \ |u_n - u_m| \leq \varepsilon \ .$$

Notons que cette définition n'utilise que des nombres rationnels (la définition plus standard des suites numériques de Cauchy sera rappelée dans le chapitre suivant). Une suite convergente dans $\mathbb{Q}$ est de Cauchy mais certaines suites sont de Cauchy sans converger dans $\mathbb{Q}$ car leur potentielle limite n'y est pas. On définit alors les réels comme toutes les limites possibles de suite de Cauchy de rationnels. Comme plusieurs suites donnent la même limite, on quotiente l'ensemble des suites de Cauchy par l'équivalence $(u_n) \equiv (v_n)$ si et seulement si $|u_n - v_n| \to 0$. L'ensemble des classes d'équivalence des suites de Cauchy de rationnels est $\mathbb{R}$ suivant cette construction. La définition de l'addition et de la multiplication est simple car il suffit d'additionner et multiplier les suites (en vérifiant que c'est compatible avec les classes d'équivalence). Le procédé a aussi l'avantage d'être utilisable dans beaucoup d'autres situations mathématiques où il faut « compléter » un espace où certaines suites de Cauchy ne convergent pas. En contrepartie, certaines propriétés de $\mathbb{R}$ sont plus difficiles à obtenir selon cette construction.

Louis Augustin Cauchy
1789-1857
France

3 Cardinalité

Le cardinal $|A|$ d'un ensemble A correspond à la taille de cet ensemble. On pourrait se limiter à distinguer simplement les ensembles de taille finie et ceux de taille infinie. Mais en fait, il existe plusieurs degré d'infini. On formalise cela avec les définitions suivantes. Dans toute la suite, si $a \leq b$ sont deux entiers, on note

$$[\![a,b]\!] := \{ n \in \mathbb{Z} , a \leq n \leq b \} .$$

Définition 1.4 Cardinal d'un ensemble

Soient A et B deux ensembles. On dit que A et B sont **équipotents** ou **ont même cardinal** s'il existe une bijection entre A et B. On note alors $|A| = |B|$.

On dit que A est de cardinal plus petit que B s'il existe une injection de A dans B et on note alors $|A| \leq |B|$.

On dit que A est de cardinal **fini** s'il existe $n \in \mathbb{N}$ tel que $|A| = |[\![1,n]\!]|$, c'est-à-dire s'il existe une bijection entre A et $\{1,2,\ldots,n\}$. On note plus simplement $|A| = n$ et on dit que le cardinal de A est n. Si A n'est pas de cardinal fini, on dit qu'il est **infini**.

Si A est de cardinal fini ou si $|A| = |\mathbb{N}|$ on dit que A est **dénombrable**. Sinon A est dit **indénombrable**.

Un ensemble dénombrable est un ensemble A dont on peut lister les éléments un par un sous la forme $A = \{a_0,a_1,a_2,\ldots\}$. Ce n'est qu'au XIXème siècle que l'on a compris qu'il existe des ensembles indénombrables, c'est-à-dire de taille encore plus grande que $\mathbb{N}$. On verra ci-dessous que c'est le cas de $\mathbb{R}$. On peut construire toute une théorie de la cardinalité. Un des théorèmes importants est le suivant, que nous admettrons ici.

Théorème 1.5 Cantor-Schröder-Bernstein

Soient A et B deux ensembles, si $|A| \leq |B|$ et si $|B| \leq |A|$, alors $|A| = |B|$. Autrement dit, s'il existe une injection de A vers B et une de B vers A, alors on peut construire une bijection entre A et B.

Pour donner un peu l'esprit de ces preuves, faisons celle d'un résultat plus facile.

Proposition 1.6

Soient A et B deux ensembles non vides. On a $|A| \leq |B|$ si et seulement s'il existe une surjection de B vers A.

Démonstration : Supposons que $|A| \leq |B|$. Par définition, il existe une injection $f : a \in A \mapsto f(a) \in B$. Comme A est non vide, on peut choisir $a_* \in A$. On construit notre surjection $g : B \to A$ comme suit. Si b est dans l'image de f, on pose $g(b) = a$ avec $a \in A$ tel que $f(a) = b$. Si b n'est pas dans l'image de f, on pose $g(b) = a_*$.
Pour la réciproque, considérons une surjection $g : b \in B \mapsto g(b) \in A$. Pour tout $a \in A$, il existe au moins un $b_* \in B$ tel que $g(b_*) = a$. On pose simplement $f(a) = b_*$. Il est clair que f est une injection car si $f(a) = b_* = b'_* = f(a')$, $g(b_*) = g(b'_*)$ et donc $a = a'$. On notera au passage que pour chaque a, nous avons dû choisir un b_* dans l'ensemble $g^{-1}(a)$. Ça paraît évident, mais en fait cette opération n'est pas anodine et ne peut pas forcément être faite pour tout ensemble de points A quelle que soit sa taille. Elle demande l'utilisation d'un postulat appelé « axiome du choix ». Nous ne rentrerons pas dans les détails ici et de toute façon, nous n'utiliserons pas la proposition 1.6 dans un contexte si général que l'axiome du choix sera indispensable. □

Nous allons chercher quels ensembles de nombres sont dénombrables. Évidemment, $\mathbb{N}$ est dénombrable par définition. Avant de faire des propositions plus abstraites, nous allons faire à la main les cas de $\mathbb{Z}$ et $\mathbb{Q}$.

Proposition 1.7

L'ensemble $\mathbb{Z}$ est dénombrable.

Démonstration : On liste les entiers relatifs sous la forme $z_0 = 0$, $z_1 = 1$, $z_2 = -1$, $z_3 = 2$, $z_4 = -2$ et ainsi de suite. □

Proposition 1.8

L'ensemble $\mathbb{Q}$ est dénombrable.

Démonstration : On pose $r_0 = 0$, puis $r_1 = 1$ et $r_2 = -1$, puis $r_3 = 2$, $r_4 = 1/2$, $r_5 = -1/2$ et $r_6 = -2$, puis $r_7 = 3$, $r_8 = 3/2$ etc. À l'étape n, on liste les fractions du type p/q avec $p \in [\![-n,n]\!]$ et $q \in [\![1,n]\!]$, en sautant celles qu'on a déjà listées. Notons qu'on avance progressivement car chaque étape ne contient qu'un nombre fini de nouvelles fractions. $\square$

En fait, ces propositions peuvent se déduire des résultats plus généraux suivants, puisque $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ et $\mathbb{Q}$ est une partie de $\mathbb{Z} \times \mathbb{N}^*$ si r est identifié à sa forme irréductible p/q.

Proposition 1.9

Un ensemble est dénombrable si et seulement s'il s'injecte dans $\mathbb{N}$. En conséquence, un sous-ensemble d'un ensemble dénombrable est dénombrable.

Démonstration : laissée au lecteur. $\square$

Proposition 1.10

Une union dénombrable d'ensembles dénombrables est dénombrable.

Démonstration : Soient A_i, $i \in J$ un ensemble d'ensembles avec J dénombrable. Par définition, quitte à utiliser une bijection pour changer les indices, on peut supposer que J est fini ou $J = \mathbb{N}$. Par la suite, on va faire le cas $J = \mathbb{N}$, le cas J fini étant plus simple et laissé au lecteur. On sait qu'on peut lister les éléments de chaque ensemble A_i sous la forme $A_i = \{a_i^0, a_i^1, a_i^2, \ldots\}$. On va dénombrer les éléments de $\cup_{i\in\mathbb{N}} A_i$ suivant la liste

$$a_0^0 \quad a_1^0 \quad a_0^1 \quad a_2^0 \quad a_1^1 \quad a_0^2 \ldots$$

où à l'étape n, on liste les éléments a_i^j tels que $i + j \leq n$. On obtient ainsi une surjection de $\mathbb{N}$ dans $\cup_{i\in\mathbb{N}} A_i$ (car les A_i peuvent s'intersecter) et la proposition 1.6 conclut. $\square$

Proposition 1.11

Un produit fini d'ensembles dénombrables est dénombrable.

Démonstration : Soit A_i, $i = 0, \ldots, p$ des ensembles dénombrables que l'on liste sous la forme $A_i = \{a_i^0, a_i^1, a_i^2, \ldots\}$. On liste les éléments de $A_0 \times \ldots A_p$ en listant à l'étape n tous les $p-$uplets $(a_1^{j_1}, a_2^{j_2}, \ldots, a_p^{j_p})$ tels que $j_1 + j_2 + \ldots + j_p \leq n$. Chaque étape ne contient qu'un nombre fini de $p-$uplets et chaque $p-$uplet sera bien compté lors d'une étape. $\square$

Une des plus jolies preuves sur la cardinalité correspond au paradoxe du « barbier qui ne se rase pas lui-même ». On la doit à Cantor. Elle permet de montrer que l'on peut construire des ensembles toujours plus grands et qu'il existe ainsi une infinité de degrés dans la cardinalité infinie. Nous nous limiterons à la nuance dénombrable/indénombrable dans ce cours.

Théorème 1.12 Cantor

Soit A un ensemble et $\mathcal{P}(A)$ l'ensemble des parties de A. Alors $|A| < |\mathcal{P}(A)|$.

Démonstration : Comme on a l'injection $f : a \in A \mapsto \{a\} \in \mathcal{P}(A)$, on a $|A| \leq |\mathcal{P}(A)|$. Supposons qu'il existe une surjection $g : A \to \mathcal{P}(A)$. On regarde l'ensemble

$$E = \{a \in A\ ,\ \ a \notin g(a)\}\ .$$

Il s'agit d'un sous-ensemble de A, donc il existe $e \in A$ tel que $g(e) = E$. Si on a $e \in E$, alors par définition de E, $e \notin g(e) = E$, ce qui est absurde. Mais si on avait $e \notin E = g(e)$, alors par définition de E, on devrait avoir $e \in E$, ce qui est encore absurde. Donc l'existence de la surjection est absurde et d'après la proposition 6, le cardinal de $\mathcal{P}(A)$ est strictement plus grand que celui de A. $\square$

Le théorème de Cantor montre que $\mathbb{R}$ n'est pas dénombrable en associant au développement en base 2 d'un réel $x \in]0,1[$ l'ensemble des entiers n tels que le $n-$ième chiffre de x est 1. Mais il existe une preuve bien plus frappante, encore due à Cantor.

Georg Cantor (1845-1918) Allemagne

Proposition 1.13

L'ensemble $]0,1[$ est indénombrable.

Démonstration : On utilise l'argument diagonal de Cantor, qui est un raisonnement par l'absurde. Imaginons avoir listé tous les réels de $]0,1[$ dans un tableau de taille infinie :

$$\begin{aligned} x_1 &= 0,\ a_1^1\ a_1^2\ a_1^3\ a_1^4 \ldots \\ x_2 &= 0,\ a_2^1\ a_2^2\ a_2^3\ a_2^4 \ldots \\ x_3 &= 0,\ a_3^1\ a_3^2\ a_3^3\ a_3^4 \ldots \\ x_4 &= 0,\ a_4^1\ a_4^2\ a_4^3\ a_4^4 \ldots \\ &\vdots \end{aligned}$$

On construit un réel $y \in]0,1[$ en prenant comme $i-$ème chiffre un chiffre différent de a_i^i et de 9 (et au moins un chiffre non nul pour éviter d'avoir $y = 0$). On obtient un réel avec une écriture décimale propre et y n'est pas dans le tableau puisque s'il y était à la $n-$ième ligne, alors son $n-$ième chiffre serait a_n^n, ce qui est exclu par construction. Donc notre liste ne peut pas être exhaustive. □

Proposition 1.14

Tout intervalle non trivial de $\mathbb{R}$ est équipotent à $\mathbb{R}$. En conséquence, l'ensemble $\mathbb{R}$ ainsi que tout intervalle non trivial de $\mathbb{R}$ est indénombrable.

Démonstration : La fonction arctangente fournit une bijection entre $\mathbb{R}$ et $]-\pi/2,\pi/2[$. L'exponentielle fournit une bijection entre $\mathbb{R}$ et $]0,+\infty[$. Deux intervalles du type $]a,b[$ sont mis en bijection par de simples homothéties et translations, de même pour les intervalles d'autres types comme $[a,b]$, $]a,b]$, $[a,+\infty[$ etc. On peut obtenir des bijections explicites entre des intervalles de type différents en utilisant des arguments comme celui de l'hôtel de Hilbert (voir les compléments de ce chapitre). Si on ne cherche pas une forme explicite, on peut simplement utiliser le théorème 1.5 : tous les intervalles sont contenus dans $\mathbb{R}$ et tous les intervalles non triviaux contiennent un intervalle du type $]a,b[$ qui est équipotent à $\mathbb{R}$. □

Une conséquence assez troublante de ce résultat est la suivante. Comme écrire ou manipuler un nombre prend un certain laps de temps, aussi bien pour les humains que leurs ordinateurs, et qu'il n'y a qu'un nombre fini d'humains, alors on n'utilisera pendant toute l'histoire de l'humanité qu'une partie négligeable des nombres réels. De même, on ne pourra jamais trouver un système d'écriture permettant de décrire tous les réels en un nombre fini de caractères.

4 Compléments

4.1 Rationnels et irrationnels

Les nombres rationnels sont dénombrables alors que les réels sont indénombrables. Cela montre non seulement qu'il existe des irrationnels, mais surtout qu'il y en a « beaucoup plus » que de rationnels. De façon plus concrète, on connaît explicitement de nombreux irrationnels. Le premier connu serait $\sqrt{2}$. La preuve suivante suit la méthode d'Euclide (vers -300, Grèce).

Proposition 1.15 (irrationalité de $\sqrt{2}$)

Le nombre $\sqrt{2}$ ne peut s'écrire sous la forme a/b avec a et b entiers. En particulier, la diagonale d'un carré n'est pas commensurable à son côté.

Démonstration : Commençons par rappeler que le carré d'un nombre pair est pair car $(2p)^2 = 4p^2 = 2(2p^2)$ et que le carré d'un nombre impair est impair

car $(2p+1)^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1$.
Supposons qu'il existe deux entiers positifs a et b tels que $\sqrt{2} = a/b$. On a alors $2b^2 = a^2$, et donc a^2 est pair. Comme le carré d'un impair est impair, ceci implique que a est pair et s'écrit $a = 2a'$ avec a' entier. Mais alors $2b^2 = a^2 = 4a'^2$ et donc $b^2 = 2a'^2$ est pair. On en déduit que b est pair et s'écrit $b = 2b'$ avec b' entier. On a donc aussi que $\sqrt{2} = a'/b'$.
Mais on pourrait de nouveau appliquer l'argument et diviser par deux chacun des nombres de la fraction et ainsi de suite une infinité de fois, ce qui est absurde. Donc notre hypothèse de départ est fausse et $\sqrt{2}$ ne peut s'écrire sous forme d'une fraction. □

Cette démonstration s'adapte aux autres racines carrées qui ne sont pas entières. Ainsi, on peut montrer que $\sqrt{5}$ et donc le nombre d'or $\phi = (1+\sqrt{5})/2$ sont irrationnels. On sait aussi que e est irrationnel (1737, Leonhard Euler) ainsi que π (1768, Jean-Henri Lambert).

Il existe un lien surprenant entre les rationnels et l'écriture décimale.

Proposition 1.16

Un nombre $x \in \mathbb{R}$ est rationnel si et seulement si son développement décimal est périodique à partir d'un certain rang.

Démonstration : Supposons que x a un développement décimal périodique à partir d'un certain rang, c'est-à-dire qu'il s'écrit sous la forme

$$x = a_n \dots a_0{,}a_{-1} \dots a_m\, b_1 \dots b_p\, b_1 \dots b_p\, b_1 \dots b_p \dots$$

On pose $A = a_n \dots a_m$ et $B = b_1 \dots b_p$, qui sont deux entiers. Par définition de l'écriture décimale, on a donc

$$x = A.10^m + B \sum_{k \geq 1} 10^{m-kp} .$$

Il ne reste plus qu'à voir que

$$\sum_{k \geq 1} 10^{m-kp} = \frac{10^{m-p}}{1 - 10^{-p}}$$

est rationnel.
Réciproquement, soit $x = p/q$ un rationnel. Le développement décimal de x se trouve en faisant la division de p par q selon la méthode classique. À chaque étape, on a un reste entre 0 et $p-1$. Comme il y a un nombre fini de restes possibles, on tombe forcément à un moment sur un reste déjà vu. Dans ce cas, l'algorithme de division boucle et on retombe sur une suite de décimale qui vont se répéter. □

Ceci permet de créer de nombreux irrationnels. Par exemple $0{,}1010010001000010\dots$

est irrationnel ainsi que 0,12345678910111213...

4.2 L'hôtel de Hilbert

L'hôtel de Hilbert est une illustration des paradoxes sur l'infini dont la paternité est attribuée à David Hilbert.

Imaginons un hôtel possédant une infinité (dénombrable) de chambres numérotées 1, 2, 3... et imaginons que toutes les chambres sont occupées. Un nouveau client se présente, on pourrait penser qu'il n'aura pas de chambre pour lui. Mais l'hôtelier demande à chaque client de passer de la chambre n à la chambre $n+1$. La première chambre devient libre et le nouveau client peut s'y installer. Mathématiquement, on a montré que $\{-1\} \cup \mathbb{N}$ est équipotent à $\mathbb{N}$.

David Hilbert (1862-1943) Allemagne

Imaginons maintenant qu'un car contenant une infinité de clients arrive à l'hôtel. Toutes les chambres sont prises, mais l'hôtelier demande à chaque client de passer de la chambre n à la chambre $2n$. Toutes les chambres impaires deviennent libres et les nouveaux clients peuvent s'y installer. En termes mathématiques, on a montré que $\mathbb{Z}$ est équipotent à $\mathbb{N}$.

On peut utiliser la même idée pour obtenir des bijections explicites plus complexes.

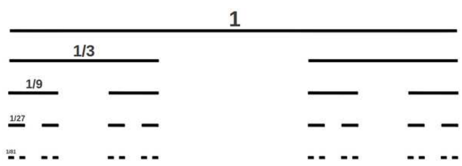
Exemple :

On veut obtenir une bijection explicite entre]0,1] et]0,1[. On va utiliser le premier argument de l'hôtel avec la suite $1/n$. On pose $f(x) = 1/(n+1)$ si $x = 1/n$ pour $n \in \mathbb{N}^*$ et $f(x) = x$ sinon. On a poussé d'un cran les « clients » des places $1/n$ pour caser le 1.
Notons que cette bijection n'est pas continue. On montrera dans ce cours qu'il n'est pas possible de construire une bijection f continue entre]0,1] et]0,1[pour des raisons topologiques, c'est-à-dire par l'essence même de ce qu'on apprendra dans ce cours.

4.3 L'ensemble de Cantor

L'ensemble de Cantor est un des fractals les plus simples. De ce fait, c'est un bon candidat pour obtenir des contre-exemples à des propriétés que l'on penserait vraies pour les ensembles de réels si on se limiterait à l'intuition que nous donnent les intervalles.

Il se construit ainsi : on part de [0,1] et on supprime le tiers central pour ne garder que $[0,1/3] \cup [2/3,1]$. Puis pour chaque intervalle restant, on recoupe en trois et on élimine le tiers central, puis on répète ainsi l'opération à l'infini. On peut montrer que l'ensemble obtenu est sous la forme



Les premières étapes de construction de l'ensemble de Cantor

$$\mathcal{C} = \left\{ x \in [0{,}1] \mid \exists (\epsilon_n)_{n\geq 1} \in \{0{,}1\}^{\mathbb{N}} \ , \ \ x = \sum_{n\geq 1} \frac{2\epsilon_n}{3^n} \right\} \ .$$

Cette description correspond à dire qu'on ne garde que les $x \in [0{,}1]$ tels que x s'écrive en base 3 qu'avec les chiffres 0 et 2, en autorisant les écritures impropres. En effet, retirer le tiers central de $[0{,}1]$ correspond à ne pas prendre les nombres qui s'écrivent $0{,}1\ldots$ en base deux. On s'autorise juste à prendre $0{,}1 = 0{,}022222\ldots$ Le découpage de l'étape n élimine les nombres qui utilisent le chiffre 1 en position n.

Pour tout n, l'ensemble de Cantor est contenu dans l'ensemble de l'étape n qui est composé de 2^n intervalles de longueurs $1/3^n$. Il est donc de « mesure » plus petite que $(2/3)^n$ pour tout n. On dit que l'ensemble de Cantor est *de mesure nulle* (un sens plus rigoureux sera vu au second semestre). L'ensemble des rationnels est aussi de mesure nulle, mais ce qui est particulier à l'ensemble de Cantor, c'est qu'il est de mesure nulle tout en étant indénombrable. C'est ainsi un exemple d'ensemble indénombrable qui ne contient aucun segment $]a{,}b[$.

Pour montrer que l'ensemble de Cantor est indénombrable, on peut considérer la surjection suivante

$$f \ : \ x = \sum_{n\geq 1} \frac{2\epsilon_n}{3^n} \ \in \mathcal{C} \ \longmapsto \ f(x) = \sum_{n\geq 1} \frac{\epsilon_n}{2^n} \in [0{,}1] \ .$$

Autrement dit, on associe à l'écriture en base 3 avec des 0 et des 2, l'écriture en base 2 avec des 0 et des 1. On obtient une surjection qui n'est pas une bijection à cause des écritures impropres. Mais cela suffit à dire que le cardinal de $\mathcal{C}$ est plus grand que celui de $[0{,}1]$ et donc que $\mathcal{C}$ est indénombrable.