Chapitre 1

Logique, ensembles, arithmétique

La logique mathématique prend naissance avec George Boole au milieu du XIX^e siècle et se formalise aux alentours de 1900 alors qu'apparaît la théorie des ensembles sous l'impulsion de Georg Cantor (1845-1918) et Richard Dedekind (1831-1916). Elle permet de fonder rigoureusement les mathématiques, tâche qui devient nécessaire lorsque les mathématiques se détachent de la physique. Quant à l'arithmétique, elle est aussi ancienne que les mathématiques puisqu'elle débute dès l'Antiquité ; certaines conjectures en arithmétique se sont révélées fausses, comme nous le verrons grâce à quelques contre-exemples.

■ Logique des prédicats du premier ordre

Les mathématiques se fondent en particulier sur la logique des prédicats du premier ordre, construite à l'aide des connecteurs propositionnels « non », « et », « ou », « implique » et « équivalent », de variables x, y, $z\ldots$, de propositions, de prédicats $P(x)$, $Q(x,y)\ldots$ et des quantificateurs existentiel $\exists$ et universel $\forall$.

Si l'on souhaite utiliser des quantificateurs dans un texte mathématique — ce n'est jamais indispensable... —, leur maniement doit se faire avec soin. On peut intervertir deux quantificateurs de même nature se suivant dans une formule, mais il n'en est pas de même pour deux quantificateurs de natures différentes.

1.1. Exemple où la proposition $\forall x\,\exists y\,\big(P(x,y)\big)$ est vraie alors que l'assertion $\exists y\,\forall x\,\big(P(x,y)\big)$ est fausse.

Nous prenons $\mathbb{N}$ comme ensemble de référence et nous symbolisons par $P(x,y)$ l'assertion : x est inférieur ou égal à y. Alors, pour tout entier naturel x, si l'on choisit un entier naturel y supérieur ou égal à x, l'assertion $P(x,y)$ est vraie ; la proposition $\forall x\,\exists y\,\big(P(x,y)\big)$ est donc vraie. Par contre, $\mathbb{N}$ n'ayant pas de plus grand élément, l'assertion $\exists y\,\forall x\,\big(P(x,y)\big)$ est fausse. □

Remarquons que si la deuxième des formules de l'exemple 1.1 est vraie, alors la première l'est, c'est-à-dire que l'implication $\exists y\,\forall x\,\big(P(x,y)\big) \implies \forall x\,\exists y\,\big(P(x,y)\big)$ est universellement valide ; intuitivement nous voyons que dans le terme de gauche y ne dépend pas de x, alors que dans celui de droite il peut en dépendre : la condition est donc moins forte. C'est ainsi qu'une utilisation de l'interversion de quantificateurs de natures différentes est faite pour passer de la continuité à la continuité uniforme[1] : $\mathcal{A}$ étant une partie de $\mathbb{R}$ et f une fonction de $\mathbb{R}$ dans $\mathbb{R}$ définie sur $\mathcal{A}$, la continuité de f sur $\mathcal{A}$ s'exprime par la proposition :

$$(\forall\varepsilon > 0)(\forall x \in \mathcal{A})(\exists\eta > 0)(\forall y \in \mathcal{A})\big(|\,x - y\,| < \eta \Longrightarrow |\,f(x) - f(y)\,| < \varepsilon\big)$$

et la continuité uniforme de f sur $\mathcal{A}$ par l'assertion :

$$(\forall\varepsilon > 0)(\exists\eta > 0)(\forall x \in \mathcal{A})(\forall y \in \mathcal{A})\big(|\,x - y\,| < \eta \Longrightarrow |\,f(x) - f(y)\,| < \varepsilon\big).$$

Les connecteurs « et » et « ou » étant symbolisés respectivement par $\wedge$ et $\vee$, les propositions $\forall x\,\big(P(x) \wedge Q(x)\big)$ et $\forall x\,\big(P(x)\big) \wedge \forall x\,\big(Q(x)\big)$ sont équivalentes, de même que les assertions $\exists x\,\big(P(x) \vee Q(x)\big)$ et $\exists x\,\big(P(x)\big) \vee \exists x\,\big(Q(x)\big)$.

1.2. Exemple où l'assertion $\forall x\,\big(P(x) \vee Q(x)\big)$ est vraie alors que la proposition $\forall x\,\big(P(x)\big) \vee \forall x\,\big(Q(x)\big)$ est fausse.

Nous prenons de nouveau $\mathbb{N}$ comme ensemble de référence et nous symbolisons, pour tout entier naturel x, par $P(x)$ l'assertion : x est pair, et par $Q(x)$ la proposition : x est impair. Alors $\forall x\,\big(P(x) \vee Q(x)\big)$ exprime que tout entier naturel est pair ou impair, ce qui est vrai ; par contre $\forall x\,\big(P(x)\big) \vee \forall x\,\big(Q(x)\big)$ exprime que soit tous les entiers sont pairs, soit ils sont tous impairs, ce qui est bien sûr faux. $\square$

1.3. Exemple où la proposition $\exists x\,\big(P(x)\big) \wedge \exists x\,\big(Q(x)\big)$ est vraie alors que l'assertion $\exists x\,\big(P(x) \wedge Q(x)\big)$ est fausse.

Les hypothèses sont celles l'exemple 1.2. Alors $\exists x\,\big(P(x)\big) \wedge \exists x\,\big(Q(x))\big)$ exprime qu'il existe (au moins) un entier pair et (au moins) un entier impair, alors que $\exists x\,\big(P(x) \wedge Q(x)\big)$ exprime qu'il existe un entier simultanément pair et impair. $\square$

Remarquons que dans la première des propositions de l'exemple précédent 1.3, on peut remplacer la deuxième occurrence de x par y, car x est ici une variable muette, et que donc un élément qui vérifie $\exists x\,\big(P(x)\big)$ n'est pas forcément le même qu'un élément vérifiant $\exists x\,\big(Q(x)\big)$; par contre, dans la deuxième proposition, c'est le même élément qui doit remplir les deux conditions.

■ Paradoxes de la théorie "naïve" des ensembles

La théorie des ensembles, œuvre des mathématiciens allemands Georg Cantor et Richard Dedekind, apparaît à la fin du XIXᵉ siècle. Dans cette première approche, que l'on qualifie maintenant de « naïve », on appelle ensemble n'importe quelle collection d'objets[2], ce qui conduit à des paradoxes.

1.4. Paradoxe de Russel[3].

Nous considérons l'ensemble $A = \{\,X \mid X \notin X\,\}$. Alors *l'objet* A appartient ou bien n'appartient pas à *l'ensemble* A. Si A appartient à A, alors, par définition de A, on obtient que A n'appartient à pas A ; si A n'appartient pas à A, cette même

1. Voir le chapitre 8, page 144.
2. Georg Cantor débute son mémoire de mars 1895, publié dans les *Mathematische Annalen*, ainsi : « *Nous appelons "ensemble" toute réunion M d'objets de notre conception m, déterminés et bien distincts, et que nous appelons "éléments" de M.* »
3. Il est énoncé en 1905 par le mathématicien et philosophe anglais Bertrand Russel (1872-1970).

définition nous permet d'affirmer que A appartient à A. Ainsi les deux assertions « A appartient à A » et « A n'appartient pas à A » sont simultanément vraies... $\square$

Nous rappelons que l'ensemble des parties d'un ensemble E est noté $\mathcal{P}(E)$.

THÉORÈME 1.1. — Théorème de Cantor.
Si E est un ensemble, il n'existe aucune injection de $\mathcal{P}(E)$ dans E.

1.5. Paradoxe de Cantor.

En notant E l'ensemble de tous les ensembles, l'ensemble $\mathcal{P}(E)$ est inclus dans E donc l'injection canonique de $\mathcal{P}(E)$ dans E contredit le théorème de Cantor. $\square$

Pour remédier à de tels paradoxes, une théorie axiomatique des ensembles a été élaborée. C'est la théorie des ensembles Zermelo-Fraenkel, en abrégé ZF, ainsi dénommée car elle a été conçue par Ernst Zermelo[4] en 1908 — il l'expose dans ses *Recherches sur les fondements de la théorie des ensembles* — et modifiée par Abraham Fraenkel[5] en 1921 et 1922. La théorie ZF sert depuis cette époque de fondement aux mathématiques, dont elle permet une construction rigoureuse, même si sa consistance, c'est-à-dire l'absence de paradoxes, ne pourra jamais être prouvée, comme le montre Kurt Gődel[6] en 1931. Les mathématiciens d'aujourd'hui font le pari de cette consistance et fondent les mathématiques sur la théorie ZF.

■ Image directe et image réciproque d'une partie

Ayant surtout en vue de l'étude de la notion de cardinal, Georg Cantor utilise essentiellement des correspondances biunivoques entres les ensembles, ce que nous appelons maintenant des bijections, alors que Richard Dedekind introduit dans toute sa généralité la notion d'application d'un ensemble dans un autre.

Soit f une application d'un ensemble E dans un ensemble F.

Si A est une partie de l'ensemble E, l'image directe de A par f est la partie $f(A) = \{\, f(x) \mid x \in A\,\}$ de F et, si M est une partie de F, l'image réciproque de M par f est la partie $f^{-1}(M) = \{\, x \in E \mid f(x) \in M\,\}$ de E.

Si A et B sont des parties de E, alors $f(A \cup B) = f(A) \cup f(B)$, mais en général on a seulement l'inclusion $f(A \cap B) \subset f(A) \cap f(B)$. Cependant, si l'application f est injective, cette inclusion devient une égalité.

1.6. Parties A et B de E telles que $f(A \cap B) \neq f(A) \cap f(B)$.

Nous introduisons l'application $f : n \mapsto f(n) = |n|$ de $\mathbb{Z}$ dans $\mathbb{Z}$ et les parties $A = \mathbb{N}$ et $B = -\mathbb{N}$ de $\mathbb{Z}$. Alors $A \cap B = \{0\}$ donc $f(A \cap B) = \{0\}$. Par contre $f(A) = f(B) = \mathbb{N}$ donc $f(A) \cap f(B) = \mathbb{N}$. $\square$

Pour une partie A de E, une partie B de F et une application f de E dans F, on a les inclusions $A \subset f^{-1}\big(f(A)\big)$ et $f\big(f^{-1}(B)\big) \subset B$. La première est une égalité si f est injective et la seconde si f est une surjection de E sur F.

4. Mathématicien et logicien allemand (1871-1953).
5. Mathématicien et logicien israélien d'origine allemande (1891-1965).
6. Mathématicien et logicien autrichien (1906-1978).

1.7. Partie A de E telle que $A \neq f^{-1}\big(f(A)\big)$.

Nous utilisons de nouveau l'application $f : n \mapsto f(n) = |n|$ de $\mathbb{Z}$ dans $\mathbb{Z}$ et nous posons $A=\mathbb{N}$. Alors $f(A)=\mathbb{N}=f(\mathbb{Z})$ donc $f^{-1}\big(f(A)\big)=\mathbb{Z} \neq A$. □

1.8. Partie M de F telle que $M \neq f\big(f^{-1}(M)\big)$.

Pour l'application $f : n \mapsto f(n) = |n|$ de $\mathbb{Z}$ dans $\mathbb{Z}$ et $M = -\mathbb{N}$, $f^{-1}(M) = \{0\}$ — seul 0 s'envoit sur un élément de $-\mathbb{N}$—, donc $f\big(f^{-1}(M)\big) = \{0\} \neq M$. □

On a, pour toute partie M de F, $f^{-1}\big(\complement_F M\big) = \complement_E f^{-1}(M)$. Ceci est faux pour l'image directe et il n'y a dans ce cas d'inclusion ni dans un sens, ni dans l'autre.

1.9. Partie A de E telle que $f\big(\complement_E A\big) \neq \complement_F f(A)$.

Nous considérons de nouveau l'application $f : n \mapsto f(n) = |n|$ de $\mathbb{Z}$ dans $\mathbb{Z}$ et nous posons $A = \mathbb{N}$. Alors $\complement_{\mathbb{Z}} A = -\mathbb{N}^*$, ensemble des entiers strictement négatifs, donc $f\big(\complement_{\mathbb{Z}} A\big) = \mathbb{N}^*$. Par ailleurs $f(A) = \mathbb{N}$, donc $\complement_{\mathbb{Z}} f(A) = -\mathbb{N}^*$; non seulement les deux ensembles diffèrent mais ils sont disjoints. □

■ Ensembles équipotents

DÉFINITION 1.1. — Si E et F sont des ensembles, E est équipotent à F s'il existe une bijection de E sur F.

La relation d'équipotence, symbolisée par $\mathcal{E}q$, est une relation réflexive, transitive et symétrique sur la « classe » — et non l'ensemble, voir l'exemple 1.5 — de tous les ensembles, ce qui signifie que, quels que soient les ensembles X, Y et Z, $X \ \mathcal{E}q\ X$ (réflexivité), $X\ \mathcal{E}q\ Y$ et $Y\ \mathcal{E}q\ Z$ entraînent $X\ \mathcal{E}q\ Z$ (transitivité), et $X\ \mathcal{E}q\ Y$ entraîne $Y\ \mathcal{E}q\ X$ (symétrie). Compte tenu de la symétrie, on dit que les ensembles E et F sont équipotents pour exprimer que E (ou F) est équipotent à F (ou à E).

Intuitivement, des ensembles E et F sont équipotents s'ils ont « le même nombre d'éléments », ce qui conduit à la notion de cardinal d'un ensemble, développée par Cantor parallèlement à la notion d'ordinal — les cardinaux servent à « compter » le nombre des éléments d'un ensemble et les ordinaux à les « numéroter ».

Tous les ensembles ont un cardinal, des ensembles sont équipotents si, et seulement si, ils ont le même cardinal et le cardinal d'un ensemble fini est le nombre de ses éléments au sens traditionnel. Le cardinal d'un ensemble E se note $\mathrm{card}(E)$.

Euclide cite parmi ses axiomes : « *La partie est toujours plus petite que le tout* ». Ce n'est en fait vrai que pour les ensembles finis : dans un ensemble infini E, il existe une partie stricte de même cardinal que E, c'est-à-dire équipotente à E.

1.10. Partie stricte de $\mathbb{N}$ équipotente à $\mathbb{N}$.

L'ensemble $\mathbb{P}$ des nombres entiers naturels pairs est une partie stricte de $\mathbb{N}$ et l'application $f : n \mapsto f(n) = 2n$ une bijection de $\mathbb{N}$ sur $\mathbb{P}$, donc $\mathbb{N}$ et $\mathbb{P}$ sont des ensembles équipotents[7]. □

7. Galilée avait déjà remarqué que l'application $\varphi : n \mapsto \varphi(n) = n^2$ de $\mathbb{N}$ dans $\mathbb{N}$ est une bijection de $\mathbb{N}$ sur l'ensemble C des carrés d'entiers naturels, partie stricte de $\mathbb{N}$.

1.11. Partie stricte de $\mathbb{R}$ équipotente à $\mathbb{R}$.

Pour tout réel x, $\left|\dfrac{x}{1+|x|}\right| = \dfrac{|x|}{1+|x|} < 1$, ce qui justifie l'existence de l'application :

$$\left|\begin{array}{rcl} f\ :\ \mathbb{R} & \longrightarrow &]-1,1[\\ x & \longmapsto & f(x) = \dfrac{x}{1+|x|}. \end{array}\right.$$

Nous remarquons que, pour tout réel x, les réels x et $f(x)$ sont de même signe. Si x et y sont des nombres réels et si $f(x) = f(y)$, x et y sont de même signe donc, si $x \geqslant 0$, $x/(1+x) = y/(1+y)$ et, si $x < 0$, $x/(1-x) = y/(1-y)$, d'où l'on déduit que $x = y$. Si c appartient à l'intervalle ouvert $]-1,1[$, alors, en notant a la solution de l'équation $x/(1+x) = c$ si $c \geqslant 0$ et la solution de $x/(1-x) = c$ si $c < 0$, a est un antécédent de c par f. Ainsi f est une bijection de $\mathbb{R}$ sur $]-1,1[$. En conclusion, la partie stricte $]-1,1[$ de $\mathbb{R}$ est équipotente à $\mathbb{R}$. $\square$

Remarquons que si a et b sont des réels et si $a < b$, l'intervalle ouvert $]a,b[$ est équipotent à $\mathbb{R}$. En effet, en notant φ l'unique application affine de $\mathbb{R}$ dans $\mathbb{R}$ telle que $\varphi(-1) = a$ et $\varphi(1) = b$ — c'est l'application $\varphi : x \mapsto \alpha x + \beta$ où $\alpha = (b-a)/2$ et $\beta = (b+a)/2$ — la restriction de φ à $]-1,1[$ est une bijection de $]-1,1[$ sur $]a,b[$, donc $]a,b[$ est équipotent à $]-1,1[$ et, comme l'intervalle $]-1,1[$ est équipotent à $\mathbb{R}$ — voir l'exemple précédent 1.11 —, les ensembles $]a,b[$ et $\mathbb{R}$ sont équipotents.

On peut remplacer l'application f de l'exemple 1.11 par la fonction « tangente hyperbolique » ou l'application $g : x \mapsto g(x) = (2/\pi)\arctan x$ de $\mathbb{R}$ dans $]-1,1[$.

L'ensemble $\mathbb{N}$ paraît avoir « moins d'éléments » que $\mathbb{N}^2$. En fait il n'en est rien : ces ensembles sont équipotents.

1.12. Bijection de $\mathbb{N}^2$ sur $\mathbb{N}$.

Nous introduisons la suite $(a_n)_{n\in\mathbb{N}}$ d'entiers naturels, de terme général :

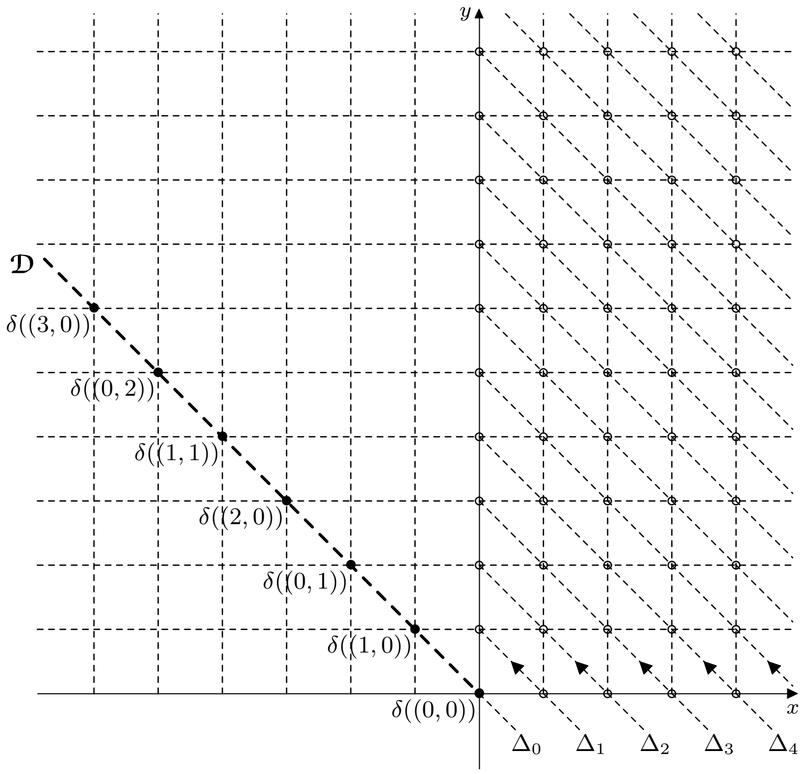
$$a_n = \sum_{i=0}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ (quotient exact).}$$

On a, pour tout entier naturel n, $a_{n+1} = a_n + (n+1)$; en particulier, $(a_n)_{n\in\mathbb{N}}$ est strictement croissante. Nous déduisons de la suite $(a_n)_{n\in\mathbb{N}}$ l'application :

$$\left|\begin{array}{rcl} f\ :\ \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (p,q) & \longmapsto & f\big((p,q)\big) = a_{p+q} + q. \end{array}\right.$$

Soit $m \in \mathbb{N}$. Comme $a_0 = 0 \leqslant m \leqslant a_m$, l'ensemble $M = \{k \in \mathbb{N} \mid a_k \leqslant m\}$ est une partie non vide de $\mathbb{N}$ majorée dans $\mathbb{N}$ (par m) donc M admet un plus grand élément n, et n est l'unique entier naturel tel que $a_n \leqslant m < a_{n+1}$. Si (p,q) est un antécédent de m par f, alors $m = f\big((p,q)\big) = a_{p+q}+q$ et $a_{p+q+1} = a_{p+q}+(p+q+1)$, donc $a_{p+q} \leqslant m < a_{p+q+1}$, ce qui montre que $p+q = n$ et $q = m-a_n$, d'où l'unicité du couple (p,q). Inversement, $m - a_n$ et $n - m + a_n$ sont des entiers naturels de somme n et $f(n-m+a_n, m-a_n) = a_n + (m-a_n) = m$, donc $(n-m+a_n, m-a_n)$ est un antécédent de m par f. En conclusion, f est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$. $\square$

Nous gardons les définitions et les notations de l'exemple précédent 1.12 et nous posons, pour tout entier naturel n, $\Delta_n = \{(p,q) \mid p,q \in \mathbb{N} \text{ et } p+q = n\}$, c'est-à-dire $\Delta_n = \{(n,0),(n-1,1),\dots,(n-k,k),\dots,(1,n-1),(0,n)\}$, ensemble fini de cardinal $n+1$ ordonné par les deuxièmes projections des couples — voir les flèches du dessin ci-dessous sur Δ_1, Δ_2, $\Delta_3\dots$ Sur ce dessin, $\mathbb{N}^2$ est représenté dans le plan $\mathbb{R}^2$, les couples (p,q) pour $p,q\in\mathbb{N}$ étant figurés par de petits cercles.



La famille $(\Delta_n)_{n\in\mathbb{N}}$ est une partition de $\mathbb{N}^2$ et la famille $([\![a_n, a_{n+1}-1]\!])_{n\in\mathbb{N}}$ une partition de $\mathbb{N}$, et, pour tout $n\in\mathbb{N}$, la restriction f_n de f à Δ_n est la bijection de Δ_n sur $[\![a_n, a_{n+1}-1]\!]$ définie par $f_n\big((n-k,k)\big) = a_n + k$ pour tout $k\in[\![0,n]\!]$. Nous notons, pour tout entier naturel n, δ_n la restriction à Δ_n de la translation τ_n de $\mathbb{R}^2$ de vecteur $(-n-a_n, a_n)$, qui transforme $(n,0)$ en $(-a_n,a_n)$, et nous posons $\mathcal{D} = \{(-n,n)\mid n\in\mathbb{N}\}$, ensemble évidemment équipotent à $\mathbb{N}$. Alors, en « recollant » la famille $(\delta_n)_{n\in\mathbb{N}}$, on obtient une bijection δ de $\mathbb{N}^2$ sur $\mathcal{D}$ qui illustre de façon beaucoup plus visuelle que f l'équipotence entre $\mathbb{N}^2$ et $\mathbb{N}$.

Ces considérations montrent que l'équipotence entre $\mathbb{N}^2$ et $\mathbb{N}$ est bien moins étonnante qu'il n'y paraît au premier abord : nous avons transformé facilement, par une bijection, $\mathbb{N}^2$ en une partie $\mathcal{D}$ de $\mathbb{R}^2$ équipotente à $\mathbb{N}$. Il paraît en revanche impossible de tranformer par une bijection le plan $\mathbb{R}^2$ (une plaque d'aire infinie) en une droite de $\mathbb{R}^2$ (un fil de fer). Pourtant Cantor démontre, en juin 1877, que $\mathbb{R}^2$ est équipotent à $\mathbb{R}$ et il en est stupéfait [8]. On sait maintenant que tout ensemble infini E est équipotent à son carré $E^2 = E\times E$.

8. Dans une lettre à Dedekind datée du 29 juin 1877, il écrit, en français dans le texte : *Je le vois, mais je ne le crois pas.*

THÉORÈME 1.2. — Théorème de Cantor-Bernstein[9].
Si E et F sont des ensembles et s'il existe une injection de E dans F et une injection de F dans E, alors les ensembles E et F sont équipotents.

DÉFINITION 1.2. — Un ensemble est dénombrable s'il est équipotent à $\mathbb{N}$.

L'ensemble E est donc dénombrable si, et seulement si, il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments deux à deux distincts de E telle que $E=\{a_n \mid n \in \mathbb{N}\}=\{a_0, a_1, a_2, \ldots\}$, ce qui signifie que l'on peut « numéroter » les éléments de E par les entiers naturels.

Les ensembles $\mathbb{Z}$ et $\mathbb{N}^2$, l'ensemble $\mathbb{Q}$ des nombres rationnels et l'ensemble $\mathbb{A}$ des nombre algébriques[10] sont dénombrables. Pour $\mathbb{N}^2$ une preuve en est faite dans l'exemple précédent 1.12, mais on peut aussi raisonner de la manière suivante : l'application $n \mapsto (n, 0)$ est une injection de $\mathbb{N}$ dans $\mathbb{N}^2$ et, 2 et 3 étant des nombres premiers, l'application $(k, \ell) \mapsto 2^k 3^\ell$ est une injection de $\mathbb{N}^2$ dans $\mathbb{N}$, donc on déduit du théorème de Cantor-Bernstein que $\mathbb{N}$ et $\mathbb{N}^2$ sont équipotents. Un raisonnement analogue, utilisant n nombres premiers $p_1, \ldots, p_n$ deux à deux distincts, permet de prouver que, pour tout entier $n \geqslant 2$, les ensembles $\mathbb{N}$ et $\mathbb{N}^n$ sont équipotents.

Les ensembles $\mathbb{Z}$, puis $\mathbb{Q}$, les $\mathbb{N}^n$ pour $n \geqslant 2$ et $\mathbb{A}$, sont « de plus en plus grands » mais ils sont tous dénombrables. On pourrait donc penser qu'il en est de même pour tous les ensembles infinis, ce qui est faux comme le montre l'exemple suivant.

1.13. Ensemble infini qui n'est pas dénombrable.

Nous démontrons que l'ensemble infini $\mathbb{R}$ n'est pas dénombrable. La preuve la plus souvent donnée de ce résultat utilise les développements décimaux illimités. Cependant la première démonstration de cette assertion par Cantor est plus simple et elle met bien en évidence la propriété fondamentale du corps des nombres réels qui est mise en œuvre.

Nous débutons par une remarque : si a, b et x sont des réels et si $a < b$, on peut construire un couple (a', b') de nombres réels tel que $a \leqslant a' < b' \leqslant b$ et $x \notin [a', b']$ — en posant par exemple $c = a + (b - a)/2$, $d = a + (b - a)/3$ et : $a' = c$ et $b' = b$ si $x < c$; $a' = a$ et $b' = d$ si $x \geqslant c$.

Supposons $\mathbb{R}$ dénombrable. Alors $\mathbb{R} = \{\omega_n \mid n \in \mathbb{N}\} = \{\omega_0, \omega_1, \omega_2, \ldots, \omega_n, \ldots\ldots\}$ où $(\omega_n)_{n\in\mathbb{N}}$ est une suite de réels deux à deux distincts. On construit les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ de réels, par récurrence sur $n \in \mathbb{N}$, en posant $a_0 = 0$ et $b_0 = 1$ et en notant, pour tout entier naturel n, (a_{n+1}, b_{n+1}) le couple de réels tel que $a_n \leqslant a_{n+1} < b_{n+1} \leqslant b_n$ et $\omega_n \notin [a_{n+1}, b_{n+1}]$ obtenu dans la remarque ci-dessus. Les suites (a_n) et (b_n) convergent dans $\mathbb{R}$ et, en notant λ la limite de (a_n) et μ celle de (b_n), on a $\lambda \leqslant \mu$ et, pour tout entier naturel n, $a_n \leqslant \lambda \leqslant \mu \leqslant b_n$. De plus il existe $p \in \mathbb{N}$ tel que $\lambda = \omega_p$; or on a $a_{p+1} \leqslant \lambda \leqslant b_{p+1}$, ce qui contredit l'assertion $\omega_p \notin [a_{p+1}, b_{p+1}]$. En conclusion, $\mathbb{R}$ n'est pas dénombrable. □

9. Ce théorème est énoncé par Cantor qui ne réussit pas à le démontrer. Indépendamment l'un de l'autre, Ernst Schrőder (1841-1902) en 1896 et Felix Bernstein (1878-1956) en 1897 en donnent une démonstration. Dedekind en expose une preuve en 1899, dans une lettre à Cantor, preuve rédigée en 1887 mais qu'il ne publie pas, en raison des doutes qui l'assaillent de plus en plus quant à la validité de la théorie des ensembles telle que créée par lui-même et Cantor, et qu'il développe dans son ouvrage « *Was sind und was sollen die Zahlen ?* » — en français « *Que sont et que représentent les nombres ?* » — élaboré entre 1872 et 1878 et publié seulement en 1888.
10. Voir la définition 5.1, page 84.

1.14. Autre ensemble infini qui n'est pas dénombrable.

Supposons que l'ensemble infini $\mathcal{A} = \mathfrak{F}(\mathbb{N}, \mathbb{N})$ des applications de $\mathbb{N}$ dans $\mathbb{N}$ soit dénombrable. Alors $\mathcal{A} = \{\varphi_n \mid n \in \mathbb{N}\} = \{\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n, \ldots\ldots\}$ où $(\varphi_n)_{n\in\mathbb{N}}$ est une suite d'applications deux à deux distinctes de $\mathbb{N}$ dans $\mathbb{N}$. Nous introduisons l'application $f : n \mapsto f(n) = 1 + \varphi_n(n)$ de $\mathbb{N}$ dans $\mathbb{N}$. Comme $f \in \mathcal{A}$, il existe un entier naturel p tel que $f = \varphi_p$. On a, pour tout $n \in \mathbb{N}$, $\varphi_p(n) = f(n)$, donc en particulier $\varphi_p(p) = f(p) = 1 + \varphi_p(p)$, ce qui est évidemment faux. Par conséquent l'ensemble $\mathcal{A} = \mathfrak{F}(\mathbb{N}, \mathbb{N})$ n'est pas dénombrable. □

La méthode utilisée dans l'exemple précédent 1.14 est *le procédé diagonal de Cantor* et c'est avec ce procédé, appliqué aux suites des décimales des points de $]0, 1[$, supposé dénombrable, donc s'écrivant $\{a_n \mid n \in \mathbb{N}\}$ où $(a_n)_{n\in\mathbb{N}}$ est une suite de réels deux à deux distincts, que l'on peut prouver que $\mathbb{R}$ n'est pas dénombrable.

■ Relations binaires fondamentales

Parmi les relations binaires sur un ensemble [11], les relations d'équivalence sont essentielles, car elles permettent d'identifier les éléments jouant un même rôle dans une structure, ainsi que les relations d'ordre, indispensables à l'étude des nombres réels et plus généralement à l'analyse, mais aussi, par l'intermédiaire de la notion de bon ordre — voir dans la suite de ce chapitre — à la théorie des ensembles.

DÉFINITION 1.3. — Une relation d'équivalence sur un ensemble E est une relation binaire réflexive, transitive et symétrique sur E.

Montrons que chacune des trois propriétés est nécessaire, car deux d'entre elles n'entraînent pas nécessairement la troisième. Remarquons tout d'abord que la relation de divisibilité sur $\mathbb{N}$ est réflexive et transitive mais n'est pas symétrique. Remarquons aussi qu'un raisonnement fallacieux pourrait faire penser qu'une relation $\mathcal{R}$ symétrique et transitive est nécessairement réflexive, car $a\,\mathcal{R}\,b$ entraîne $b\,\mathcal{R}\,a$ par symétrie et $a\,\mathcal{R}\,a$ par transitivité ; cependant un élément peut n'être en relation avec aucun autre, comme dans l'exemple qui suit.

1.15. Relation symétrique et transitive qui n'est pas réflexive.

Définissons sur l'ensemble $\mathbb{Z}$ des entiers relatifs la relation binaire $\mathcal{R}$ par : $a\,\mathcal{R}\,b$ si $ab > 0$. La relation $\mathcal{R}$ est clairement symétrique. Si $a, b, c \in \mathbb{Z}$ et si $a\,\mathcal{R}\,b$ et $b\,\mathcal{R}\,c$, alors $ab > 0$ et $bc > 0$ donc, en multipliant membre à membre, $ab^2c > 0$, et comme $b^2 > 0$ — en effet, $ab > 0$, donc $b \neq 0$ —, on a $ac > 0$, donc $a\,\mathcal{R}\,c$: $\mathcal{R}$ est transitive. Cependant l'assertion $0\,\mathcal{R}\,0$ est fausse, donc $\mathcal{R}$ n'est pas réflexive. □

1.16. Relation réflexive et symétrique qui n'est pas transitive.

Nous posons $N = \{n \in \mathbb{N} \mid n \geqslant 2\}$ et nous introduisons la relation binaire $\mathcal{R}$ définie sur N par : $a\mathcal{R}b$ si a et b ont en commun un diviseur premier. Tout élément de N possèdant au moins un diviseur premier, $\mathcal{R}$ est réflexive ; la symétrie de $\mathcal{R}$ est

11. Pour les définitions, voir [RAM1], chapitre 1, §**1**.3.