Chapitre I

Le type « ensemble »

Partant des intuitions de base, et rapidement convaincus que des problèmes difficiles se posent dès que des ensembles infinis sont introduits, nous cherchons ici les fondements sur lesquels une théorie des ensembles peut être élaborée : que sont les ensembles, quelles opérations et relations s'y rattachent, quels principes de base les gouvernent ? En nous efforçant de garder l'approche la plus élémentaire possible, nous serons conduits à emprunter le chemin ouvert par Georg Cantor à la fin du XIX^{e} siècle, puis à suivre ses ajustements successifs pour parvenir au système de Zermelo, fondement des développements ultérieurs.

> ▷ *On trouvera ici davantage de discussions informelles que de démonstrations, ce qui est naturel puisque l'opportunité de bâtir une théorie et le choix d'un système axiomatique de départ sont affaires de* consensus *et non de démonstration : sauf à proclamer un dogme que rien ne justifie, la seule chose qui puisse être recherchée est un accord partagé sur une position du type « Oui, la formalisation proposée est conforme à l'intuition que nous partageons des objets étudiés, ici les ensembles et l'infini » et, de là, « Oui, il est raisonnable d'explorer les problèmes ouverts sur de telles bases et nous jugerons convaincantes les conséquences de celles-ci ». Refaire le chemin tracé par les pionniers n'est peut-être pas la seule manière d'obtenir un tel accord, mais c'est en tout cas une manière commode de procéder pour écarter les approches trop simplistes et comprendre les subtilités du système finalement retenu, lequel pourrait au départ être jugé non intuitif, voire artificiel.*
>
> *Ce que nous verrons vite dans la suite est que la théorie des ensembles est une théorie de l'infini plus qu'une théorie des ensembles au sens propre : pour les ensembles finis, comme on le constatera dans la section* 2*, (presque) tout est dit quand on a dégagé la structure d'algèbre de Boole. En revanche, dès qu'il est jugé opportun de considérer des ensembles infinis, la situation est radicalement différente et c'est là que la théorie des ensembles aura à se déployer.* ◁

Le chapitre comporte trois sections. Dans la section 1, on justifie l'opportunité de développer une théorie des ensembles par l'irruption immédiate de problèmes apparemment difficiles dès que des ensembles infinis entrent en jeu. Dans la section 2, on introduit les opérations ensemblistes usuelles,

réunion, intersection, *etc.*, et on montre que la structure d'algèbre de Boole en capture toutes les propriétés dans le cas fini. Dans la section 3, on ébauche une théorie des ensembles. Comme une définition *ex nihilo* est malaisée, on recourt à une approche axiomatique, et la nécessité d'échapper aux paradoxes de Berry et de Russell mène au système de Zermelo.

1. Pourquoi une théorie des ensembles ?

Après une brève discussion de la notion d'ensemble et de son utilité, on examine les problèmes liés à la comparaison de la taille des ensembles. Dans le cas fini, on établit facilement les résultats combinatoires élémentaires. En revanche, des problèmes surgissent rapidement lorsque l'on passe aux ensembles infinis, au premier plan desquels le problème du continu de Cantor. L'existence de tels problèmes est la justification la plus naturelle de l'intérêt de développer une *théorie* des ensembles.

> ▷ *Les mathématiques étudient des objets appartenant à des types variés : entiers, réels, points, fonctions, etc., chacun muni d'opérations et de relations qui lui sont spécifiques. Les ensembles constituent un tel type d'objet, et élaborer une théorie des ensembles signifie organiser en une suite cohérente nos connaissances sur ceux des objets mathématiques qui se trouvent être des ensembles, à la manière dont on développe une théorie des nombres ou une théorie des fonctions réelles.*
>
> *Même s'il est facile de se convaincre de l'utilité des ensembles en mathématiques, il n'est pas a priori évident qu'il soit utile ou nécessaire d'en développer une théorie. Comme on le verra, ce qui a rendu nécessaire la construction d'une théorie des ensembles, c'est l'apparition, à la fin du* XIX^{e} *siècle et au début du* XX^{e}*, de problèmes ouverts difficiles et naturels mettant en jeu les ensembles infinis. On peut alors espérer qu'une théorie cohérente les résoudra ou, au moins, les éclairera. En somme, il y a comme un rendez-vous proposé au lecteur : estimera-t-il, à la fin du livre, qu'il en sait davantage sur ces questions initiales ou, tout au moins, que l'étude ainsi développée lui aura permis de mieux comprendre l'infini en mathématiques et d'en tirer des applications ?* ◁

Cette section comporte trois sous-sections. Dans la sous-section 1.1, on rappelle la notion d'ensemble de la façon la plus élémentaire possible, avant d'en discuter l'utilité dans la sous-section 1.2, puis de rencontrer dans la sous-section 1.3 les premiers problèmes de dénombrement qui légitiment le développement d'une théorie.

1.1. La notion d'ensemble

> ▶ Résumé.— Nommer un ensemble, c'est proclamer l'existence d'un nouvel objet rassemblant des objets qui partagent une propriété. ◀

1.1.1.— Plutôt que des objets mathématiques isolés, par exemple l'entier 2 ou le réel π, il arrive que plusieurs objets soient considérés simultanément sans que l'on veuille ou puisse référer à l'un d'entre eux spécifiquement, par

exemple les solutions d'une équation, les entiers pairs ou les réels transcendants : l'usage est alors de *nommer* cette collection d'objets, donc, ce faisant, de l'introduire comme un nouvel objet mathématique. Ainsi, lorsque l'on dit : « Soit P l'ensemble des entiers pairs », à côté des entiers $0, 2, 4 \ldots$ pris individuellement, on introduit, et en particulier on nomme, un nouvel objet référant à tous ces entiers pris collectivement. On déclare alors « n appartient à P », ou encore « n est élément de P », noté $n \in P$, comme une autre façon d'exprimer que n a la propriété définissant P, ici être un nombre pair. En d'autres termes, on remplace un prédicat par son extension ou, tout au moins, on donne un nom à celle-ci.

1.1.2.— La notation traditionnelle [1] pour l'ensemble dont les éléments sont les objets x possédant une certaine propriété $\mathcal{P}(x)$ est $\{x \mid \mathcal{P}(x)\}$, et celle pour l'ensemble dont les éléments sont des objets $a_1, \ldots, a_n$ explicitement énumérés est $\{a_1, \ldots, a_n\}$. Par exemple $\{-1, 1\}$ est l'ensemble dont les deux éléments sont les entiers -1 et 1. Cet ensemble est aussi $\{1, -1\}$, et également $\{-1, 1, 1\}$, puisque seuls comptent les éléments indépendamment de tout ordre ou multiplicité. Diverses représentations graphiques sont utilisées, par exemple les diagrammes dits *de Venn* (figure 1).

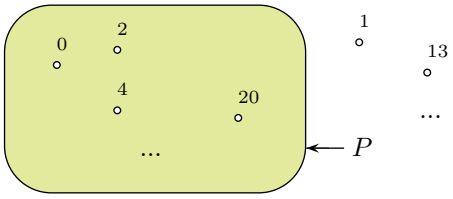


FIGURE 1.— Représentation graphique d'un ensemble par un diagramme de Venn, ici l'ensemble P des nombres pairs : un cadre entoure les éléments et les isole des non-éléments ; dans le cas présent, la représentation est forcément incomplète puisqu'il existe une infinité d'entiers.

1.1.3.— On pourrait confondre ensemble et propriété en identifiant un ensemble avec la propriété qui le définit. Ce n'est pas le point de vue adopté : l'ensemble ne retient que le résultat final, c'est-à-dire les objets sélectionnés, et non la propriété utilisée pour opérer la sélection. De la sorte, un ensemble est complètement déterminé par ses éléments, et par eux seuls (propriété dite d'*extensionnalité*) : deux propriétés équivalentes conduisent à sélectionner les mêmes objets, et elles définissent donc un seul ensemble.

▷ *Par exemple, pour un entier, être le double d'un entier est équivalent à être congru à* 0*,* 2*,* 4*,* 6*, ou* 8 *modulo* 10 *: les deux propriétés sont distinctes, mais l'ensemble qu'elles définissent est le même. Ainsi, un ensemble est associé à une classe d'équivalence de propriétés plutôt qu'à une propriété spécifique* [2].

1. Notation à laquelle on se tiendra ici ; on trouve également $\{x : \mathcal{P}(x)\}$ et $\{x\,;\mathcal{P}(x)\}$.

2. Comme il n'est pas garanti que l'équivalence des propriétés puisse être reconnue, l'égalité des ensembles ne l'est pas davantage : on introduit comme objets mathématiques abstraits des ensembles dont il peut être impossible en pratique de déterminer les éléments.

*L'approche qui sera adoptée dans la suite de ce texte est extrêmement libérale dans la mesure où les propriétés définissantes seront souvent oubliées, de sorte que des ensembles puissent être envisagés indépendamment de toute définition. Par exemple, une expression telle que « soit A un ensemble d'entiers » indiquera seulement que A est un objet tel que, pour chaque entier n, l'assertion $n \in A$ est soit vraie, soit fausse, et que A est entièrement déterminé par les entiers n qui vérifient $n \in A$, qu'une propriété explicite caractérisant ceux-ci ait été donnée ou non. Une telle approche est qualifiée d'*imprédicative*, par opposition à l'approche* prédicative *qui ne considérerait que des objets explicitement définis. Cette étape supplémentaire d'abstraction est une option, et elle est discutable : on peut estimer n'être intéressé que par des objets explicitement définis et donc considérer comme vides de sens des énoncés mettant en jeu des objets qui ne le sont pas. Le point de vue de la théorie des ensembles n'exclut pas une telle position, mais ce n'est pas celle qu'il retient — voir plus loin la discussion sur les axiomes de compréhension et des parties dans la sous-section* 3.4*, ou encore sur l'axiome du choix au chapitre* IV*.* ◁

1.2. Utilité des ensembles

▶ Résumé.— Introduire des ensembles est utile pour exprimer des propriétés collectives ne faisant pas sens pour des objets individuels. ◀

1.2.1.— La fréquence des termes « ensemble », « famille », « collection » dans les textes mathématiques récents montre que l'introduction d'ensembles est au moins une convention commode : séparer les entiers pairs des impairs permet ensuite de travailler avec ceux-ci de manière uniforme, indépendamment de la propriété utilisée pour les séparer. De plus, de nombreux objets mathématiques sont définis comme des domaines, donc des ensembles, munis d'une structure additionnelle, algébrique, topologique ... et il serait donc malcommode, au moins formellement, de se passer d'ensembles pour définir un groupe, un corps, ou une variété différentiable [3].

1.2.2.— Il y a plus important : au-delà de la commodité de formulation, l'introduction d'ensembles permet surtout de saisir des propriétés globales qui ne font pas sens pour chaque élément pris individuellement. Par exemple, affirmer que les multiples de 5 forment un sous-groupe de $\mathbb{Z}$ dit quelque chose de plus [4] que les propriétés individuelles de 10 ou -15.

Exemple. Soit à montrer qu'aucun entier n plus grand que 1 ne divise $3^n - 2^n$. Supposons, en vue d'une contradiction, que n divise $3^n - 2^n$, et soit p le plus petit facteur premier de n. Si p est 2 ou 3, alors p, donc a fortiori n, ne divise pas $3^n - 2^n$. Supposons $p \geqslant 5$. Les classes $\overline{2}$ et $\overline{3}$ de 2 et 3 dans $\mathbb{Z}/p\mathbb{Z}$ sont alors inversibles. L'ensemble $\{k \in \mathbb{Z} \mid \overline{2}^k = \overline{3}^k\}$ est un sous-groupe de $\mathbb{Z}$, et est donc de la forme $m\mathbb{Z}$ pour un certain m positif. Le petit théorème de Fermat implique l'égalité $\overline{2}^{p-1} = \overline{3}^{p-1} = \overline{1}$, donc $p - 1 \in m\mathbb{Z}$, et $m \leqslant p - 1$. Donc, m ne peut diviser n, puisque p est son plus petit facteur premier. On a donc $n \notin m\mathbb{Z}$, et p,

3. Mais on ne doit pas oublier que la plupart des résultats mathématiques démontrés avant le XX$^{\text{e}}$ siècle l'ont été sans que des ensembles y soient mentionnés formellement.

4. Mais il faut reconnaître qu'au lieu de parler du sous-groupe $5\mathbb{Z}$, donc d'un ensemble, on pourrait exprimer tous les énoncés en termes de la seule congruence *modulo* 5.

donc n, ne divise pas $3^n - 2^n$. Dans la démonstration précédente, le point essentiel est l'introduction de l'ensemble $\{k \in \mathbb{Z} \mid \bar{2}^k = \bar{3}^k\}$, et le fait que tout sous-groupe de $\mathbb{Z}$ est de la forme $m\mathbb{Z}$. On pourrait s'en passer en redémontrant le résultat dans le cas particulier, en l'occurrence en considérant le plus petit m vérifiant $\bar{2}^m = \bar{3}^m$, puis en montrant par division euclidienne que tout entier k vérifiant $\bar{2}^k = \bar{3}^k$ est multiple de m. Mais on perdrait ainsi probablement une part de la compréhension et, en tout cas, de l'économie apportées par le résultat structurel sur les sous-groupes de $\mathbb{Z}$, donc par l'introduction d'un ensemble.

1.3. Premiers résultats, premiers problèmes

▶ Résumé.— Comparer les ensembles (infinis) mène au problème du continu sur les tailles intermédiaires entre celles de $\mathbb{N}$ et de $\mathbb{R}$: l'absence d'une solution évidente motive l'élaboration d'une théorie. ◀

1.3.1.— Même si l'utilité des ensembles est tenue pour acquise, il ne va pas de soi qu'il faille en construire une théorie générale : par exemple, les suites ou les fonctions sont aussi des outils importants et pourtant la nécessité d'une théorie générale des suites ou des fonctions ne s'est pas fait ressentir [5]. Ce qui rend l'élaboration d'une théorie des ensembles nécessaire, ou, au moins, opportune, c'est l'apparition de nombreux problèmes ouverts mettant en jeu des ensembles infinis et leur classification à bijection près.

1.3.2.— La plupart des structures mathématiques vont de pair avec une notion de morphisme. Dans le cas des ensembles, comme aucune structure additionnelle n'est considérée, les morphismes naturels sont les applications, et les isomorphismes sont les bijections [6].

Définition (équipotence).— Deux ensembles A et B sont dits *en bijection*, ou *équipotents* [7], s'il existe une bijection de A sur B.

L'identité, l'inverse d'une bijection, et la composée de deux bijections sont des bijections, donc l'équipotence est une relation d'équivalence.

▷ *L'existence de bijections ou d'injections entre des ensembles formalise la notion intuitive de nombre d'éléments, donc une notion de taille. Une bijection entre deux ensembles A et B fait se correspondre un à un les éléments de A et de B, et traduit l'intuition que A et B ont la même taille. De même, une injection de A dans B établit une correspondance bijective entre A et un sous-ensemble de B, et elle traduit l'intuition que la taille de A est au plus celle de B.* ◁

5. Cependant, on pourrait dire que le lambda-calcul évoqué dans la sous-section XVI.1.3 est une théorie générale des fonctions.

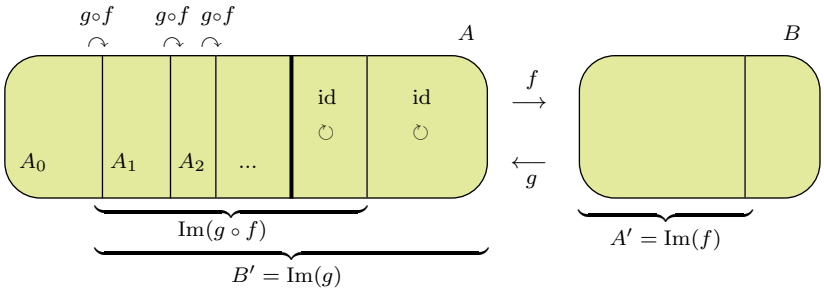
6. On rappelle la terminologie usuelle (sur laquelle on reviendra dans la section III.1.3) : une *fonction* de A dans B est une correspondance entre éléments de A et de B dans laquelle chaque élément de A a au plus une image ; de plus, elle est dite *partout définie*, ou appelée *application* de A dans B, si tout élément de A a une image ; une fonction de A dans B est dite *injective*si deux éléments distincts de A ont des images distinctes, et*surjective* si tout élément de B est image d'au moins un élément de A ; enfin une *injection* (*resp., surjection*, *resp., bijection*) de A dans B est une application de A dans B qui est injective (*resp.,* surjective, *resp.,* injective et surjective).

7. Le terme est un peu tombé en désuétude.

1.3.3.— Lier la notion intuitive de taille d'un ensemble à l'existence d'une bijection et utiliser un vocabulaire d'ordre en liaison avec l'existence d'une injection est rendu cohérent par le résultat classique suivant.

Proposition (théorème de Cantor–Bernstein).— *Si A et B sont deux ensembles et qu'il existe une injection de A dans B et une injection de B dans A, alors il existe une bijection de A sur B.*

Démonstration. (Voir aussi l'exercice 1.) Supposons que $f : A \to B$ et $g : B \to A$ sont des injections. Posons $A' = \mathrm{Im}(f)$ et $B' = \mathrm{Im}(g)$. Alors, f est une bijection de A sur A', et g une bijection de B sur B'. On va construire une bijection h de A sur B'. Pour cela, posons $A_0 := A \setminus B'$, puis, inductivement, soit A_i l'image de A_{i-1} par $g \circ f$ pour $i \geqslant 1$. L'ensemble A_0 est disjoint de A_i pour $i \geqslant 1$ car A_0 est disjoint de B' et A_i inclus dans B'. Comme la composée $(g \circ f)^j$ est injective pour tout j, les ensembles A_j et A_{j+i} sont disjoints pour tous $j \geqslant 0$ et $i \geqslant 1$. Par construction, $g \circ f$ envoie $\bigcup_{i \geqslant 0} A_i$ sur $\bigcup_{i \geqslant 1} A_i$, lequel ensemble est inclus dans B'.



Définissons alors h par

$$h(a) := g \circ f(a) \text{ si } a \text{ est dans } \bigcup_{i \geqslant 0} A_i, \quad \text{et } h(a) := a \text{ sinon.}$$

Par construction, l'image de h est B', et, d'autre part, h est injective car obtenue en recollant deux injections dont les images sont disjointes. Donc, h est une bijection de A sur B', et, finalement, $g^{-1} \circ h$ est une bijection de A sur B. □

1.3.4.— La notion duale de celle d'injection est celle de surjection. L'existence d'une injection de A dans B entraîne celle d'une surjection de B sur A : si A est non vide et si $f : A \to B$ est injective, on définit une surjection $g : B \to A$ en choisissant un élément a de A et en posant $g(b) := f^{-1}(b)$ pour b dans $\mathrm{Im}(f)$ et $g(b) := a$ sinon.

Question.— *L'existence d'une injection de A dans B est-elle équivalente à celle d'une surjection de B sur A ?*

Mis à part le cas des ensembles finis (voir 1.3.7 ci-dessous), la réponse n'est *pas* évidente, on y reviendra au chapitre IV.

1.3.5.— De nombreuses questions apparaissent lorsque les ensembles finis et infinis sont distingués. On définit ici ces notions en partant du principe qu'un ensemble fini est un ensemble dont on peut numéroter les éléments. On rappelle les notations conventionnelles : $\mathbb{N}$ désigne l'ensemble des entiers naturels (positifs ou nul), $\mathbb{Z}$ celui des entiers relatifs, $\mathbb{Q}$ celui des nombres rationnels, $\mathbb{R}$ celui des nombres réels, et $\mathbb{C}$ celui des nombres complexes.

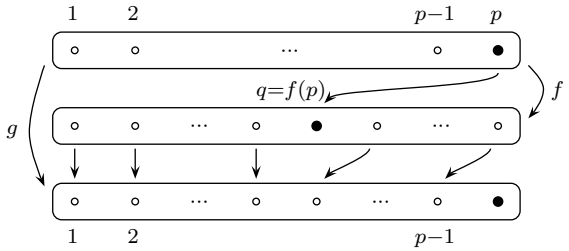
Définition (fini, infini, dénombrable).— Un ensemble est dit *fini* s'il est vide ou en bijection avec un intervalle de $\mathbb{N}$ de la forme $\{1, 2, \dots, p\}$; un ensemble qui n'est pas fini est dit *infini*. Un ensemble en bijection avec $\mathbb{N}$ est dit *dénombrable*.

▷ *La définition précédente présuppose (bien sûr !) l'existence des nombres entiers et de l'ensemble* $\mathbb{N}$ *de ces nombres. On se demandera plus loin si une définition plus intrinsèque est possible : on renvoie ici à la sous-section* III.2.3. ◁

1.3.6.— Partant de cette définition, il est facile de légitimer les propriétés usuelles des ensembles finis en utilisant le résultat technique suivant.

Lemme.— *Toute injection d'un ensemble fini dans lui-même est bijective.*

Démonstration. Il suffit de montrer le résultat pour les intervalles $\{1, \dots, p\}$. On raisonne par récurrence sur $p \geqslant 1$. Pour $p = 1$, l'intervalle $\{1, \dots, p\}$ est le singleton $\{1\}$, et la seule application de $\{1\}$ dans lui-même est l'identité, qui est une bijection. Supposons $p \geqslant 2$, et soit f une injection de $\{1, \dots, p\}$ dans lui-même. Posons $q := f(p)$. On définit une application g de $\{1, \dots, p-1\}$ dans lui-même en posant $g(i) := f(i)$ pour $f(i) < q$ et $g(i) := f(i) - 1$ pour $f(i) > q$.



Alors, g est injective puisque q n'appartient pas à l'image de $\{1, \dots, p-1\}$ par f. Par hypothèse de récurrence, g est surjective. Par construction, $\mathrm{Im}(f)$ est $\mathrm{Im}(g) \cup \{p\}$, donc on trouve finalement $\mathrm{Im}(f) = \{1, \dots, p\}$. □

1.3.7.— On en déduit le résultat principal concernant les ensembles finis.

Proposition (cardinal).— *Tout ensemble fini non vide A est en bijection avec un unique intervalle $\{1, 2, \dots, p\}$ de $\mathbb{N}$. L'entier p est appelé le* cardinal *de A, noté $\|A\|$, et 0 est appelé le cardinal de l'ensemble vide.*

Démonstration. Par définition, A est en bijection avec un intervalle $\{1, \dots, p\}$. Celui-ci est unique, puisque, pour $q < p$, une bijection de $\{1, \dots, p\}$ sur $\{1, \dots, q\}$ serait une injection non bijective de $\{1, \dots, p\}$ dans lui-même, qu'exclut 1.3.6. □

On obtient ainsi une classification complète des ensembles finis à l'aide des entiers : deux ensembles finis A, B sont en bijection si l'on a $\|A\| = \|B\|$. De même, il existe une injection de A dans B si l'on a $\|A\| \leqslant \|B\|$.

1.3.8.— Toujours pour les ensembles finis, on déduit une réponse positive à la question 1.3.4.

Corollaire (injection/surjection).— *Pour A et B finis avec A non vide, l'existence d'une injection de A dans B équivaut à celle d'une surjection de B sur A.*

Démonstration. L'existence d'une injection de A dans B équivaut à $\|A\| \leqslant \|B\|$, celle d'une surjection de B sur A à $\|B\| \geqslant \|A\|$ ... □

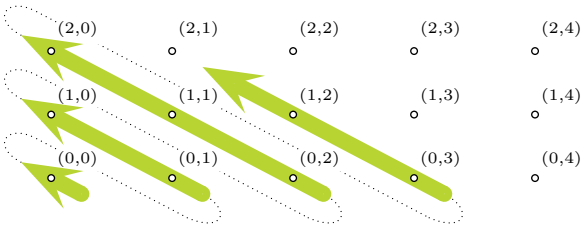
1.3.9.— On passe maintenant aux ensembles infinis, où la situation est beaucoup plus compliquée, et où des bijections, c'est-à-dire des égalités de taille, étonnantes apparaissent.

▷ *On a vu en* 1.3.6 *qu'une partie propre d'un ensemble fini est strictement plus petite que celui-ci. Par définition, ce résultat ne s'étend pas aux ensembles infinis : par exemple, l'application « successeur » qui, pour tout entier n, envoie n sur $n+1$ définit une bijection de $\mathbb{N}$ sur la partie propre de $\mathbb{N}$ composée des entiers non nuls. Autrement dit, $\mathbb{N}$ privé de 0 n'est pas plus petit que $\mathbb{N}$. De même, l'application qui, pour tout entier n, envoie n sur $2n$ définit une bijection de $\mathbb{N}$ sur l'ensemble des nombres pairs, ce qui montre que ce dernier, ne contenant pourtant qu'un entier sur deux, n'est pas plus petit que $\mathbb{N}$: la moitié de $\mathbb{N}$ n'est pas plus petite que $\mathbb{N}$.* ◁

Proposition (carré).— *Les ensembles $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$ sont en bijection.*

Démonstration. Comme tout entier non nul s'écrit de façon unique comme le produit d'une puissance de 2 et d'un entier impair, l'application $(p, q) \mapsto 2^p(2q+1)$ est une bijection de $\mathbb{N}\times\mathbb{N}$ sur $\mathbb{N}\setminus\{0\}$, donc $(p, q) \mapsto 2^p(2q+1)-1$ est une bijection de $\mathbb{N} \times \mathbb{N}$ sur $\mathbb{N}$.

Une autre bijection classique, qui suit le parcours des diagonales successives du réseau $\mathbb{N} \times \mathbb{N}$ écrit dans un quadrant comme ci-dessous



correspond à la formule polynomiale[8] $(p, q) \mapsto (p + q)(p + q + 1)/2 + q$. □

8. Polya a montré que le polynôme indiqué et son symétrique sont les seuls polynômes de degré au plus 2 établissant une bijection entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$.

1.3.10.— Les résultats suivants relèvent de la même famille.

Corollaire (bijections).— (i) *Les ensembles* $\mathbb{N}$, $\mathbb{Z}$, *et* $\mathbb{Q}$ *sont en bijection.*
(ii) *Les ensembles* $\mathfrak{P}(\mathbb{N})$ *et* $\mathfrak{P}(\mathbb{N}) \times \mathfrak{P}(\mathbb{N})$ *sont en bijection.*

Démonstration. (i) Une bijection de $\mathbb{N}$ sur $\mathbb{Z}$ s'obtient directement en posant
$$2n \mapsto n, \quad 2n+1 \mapsto -n-1.$$
Ensuite, $\mathbb{N}$ s'injecte dans $\mathbb{Q}$, tandis que $\mathbb{Q}$ s'injecte dans $\mathbb{Z} \times \mathbb{Z}$, donc, de là, dans $\mathbb{N} \times \mathbb{N}$, puis, par 1.3.9, dans $\mathbb{N}$. On conclut que $\mathbb{Q}$ et $\mathbb{N}$ sont en bijection par le théorème de Cantor–Bernstein.
(ii) Une bijection de $\mathfrak{P}(\mathbb{N})$ sur $\mathfrak{P}(\mathbb{N}) \times \mathfrak{P}(\mathbb{N})$ s'obtient en posant
$$X \mapsto (\{p \mid 2p \in X\}, \{q \mid 2q+1 \in X\}).$$ □

1.3.11.— Utilisant ici la notation A^B pour l'ensemble des applications de B dans A, nous obtenons de nouvelles bijections. On notera que le théorème de Cantor–Bernstein simplifie les démonstrations en remplaçant la construction d'une bijection par celle de deux injections indépendantes.

Proposition (réels).— *Les ensembles* $\mathfrak{P}(\mathbb{N})$, $\mathbb{R}$, $\mathbb{N}^{\mathbb{N}}$, *et* $\{0,1\}^{\mathbb{N}}$ *sont deux à deux en bijection.*

Démonstration. Par le théorème de Cantor–Bernstein, il suffit de construire des injections formant un cycle reliant les quatre ensembles. Or, envoyer une partie A de $\mathbb{N}$ sur le réel $\sum_{i \in A} 3^{-i}$ fournit une injection de $\mathfrak{P}(\mathbb{N})$ dans $\mathbb{R}$ (le choix de la base 3 plutôt que 2 garantissant l'unicité des développements considérés).
Ensuite, pour x réel, notons $\mathrm{sgn}(x)$ l'entier 1 pour $x \geqslant 0$ et 0 sinon, $E(x)$ la partie entière de $|x|$, et posons $d_i(x) := E(2^i|x|)$. Envoyer x sur la suite
$$(\mathrm{sgn}(x), E(x), d_1(x), d_2(x), \ldots)$$
définit une injection de $\mathbb{R}$ dans $\mathbb{N}^{\mathbb{N}}$.
Pour f fonction de $\mathbb{N}$ dans $\mathbb{N}$, notons $S(f)$ le mot infini $1^{f(0)}01^{f(1)}01^{f(2)}0\ldots$, où 1^n signifie $11\cdots1$ avec 1 répété n fois. Envoyer f sur la fonction de $\mathbb{N}$ dans $\{0,1\}$ dont la valeur en i est la $i^{\text{ième}}$ lettre du mot $S(f)$ définit une injection de $\mathbb{N}^{\mathbb{N}}$ dans $\{0,1\}^{\mathbb{N}}$.
Enfin, envoyer une fonction f de $\mathbb{N}$ dans $\{0,1\}$ sur l'ensemble des entiers i vérifiant $f(i) = 1$ définit une injection de $\{0,1\}^{\mathbb{N}}$ dans $\mathfrak{P}(\mathbb{N})$. □

En composant les résultats, on déduit par exemple que le produit $\mathbb{R} \times \mathbb{R}$ est en bijection avec $\mathbb{R}$, puis qu'il en est de même de toute puissance finie $\mathbb{R}^n$.

1.3.12.— À ce point, on peut se demander si *tous* les ensembles infinis sont deux à deux en bijection, c'est-à-dire s'il existe plusieurs infinis distincts. Due à Georg Cantor, la réponse, négative, est le point « zéro » de la théorie des ensembles, l'événement primordial d'où procède toute la suite.

Proposition (argument diagonal).— *L'ensemble* $\mathbb{R}$ *des nombres réels n'est pas en bijection avec l'ensemble* $\mathbb{N}$ *des nombres entiers.*

Démonstration. Il suffit de montrer que l'intervalle $[0,1]$ n'est pas en bijection avec $\mathbb{N}$. Or, soit A l'ensemble des nombres réels compris entre 0 et 1 dont un développement en base 3 ne contient que des 0 et des 1, et soit f une fonction quelconque de $\mathbb{N}$ dans A. On montre qu'il existe au moins un réel dans A distinct de chacun des réels $f(0)$, $f(1)$, ... et donc que f n'est pas surjective, ni *a fortiori* bijective. Pour cela, écrivons le développement en base 3 de $f(i)$ sous la forme $0, a_{i,0}a_{i,1}...$, où les chiffres $a_{i,j}$ sont 0 ou 1. Posons $\bar{0} = 1$, $\bar{1} = 0$, et soit a le réel dont le développement est $0, \overline{a_{0,0}}\ \overline{a_{1,1}}\ \overline{a_{2,2}}...$. Alors, a, qui est dans A par construction, ne peut être, quel que soit i, égal à $f(i)$, car le $i^{\text{ième}}$ chiffre du développement de $f(i)$ est $a_{i,i}$, alors que celui de a est $\overline{a_{i,i}}$, et que le développement en base 3 sans chiffre 2 est unique quand il existe. Donc, f n'est pas surjective. □

▷ *Conjuguant autoréférence (ici les éléments diagonaux $a_{i,i}$) et négation (ici l'application « barre »), la démonstration précédente repose sur ce qui est appelé l'*argument diagonal. *Le recours à la base 3 plutôt que 2 n'est là que pour pallier le défaut d'unicité du développement binaire pour les rationnels dyadiques.* ◁

1.3.13.— Eu égard à l'existence d'une bijection entre $\mathbb{R}$ et $\mathfrak{P}(\mathbb{N})$, une autre démonstration de 1.3.12 est fournie par le résultat suivant, également dû à Cantor et reposant à nouveau sur un argument diagonal.

Proposition (théorème de Cantor).— *Il n'existe pas de surjection d'un ensemble A sur $\mathfrak{P}(A)$, ni d'injection de $\mathfrak{P}(A)$ dans A ; en particulier, les ensembles A et $\mathfrak{P}(A)$ ne sont pas en bijection.*

Démonstration. Soit $f : A \to \mathfrak{P}(A)$ une application quelconque. Posons
$$B := \{a \in A \mid a \notin f(a)\}.$$
Si un élément a de A est dans B, alors par définition a est dans $B \setminus f(a)$, donc il est impossible que $f(a)$ soit égal à B. D'un autre côté, si un élément a de A n'est pas dans B, alors par définition a est dans $f(a) \setminus B$ donc, à nouveau, il est impossible que $f(a)$ soit égal à B. Par conséquent, la seule possibilité est que B n'appartienne pas à l'image de f, et que f ne soit pas surjective. Il n'existe donc pas de surjection de A sur $\mathfrak{P}(A)$, et donc en particulier pas de bijection de A sur $\mathfrak{P}(A)$. Enfin, comme l'application $a \mapsto \{a\}$ définit une injection de A dans $\mathfrak{P}(A)$, s'il existait une injection de $\mathfrak{P}(A)$ dans A, on déduirait du théorème de Cantor–Bernstein l'existence d'une bijection de A sur $\mathfrak{P}(A)$, qui ne se peut. □

Noter que, dans le cas d'un ensemble fini de cardinal n, le théorème revient à l'inégalité $2^n > n$.

1.3.14.— Le résultat de 1.3.13 est plus général que celui de 1.3.12 et, en particulier, il implique l'existence d'une infinité d'ensembles infinis deux à deux non équipotents.

Corollaire (infinité d'infinis).— *Les ensembles infinis $\mathbb{N}$, $\mathfrak{P}(\mathbb{N})$, $\mathfrak{P}(\mathfrak{P}(\mathbb{N}))$, $\mathfrak{P}(\mathfrak{P}(\mathfrak{P}(\mathbb{N})))$, ... sont deux à deux non en bijection.*

1.3.15.— Revenant à l'ensemble $\mathbb{R}$, on a vu que sa taille est strictement supérieure à celle de l'ensemble $\mathbb{N}$. Parmi les sous-ensembles infinis de $\mathbb{R}$, certains sont en bijection avec $\mathbb{N}$, par exemple $\mathbb{N}$ lui-même, d'autres sont en bijection avec $\mathbb{R}$, par exemple $\mathbb{R}$ lui-même. Le problème suivant apparaît donc immédiatement.

Question (problème du continu).— *Tout sous-ensemble infini de $\mathbb{R}$ est-il en bijection soit avec $\mathbb{N}$, soit avec $\mathbb{R}$?*

Une réponse positive est appelée l'*hypothèse du continu*, abrégée en HC.

▷ *Soulevée par Cantor en 1878, la question est celle de l'existence de tailles intermédiaires entre celle de $\mathbb{N}$ (le* dénombrable*) et celle de $\mathbb{R}$ (traditionnellement appelée le* continu*). Comme on va l'expliquer dans la suite de ce livre, plus de cent quarante ans après que Cantor l'a soulevé, le problème du continu reste non résolu à ce jour. On verra néanmoins qu'un grand nombre de résultats partiels ont été démontrés, et que le problème a joué un rôle fondamental dans le développement de la théorie des ensembles, dont il est le cœur.* ◁

1.3.16.— Le problème du continu est une question extrêmement naturelle dès que l'existence des ensembles $\mathbb{N}$ et $\mathbb{R}$ est posée. L'important ici est qu'il répond à la question qui donne son titre à cette sous-section.

S'il faut développer une théorie des ensembles, c'est parce que le problème du continu — et d'autres problèmes similaires sur les ensembles infinis — se posent, et qu'il faut les résoudre.

▷ *Bien entendu, on peut discuter du caractère bien posé ou non du problème du continu, de son importance ou non vis-à-vis du reste des mathématiques, de la signification d'une éventuelle solution : nous y reviendrons plus loin en détail. Pour le moment, on peut dans tous les cas garder en mémoire que des problèmes ardus apparaissent dès que l'on commence à comparer les tailles des ensembles infinis, et considérer que c'est une raison suffisante pour essayer d'élaborer une théorie cohérente de tels objets : la difficulté des problèmes ne garantit pas la pertinence de la théorie, mais, au moins, elle lui fournit une motivation.* ◁

1.3.17.— On mentionne maintenant quelques questions élémentaires sur lesquelles on reviendra au chapitre IV, et dont on verra plus loin que, contrairement au problème du continu, elles ont trouvé des solutions pouvant être considérées comme optimales. D'abord, l'existence d'une bijection entre $\mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$, et entre $\mathbb{R}$ et $\mathbb{R} \times \mathbb{R}$, rend la question suivante naturelle.

Question.— *Tout ensemble infini A est-il en bijection avec $A \times A$?*

1.3.18.— Ensuite, s'il existe une injection f de $\mathbb{N}$ dans un ensemble A, alors A est nécessairement infini, car l'application envoyant $f(n)$ sur $f(n+1)$ pour tout n et laissant fixes les éléments hors de $\mathrm{Im}(f)$ est une injection non surjective de A dans lui-même. Il est naturel de considérer la réciproque.

Question.— *Existe-t-il une injection de* $\mathbb{N}$ *dans tout ensemble infini ?*

1.3.19.— Enfin, on termine avec un problème ne mettant pas en jeu la taille des ensembles, mais simplement le fait de savoir s'ils sont vides ou non. On a utilisé ci-dessus le produit de deux ensembles A_1, A_2, défini comme ensemble des couples (a_1, a_2) avec $a_1 \in A_1$ et $a_2 \in A_2$. La notion s'étend naturellement à une famille quelconque d'ensembles.

Définition (produit).— Si $(A_i)_{i\in I}$ est une famille d'ensembles, le *produit* $\prod_{i\in I} A_i$ est l'ensemble des suites $(a_i)_{i\in I}$ vérifiant $\forall i\,(a_i \in A_i)$.

1.3.20.— Si $A_1, \dots, A_n$ sont des ensembles non vides, le produit $A_1 \times \cdots \times A_n$ est non vide, car, en choisissant un élément a_1 de A_1, puis un élément a_2 de A_2, et ainsi de suite jusqu'à a_n dans A_n, on obtient un n-uplet $(a_1, \dots, a_n)$ qui, par définition, est dans le produit $A_1 \times \cdots \times A_n$. Dans le cas d'une famille infinie $(A_i)_{i\in I}$, la répétition du choix d'un élément une infinité de fois est une opération d'un type différent dont la validité n'est pas claire, et l'argument précédent ne s'adapte pas.

Question.— *Tout produit d'ensembles non vides est-il non vide ?*

Aucune des questions ci-dessus n'admet de réponse immédiate, et chacune contribue donc à motiver une étude plus avancée.

2. Opérations ensemblistes

De même que d'une notion de morphisme, chaque type d'objet mathématique est accompagné d'opérations et de relations qui lui sont propres. Dans le cas des ensembles, plusieurs opérations et relations s'introduisent naturellement : réunion [9], intersection, différence, inclusion, ... Dans cette brève partie, on étudie les propriétés algébriques, au demeurant simples, de ces opérations dites ensemblistes.

> ▷ *Une approche naïve pourrait faire penser que les opérations ensemblistes sont le cœur de la théorie des ensembles, et que cette dernière consiste surtout à manipuler des expressions compliquées à base de* $\cup$ *et de* $\cap$. *Ce n'est* pas *le cas : au moins dans le cas fini, les propriétés des opérations ensemblistes sont complètement décrites par le fait qu'elles définissent une algèbre de Boole, c'est-à-dire*

9. Utilisé en anglais et plus court, le mot « union » tend souvent à remplacer « réunion », qui est traditionnel en français mais ne se justifie pas.

obéissent à une certaine famille (finie) de lois algébriques explicites qui les caractérisent de façon exhaustive, et il n'y a guère de mystères à attendre de la seule manipulation de ces opérations. Bien entendu, cela n'est pas dire que la combinatoire des ensembles finis est une affaire triviale, mais c'est dire que, d'un point de vue de théorie des ensembles, les ensembles finis n'offrent pas de grand problème : résolument, la théorie des ensembles sera une théorie des ensembles infinis … ◁

Cette section comporte trois courtes sous-sections. Dans la sous-section 2.1, on observe que tout ensemble des parties a une structure de treillis, puis d'algèbre de Boole. Dans la sous-section 2.2, on axiomatise les algèbres de Boole en tant que structures algébriques. Finalement, on établit dans la sous-section 2.3 qu'inversement toute algèbre de Boole finie est de ce type, ce qui, en un sens, clôt, du point de vue de la théorie des ensembles, l'étude des ensembles finis.

2.1. Le treillis des parties d'un ensemble

► Résumé.— L'inclusion est une relation d'ordre dont la restriction à tout ensemble $\mathfrak{P}(A)$ est un treillis distributif et complémenté. ◄

2.1.1.— Diverses relations et opérations simples dérivent directement de la relation d'appartenance : inclusion, réunion, intersection, différence, *etc.* On commence par rappeler les définitions usuelles.

Définition (inclusion, parties, opérations ensemblistes).— (i) Si A et B sont des ensembles, on dit que A est *inclus* dans B, ou encore que A est un *sous-ensemble* ou une *partie* de B, noté [10] $A \subseteq B$, si tout élément de B est élément de A. On note $\mathfrak{P}(A)$ l'ensemble [11] des parties de A.

(ii) On pose

$A \cup B := \{x \mid x \in A \text{ ou } x \in B\}$, *réunion* de A et B,
$A \cap B := \{x \mid x \in A \text{ et } x \in B\}$, *intersection* de A et B,
$A \setminus B := \{x \in A \mid x \notin B\}$, *différence* de A et B,
$A \vartriangle B := (A \setminus B) \cup (B \setminus A)$, *différence symétrique* de A et B.

(iii) Si un ensemble de référence Ω est fixé, le *complémentaire* de A est défini par $A^c := \Omega \setminus A$.

2.1.2.— On se propose d'étudier les propriétés de la relation $\subseteq$, ainsi que les lois algébriques auxquelles les diverses opérations ensemblistes obéissent.

Lemme.— *La relation d'inclusion est une relation d'ordre.*

10. La notation « ordre large » est plus cohérente que $\subset$, qui suggère un ordre strict.
11. On reviendra plus loin sur l'existence d'un tel ensemble lorsque A est infini ; pour le moment, on se contente d'introduire la terminologie et d'explorer les propriétés algébriques élémentaires des opérations dérivées.

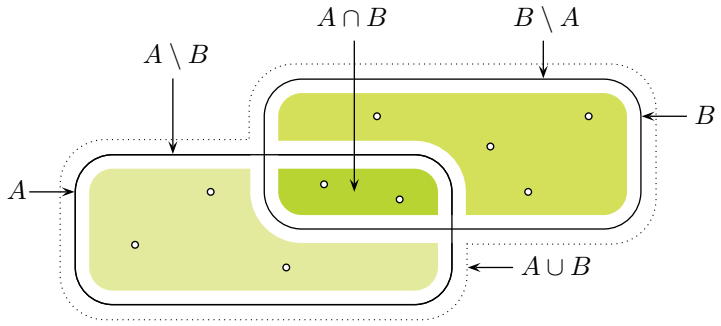


FIGURE 2.— Opérations ensemblistes représentées à l'aide des diagrammes de Venn de la figure 1.

Démonstration. La réflexivité et la transitivité sont immédiates. L'antisymétrie provient de ce qui sera appelé plus loin la propriété d'extensionnalité, à savoir l'affirmation que deux ensembles ayant les mêmes éléments coïncident. □

2.1.3.— La notion de treillis est pertinente pour en dire davantage.

Définition (treillis, algèbre de Boole).— Un *treillis* est un ensemble ordonné tel que chaque paire d'éléments possède une borne supérieure et une borne inférieure. Un treillis est *distributif* si l'opération sup est distributive par rapport à l'opération inf, et *vice versa* ; il est *complémenté* s'il possède un minimum 0, un maximum 1 et si, pour tout x, il existe un élément x^c, appelé *complément* de x, vérifiant $\sup(x, x^c) = 1$ et $\inf(x, x^c) = 0$. Une *algèbre de Boole* est un treillis distributif et complémenté.

Exemple. L'ensemble des entiers non nuls muni de la relation de divisibilité est un treillis distributif avec un élément minimum 1 *mais pas d'élément maximum, et ce n'est donc pas une algèbre de Boole. En revanche, l'ensemble des diviseurs d'un entier fixé n'ayant que des facteurs premiers simples est une algèbre de Boole.*

Dans une algèbre de Boole, le complément est unique (exercice 2).

2.1.4.— Le résultat suivant sur l'inclusion est alors classique.

Proposition (algèbre de Boole).— *Pour tout ensemble A, l'ensemble $\mathfrak{P}(A)$ muni de $\subseteq$ est une algèbre de Boole ; l'opération* sup *est la réunion, l'opération* inf *est l'intersection, le minimum est l'ensemble vide, le maximum est A, et le complément est le complémentaire.*

Démonstration. Une vérification directe est facile.

Une démonstration alternative plus rapide consiste à remarquer que les algèbres de Boole sont définies par l'obéissance à des lois algébriques (voir paragraphe suivant), d'où il résulte que tout produit d'algèbres de Boole est une algèbre de Boole. Or, définissons un ordre $\leqslant$ sur $\{0, 1\}$ en posant $0 < 1$. Alors, $(\{0, 1\}, \leqslant)$ est une algèbre de Boole. Maintenant, l'application $F : \mathfrak{P}(A) \to \{0, 1\}^A$ associant à

toute partie X sa fonction indicatrice $\mathbf{1}_X$ définie par $\mathbf{1}_X(x) := 1$ pour $x \in X$ et $\mathbf{1}_X(x) := 0$ pour $x \notin X$ induit un isomorphisme entre les structures
$(\mathfrak{P}(A), \subseteq, \cup, \cap, \emptyset, A, {}^c)$ et $(\{0,1\}, \leqslant, \sup, \inf, 0, 1, x \mapsto 1-x)^{\|A\|}$.
La première est donc une algèbre de Boole puisque la seconde l'est. □

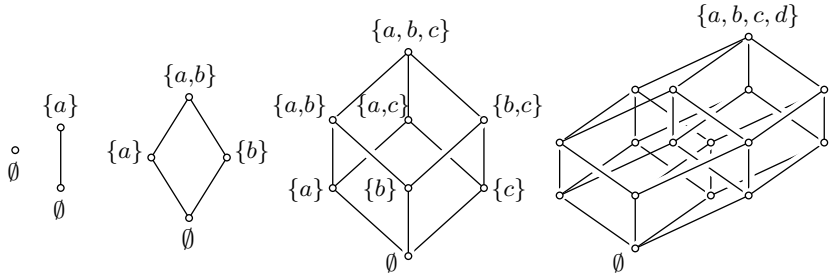


FIGURE 3.— Diagramme de Hasse des algèbres de Boole $(\mathfrak{P}(A), \subseteq)$ pour $\|A\| \leqslant 4$: les sommets sont les éléments, et une arête (ici supposée orientée de bas en haut) relie chaque élément à ses successeurs immédiats. Comme $(\mathfrak{P}(A), \subseteq)$ est isomorphe à $(\{0,1\}, \leqslant)^{\|A\|}$, le diagramme est un cube de dimension $\|A\|$.

2.2. Les algèbres de Boole comme structures algébriques

▶ Résumé.— Les algèbres de Boole sont axiomatisées par les lois algébriques auxquelles obéissent leurs opérations sup et inf. ◀

2.2.1.— Définie en termes de relation d'ordre, la structure de treillis peut également être caractérisée par les lois algébriques auxquelles obéissent les opérations de bornes supérieure et inférieure.

Proposition (axiomatisation I).— (i) *Supposons que $(T, \leqslant)$ est un treillis. Pour a, b dans B, posons $a \vee b := \sup(a,b)$ et $a \wedge b := \inf(a,b)$. Alors, la structure $(T, \vee, \wedge)$ obéit aux lois*

$$\begin{array}{cccc} x \vee x = x & (I_0) & x \wedge x = x & (I'_0) \\ x \vee y = y \vee x & (I_1) & x \wedge y = y \wedge x & (I'_1) \\ x \vee (y \vee z) = (x \vee y) \vee z & (I_2) & x \wedge (y \wedge z) = (x \wedge y) \wedge z & (I'_2) \\ x \vee (x \wedge y) = x & (I_3) & x \wedge (x \vee y) = x & (I'_3) \end{array}$$

De plus, $a \leqslant b$ est équivalent à $a \vee b = b$ et à $a \wedge b = a$.

(ii) *Inversement, supposons que $(T, \vee, \wedge)$ obéit aux lois (I_1), (I_2), (I_3), et (I'_1), (I'_2), (I'_3). Pour a, b dans T, notons $a \leqslant b$ pour $a \vee b = b$. Alors, $(T, \leqslant)$ est un treillis, et $\vee$ (resp., $\wedge$) en est l'opération* sup (*resp.,* inf).

Démonstration. (i) Pour a, b, c dans T, on a $\sup(a,a) = a$, $\sup(a,b) = \sup(b,a)$ et $\sup(a, \sup(b,c)) = \sup(a,b,c)$, donc $\sup(a, \sup(b,c)) = \sup(\sup(a,b), c)$. De plus, $a \leqslant b$ équivaut à $\sup(a,b) = b$, et à $\inf(a,b) = a$. Comme on a toujours $a \leqslant \sup(a,b)$, on a donc $\inf(a, \sup(a,b)) = a$, et de même, $\inf(a,b) \leqslant a$ entraîne $\sup(a, \inf(a,b)) = a$. Les lois (I_0), (I_1), (I_2), (I_3) et (I'_3) sont donc obéies, et (I'_0), (I'_1) et (I'_2) sont obtenues par un argument symétrique.

(ii) Notons d'abord que les opérations $\vee$ et $\wedge$ sont idempotentes, c'est-à-dire que les lois (I_0) et (I'_0) sont conséquences de $(I_1), \dots, (I'_3)$. Soit a quelconque. Par (I_3) et (I'_3), nous avons $a = a \vee (a \wedge (a \vee a)) = a \vee a$, et aussi $a \wedge (a \vee (a \wedge a)) = a \wedge a$.

On montre d'abord que $\leqslant$ est une relation d'ordre. On a en effet $a \vee a = a$ pour tout a dans T, donc $a \leqslant a$, et $\leqslant$ est réflexive. Supposons $a \leqslant b$ et $b \leqslant a$. Appliquant la commutativité de $\vee$, on obtient $a = b \vee a = a \vee b = b$, et $\leqslant$ est antisymétrique. Supposons $a \leqslant b \leqslant c$. Appliquant l'associativité de $\vee$, on obtient

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c,$$

donc $a \leqslant c$, et $\leqslant$ est transitive.

Montrons ensuite que l'élément $a \vee b$ est borne supérieure de a et b vis-à-vis de $\leqslant$. D'abord on a $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, donc

$$a \leqslant a \vee b, \text{ et } b \vee (a \vee b) = b \vee (b \vee a) = (b \vee b) \vee a = b \vee a = a \vee b,$$

donc $b \leqslant a \vee b$, et $a \vee b$ est un majorant commun à a et b. Supposons ensuite que c est un majorant commun à a et b. On a donc $a \vee c = c$ et $b \vee c = c$, donc $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$, soit $a \vee b \leqslant c$, et on conclut que $a \vee b$ est le plus petit de tous les majorants communs à a et b.

Montrons maintenant que $a \leqslant b$, c'est-à-dire $a \vee b = b$, est équivalent à $a \wedge b = a$. Supposons $a \vee b = b$. Par (I'_4), nous avons alors $a \wedge b = a \wedge (a \vee b) = a$. Inversement, supposons $a \wedge b = a$. Par (I_2) et (I_4), nous avons $a \vee b = (a \wedge b) \vee b = b \vee (b \wedge a) = b$.

Dès lors que $\vee$ et $\wedge$ jouent des rôles symétriques par rapport à l'ordre $\leqslant$, le raisonnement montrant que $a \vee b$ est borne supérieure de a et b montre *ipso facto* que $a \wedge b$ est borne inférieure de a et b, et on conclut que $(T, \leqslant)$ est un treillis. □

2.2.2.— Il existe une semblable axiomatisation pour les algèbres de Boole.

Proposition (axiomatisation II).— (i) *Supposons que* $(B, \leqslant)$ *est une algèbre de Boole de minimum* 0 *et de maximum* 1. *Pour* $a, b \in B$, *posons* $a \vee b := \sup(a, b)$, $a \wedge b := \inf(a, b)$, *et notons* $\bar{a}$ *l'unique élément vérifiant* $a \vee \bar{a} = 1$ *et* $a \wedge \bar{a} = 0$. *Alors,* $(B, \vee, \wedge, 0, 1, {}^-)$ *obéit aux lois* $(I_0), \dots, (I'_3)$ *de* 2.2.1 *et, de plus,*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \ (I_4) \qquad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), \ (I'_4)$$
$$x \vee 0 = x, \quad x \vee 1 = 1, \ (I_5) \qquad x \wedge 0 = 0, \quad x \wedge 1 = x, \ (I'_5)$$
$$x \vee \bar{x} = 1, \ (I_6) \qquad x \wedge \bar{x} = 0. \ (I'_6)$$

(ii) *Inversement, supposons que* $(B, \vee, \wedge, 0, 1, {}^-)$ *obéit aux lois* $(I_1), \dots, (I'_6)$. *Notons* $a \leqslant b$ *pour* $a \vee b = b$. *Alors,* $(B, \leqslant)$ *est une algèbre de Boole,* $\vee$ (*resp.,* $\wedge$) *est l'opération* sup (*resp.,* inf) *associée,* 1 (*resp.,* 0) *est le maximum* (*resp., le minimum*).

Démonstration. D'abord $(B, \leqslant)$ est un treillis, donc les lois $(I_0), \dots, (I'_3)$ sont obéies dans B, et, réciproquement, dès lors que $(I_1), \dots, (I'_3)$ sont obéies, on sait par 2.2.1 que $(B, \leqslant)$ est un treillis. Ensuite, (I_4) et (I'_4) traduisent directement le fait que le treillis est distributif, (I_5) et (I'_5) traduisent le fait que 0 est minimum et 1 est maximum, et (I_6) et (I'_6) le fait que $\bar{a}$ est un complément pour a. □

De là, on appelle algèbre de Boole aussi bien un treillis distributif et complémenté qu'une structure $(B, \vee, \wedge, 0, 1, {}^-)$ obéissant aux lois $(I_0), \dots, (I'_6)$.

2.2.3.— On conclut avec une autre caractérisation des algèbres de Boole, à nouveau à l'aide de lois algébriques, mais dans le langage des anneaux.

Définition (anneau de Boole).— On appelle *anneau de Boole* un anneau commutatif et idempotent, c'est-à-dire un anneau dont la multiplication est commutative et où, pour tout x, on a $x^2 = x$.

2.2.4.— Il est facile de vérifier que, pour tout ensemble A, l'ensemble $\mathfrak{P}(A)$ muni des opérations $\vartriangle$ et $\cap$ est un anneau de Boole. Ce résultat est un cas particulier du résultat général d'équivalence entre algèbre de Boole et anneau de Boole. La démonstration est une vérification facile (exercice 7).

Proposition (équivalence).— (i) *Si* $(B, \vee, \wedge, 0, 1, \bar{\ })$ *est une algèbre de Boole, alors, si l'on pose* $a \vartriangle b := (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$*, la structure* $(B, \vartriangle, \wedge)$ *est un anneau de Boole.*

(ii) *Inversement, si* $(B, +, \cdot)$ *est un anneau de Boole, alors, si l'on pose* $a \vee b := a + b + ab$*,* $a \wedge b := ab$*, et* $\bar{a} := 1 + a$*, la structure* $(B, \vee, \wedge, 0, 1, \bar{\ })$ *est une algèbre de Boole.*

2.3. Algèbres de Boole finies

▶ Résumé.— Toute algèbre de Boole finie est isomorphe à une algèbre du type $(\mathfrak{P}(A), \subseteq)$. ◀

2.3.1.— On a vu en 2.1.4 que toute structure du type $(\mathfrak{P}(A), \subseteq)$ est une algèbre de Boole. On va maintenant établir une réciproque partielle en montrant que toute algèbre de Boole *finie* est isomorphe à une algèbre du type $(\mathfrak{P}(A), \subseteq)$, obtenant ainsi une axiomatisation complète des opérations ensemblistes dans le cas fini. Le point de départ est la notion d'atome.

Définition (atome).— Si $\leqslant$ est une relation d'ordre sur un ensemble A possédant un minimum 0, un *atome* de $(A, \leqslant)$ est un successeur immédiat de 0, c'est-à-dire un élément a de A vérifiant [12] $0 < a$, mais tel qu'il n'existe pas d'élément b vérifiant $0 < b < a$.

2.3.2.— On peut alors établir le résultat de représentation des algèbres de Boole finies comme algèbres de parties d'un ensemble.

▷ *Dans une algèbre de Boole de type* $(\mathfrak{P}(A), \subseteq)$*, les atomes sont les singletons, et, par conséquent, tout élément est réunion, c'est-à-dire borne supérieure, d'atomes. Si toute algèbre de Boole finie est isomorphe à une algèbre de type* $\mathfrak{P}(A)$*, tout élément doit être borne supérieure d'atomes, ce qui rend la démonstration ci-dessous naturelle.* ◁

12. Où $a < b$ signifie « $a \leqslant b$ et $a \neq b$ », voir convention II.1.1.3 au chapitre II.

Proposition (algèbres de Boole finies).— *Toute algèbre de Boole finie est isomorphe à une algèbre du type* $(\mathfrak{P}(A), \subseteq)$.

Démonstration. On suppose que $(B, \vee, \wedge, 0, 1, \bar{}\,)$ est une algèbre de Boole finie. Soit A l'ensemble des atomes de B (dont on ne sait pas *a priori* s'il est non vide). On définit $F : B \to \mathfrak{P}(A)$ par $F(b) = \{a \in A \mid a \leqslant b\}$. On va montrer que F établit l'isomorphisme cherché de $(B, \vee, \wedge, 0, 1, \bar{}\,)$ sur $(\mathfrak{P}(A), \cup, \cap, \emptyset, A, {}^c)$. Notons déjà que, par construction, on a $F(0) = \emptyset$ et $F(1) = A$.

Montrons d'abord que $b \neq 0$ entraîne $F(b) \neq \emptyset$. En effet, soit $(b_0 = b, b_1, b_2, ...)$ une chaîne strictement décroissante partant de b et de longueur maximale. Les éléments b_i sont deux à deux distincts, donc la longueur de la chaîne est au plus le cardinal de B. Il existe donc n vérifiant $b_n = 0$. L'élément b_{n-1}, qui est un minorant de b par construction, est alors un atome de B. En effet, s'il existait c vérifiant $0 < c < b_{n-1}$, la chaîne $(b_0, b_1, ..., b_{n-1}, c, b_n)$ contredirait la maximalité de $(b_0, b_1, ..., b_{n-1}, b_n)$.

Soit b quelconque dans B. Soit a un atome. Si a minorait à la fois b et $\bar{b}$, il minorerait $b \wedge \bar{b}$, qui est 0, ce qui est impossible, donc $F(b)$ et $F(\bar{b})$ sont disjoints. D'un autre côté, supposons $a \notin F(b)$, c'est-à-dire $a \not\leqslant b$. On a $a \wedge b \leqslant a$ et $a \wedge b \neq a$ (sinon on aurait $a \leqslant b$), donc, par définition d'un atome, $a \wedge b = 0$. On obtient

$$a = a \wedge 1 = a \wedge (b \vee \bar{b}) = (a \wedge b) \vee (a \wedge \bar{b}) = 0 \vee (a \wedge \bar{b}) = a \wedge \bar{b},$$

donc $a \leqslant \bar{b}$. Par conséquent, $a \notin F(b)$ entraîne $a \in F(\bar{b})$, et on déduit $F(\bar{b}) = F(b)^c$.

Soient b et c quelconques dans B. Par définition de la borne inférieure, un atome minore $b \wedge c$ si, et seulement si, il minore b et minore c, d'où $F(b \wedge c) = F(b) \cap F(c)$. Appliquant cela à $\bar{b}$ et $\bar{c}$, ainsi que l'égalité $F(\bar{x}) = F(x)^c$, nous obtenons

$$\begin{aligned} F(b \vee c) = F(\overline{\bar{b} \vee \bar{c}})^c = F(\bar{b} \wedge \bar{c})^c &= (F(\bar{b}) \cap F(\bar{c}))^c \\ &= F(\bar{b})^c \cup F(\bar{c})^c = F(b) \cup F(c). \end{aligned}$$

À ce point, on a donc montré que F est un homomorphisme de $(B, \vee, \wedge, 0, 1, \bar{}\,)$ dans $(\mathfrak{P}(A), \cup, \cap, \emptyset, A, {}^c)$. Il reste à montrer que F est bijectif. Soient b et c deux éléments distincts de B. L'une au moins des deux relations $b \leqslant c$, $c \leqslant b$ est fausse. Supposons par exemple $b \not\leqslant c$, donc $b \neq b \wedge c$. Comme on a $b = b \wedge 1 = b \wedge (c \vee \bar{c}) = (b \wedge c) \vee (b \wedge \bar{c})$, on doit avoir $b \wedge \bar{c} \neq 0$, donc $F(b \wedge \bar{c}) \neq \emptyset$. Il existe donc un atome a minorant b et $\bar{c}$, donc ne minorant pas c, c'est-à-dire appartenant à $F(b)$ et non à $F(c)$: ces ensembles sont donc distincts, et F est injectif.

Finalement, soit X un sous-ensemble quelconque de A. Puisque B est fini, A l'est aussi, et on peut écrire $X = \{a_1, ..., a_n\}$. Posons $b = a_1 \vee \cdots \vee a_n$ (comme $\vee$ est une opération associative, il n'y a pas d'ambiguïté à supprimer les parenthèses). Soit a un atome quelconque. La distributivité de $\wedge$ vis-à-vis de $\vee$ implique l'égalité $a \wedge b = (a \wedge a_1) \vee \cdots \vee (a \wedge a_n)$: si a est l'un des a_i, on obtient $a \wedge b = a$, soit $a \leqslant b$, ou $a \in F(b)$; sinon, on obtient $a \wedge b = 0$, donc $a \notin F(b)$. On déduit donc $F(b) = X$, et F est surjective. □

2.3.3.— Le résultat de 2.3.2 montre que la notion d'algèbre de Boole capture toutes les propriétés des ensembles $\mathfrak{P}(A)$ finis : tant que seuls des ensembles finis sont considérés, les lois de 2.2.2 caractérisent complètement les opérations ensemblistes. Il clôt la partie élémentaire de la théorie des ensembles, celle qui se concentre sur les manipulations de la réunion, d'intersection et de complémentaire dans le cas fini, et il explique que la partie non triviale de la théorie concerne l'étude des ensembles infinis.

▷ *La situation est complètement différente avec les algèbres de Boole infinies : un théorème de Stone affirme que toute algèbre de Boole se plonge dans l'algèbre des parties d'un ensemble mais, en général, le plongement n'est pas un isomorphisme et, par exemple, le quotient de* $\mathfrak{P}(\mathbb{N})$ *par l'idéal des ensembles finis est une algèbre de Boole infinie extrêmement compliquée, très éloignée d'une algèbre* $\mathfrak{P}(A)$. ◁

2.3.4.— Pour terminer, signalons encore l'existence d'autres opérations élémentaires sur les ensembles (finis) qui sont bien adaptées à des contextes particuliers, comme le *produit de jointure* : partant d'une famille d'ensembles $(Z_i)_{i\in I}$ et de $X := \prod_{i\in J} Z_i$ et $Y := \prod_{i\in K} Z_i$ où J et K sont deux sous-ensembles fixés de I, et notant $t\restriction S$ la restriction à S d'une fonction t définie sur $J \cup K$, on introduit pour $A \subseteq X$ et $B \subseteq Y$

$$A \bowtie B := \{\ t \in \textstyle\prod_{i\in J\cup K} Z_i \ \big|\ t\restriction J \in A \text{ et } t\restriction K \in B\ \}. \qquad (\#1)$$

La jointure étend à la fois l'intersection, qui correspond au cas $J = K$, et le produit cartésien, qui correspond au cas où J et K sont disjoints, et c'est une opération utile pour l'analyse des bases de données (voir exercice 42).

3. Ébauche d'une théorie des ensembles

On a commencé à développer dans les sections précédentes quelques résultats et démonstrations concernant les ensembles, mais sans avoir introduit ceux-ci autrement que de façon très informelle. Si l'on veut progresser et développer une théorie élaborée, il est nécessaire de fixer un point de départ plus formel, et c'est le but de cette section. Comme il est difficile de définir les ensembles, on recourt à une démarche axiomatique fondée sur les principes d'extensionnalité et de compréhension. Mais la rencontre des paradoxes oblige à refaire le long chemin qui mène au système de Zermelo, point de départ pour la suite du voyage.

> ▷ *L'analyse au demeurant restera incomplète, dans la mesure où elle nous mènera à considérer une famille d'ensembles particuliers, les ensembles purs, dont il n'est pas évident que l'étude soit pertinente. Ce sera la tâche des chapitres* II *et* III *de montrer que la restriction aux ensembles purs ne limite pas le champ d'application de la théorie, et de légitimer ainsi les options prises dans ce chapitre.* ◁

Cette section est organisée en cinq sous-sections. Dans la sous-section 3.1, on constate la difficulté de définir naïvement et de façon satisfaisante les ensembles à partir d'autres objets. On passe donc dans la sous-section 3.2 à une axiomatisation basée sur le principe cantorien des définitions par compréhension. Dans la sous-section 3.3, on explique le paradoxe de Berry, qui oblige à restreindre les définitions au cadre d'une logique formelle. Dans la sous-section 3.4, on aborde à son tour le paradoxe de Russell, qui oblige à une nouvelle restriction du cadre. Finalement, on expose le système de Zermelo dans la sous-section 3.5.

3.1. Une tentative naïve

> ▶ Résumé.— Tenter de définir les ensembles à partir de fonctions indicatrices tourne court. ◀

3.1.1.— Comme pour n'importe quel autre type d'objet mathématique, il est naturel de débuter une théorie des ensembles par une définition des ensembles — et, de fait, c'est l'option prise dans la plupart des langages de programmation. On essaie donc de *définir* les ensembles en s'appuyant sur d'autres objets supposés plus fondamentaux.

3.1.2.— De façon intuitive et pragmatique, les objets mathématiques relèvent de types divers : entiers, points, droites, fonctions, *etc.* Dans une approche élémentaire, et notamment dans les langages de programmation, les ensembles n'apparaissent pas comme un type de base unique, mais plutôt comme *des* types *dérivés* : pour chaque type mathématique τ, on introduit un nouveau type $\mathbf{Ens}_\tau$ formé par les ensembles d'objets de type τ.

▷ *De la même façon, s'introduisent d'autres types voisins comme les suites (analogues aux ensembles, mais en tenant compte de l'ordre des facteurs), ou les multi-ensembles (analogues aux ensembles, mais en tenant compte des répétitions).* ◁

3.1.3.— On cherche donc à définir, pour chaque type τ, un type $\mathbf{Ens}_\tau$. Or, il est usuel d'associer à tout ensemble une fonction indicatrice à valeurs dans $\{0,1\}$ et une approche naturelle est de définir les ensembles à partir des fonctions. Si le type « fonction » est présent, précisément si, pour chaque paire de types τ, τ', il existe un type $\tau{\to}\tau'$ formé des fonctions allant des objets de type τ vers les objets de type τ', alors on peut identifier les ensembles à des fonctions indicatrices : se donner un ensemble A d'objets de type τ, c'est spécifier, pour chaque objet x de type τ, si x est ou non dans A, donc se donner une fonction associant à tout objet de type τ soit la valeur VRAI, soit la valeur FAUX.

3.1.4.— Utilisant la notation $x{:}\tau$ pour indiquer qu'un objet x est de type τ, et notant **Bool** (comme booléen) le type constitué de ces deux seules valeurs VRAI et FAUX, il est donc naturel de poser la définition suivante.

« Définition » (ensemble).— Pour tout type τ, le type $\tau{\to}\mathbf{Bool}$ est noté $\mathbf{Ens}_\tau$; les objets de type $\mathbf{Ens}_\tau$ sont appelés *ensembles* d'objets de type τ. Pour x de type τ, et A de type $\mathbf{Ens}_\tau$, on dit que x est *élément* de A, noté $x \in_\tau A$, si l'on a $A(x) = \text{VRAI}$.

3.1.5.— On peut alors commencer à établir des propriétés des ensembles, et en particulier montrer qu'ils obéissent aux principes informels dégagés dans la première partie de ce chapitre.

« Proposition » (ensembles).— (i) *Un objet de type* $\mathbf{Ens}_\tau$ *est déterminé par ses éléments.*

(ii) *Pour tous* $a_1, \ldots, a_n$ *de type* τ*, il existe un objet de type* $\mathbf{Ens}_\tau$ *ayant pour éléments* $a_1, \ldots, a_n$*.*

(iii) *Pour chaque propriété* $\mathcal{P}(x{:}\tau)$ *des objets de type* τ*, il existe un objet de type* $\mathbf{Ens}_\tau$ *dont les éléments sont les objets de type* τ *satisfaisant* $\mathcal{P}$*.*

Démonstration. Le point (i) découle de ce que le type **Bool** ne contient que deux valeurs : si deux ensembles A, A' ont les mêmes éléments, on a $A(x) = A'(x) = \text{VRAI}$ pour tout x de type τ appartenant à A, et donc $A(x) = A'(x) = \text{FAUX}$ pour tout autre x de type τ. Les fonctions A et A' coïncident donc (pour autant que deux fonctions prenant les mêmes valeurs partout coïncident). Pour (ii), on définit un objet A de type $\mathbf{Ens}_\tau$ en posant $A(a_1) = \cdots = A(a_n) = \text{VRAI}$, et $A(x) = \text{FAUX}$ pour tout autre objet x de type τ. Pour (iii), on définit de même $A{:}\tau{\to}\mathbf{Bool}$ par $A(x) = \text{VRAI}$ si $\mathcal{P}(x)$ est vraie, et $A(x) = \text{FAUX}$ sinon. □

3.1.6.— On doit bien sentir que ce qui précède n'est pas satisfaisant, en tout cas pas suffisant. Même formellement acceptable, la définition de 3.1.4 ne fait que reporter la définition des ensembles sur celle des fonctions, qui n'est pas donnée — et, si l'on se rappelle qu'une fonction est souvent définie comme ensemble de couples, on sent poindre le cercle vicieux. De même, les démonstrations de 3.1.5 ne sont que des vérifications de la cohérence du vocabulaire : faute d'avoir indiqué comment spécifier une fonction, l'existence des fonctions mentionnées n'est en rien établie. C'est une fausse piste !

3.2. Le système de Cantor

▶ Résumé.— Suivant l'approche de Cantor, on axiomatise les ensembles par les axiomes d'extensionnalité et de compréhension. ◀

3.2.1.— À défaut de définir les ensembles, on va chercher à les axiomatiser, c'est-à-dire à recenser une liste de principes de base qu'une intuition partagée et un consensus recommandent de tenir pour pertinents et vrais.

▷ *Le problème rencontré ci-dessus est usuel : qu'il s'agisse de débuter l'arithmétique, la géométrie, ou toute autre théorie concernant des objets basiques, on bute sur la définition des objets premiers. Or, même si la nature en soi des objets mathématiques peut être importante pour le philosophe, elle n'influe pas directement sur les démonstrations et ne concerne donc que peu le mathématicien : peu importe ce que* sont *les nombres entiers, ce qui lui importe pour établir de nouveaux théorèmes est de savoir comment ils* se comportent*, c'est-à-dire quelles en sont les propriétés. On peut donc se contenter d'une approche axiomatique, consistant, à défaut de définir les objets que l'on souhaite étudier, à en énumérer des propriétés de base, puis à déduire de celles-ci, utilisées comme axiomes, des conséquences nouvelles. On sait par exemple que le système de Peano constitue un point de départ raisonnable pour l'arithmétique, tout comme le système d'Euclide en constitue un pour la géométrie élémentaire du plan.* ◁

3.2.2.— Soit donc à développer ce type d'approche axiomatique pour les ensembles. Dans un premier temps, il s'agit de recenser les propriétés de base des ensembles, celles qui seront retenues comme axiomes. On reviendra dans la section XV.3 sur les questions délicates de choix d'axiomes — questions qui ne peuvent faire l'objet que de consensus et non de démonstrations — mais, pour le moment, il est aisé de débuter en s'appuyant sur l'analyse effectuée dans la première section du chapitre, qui assigne aux ensembles deux types de principes de base (ceux-là même que l'on avait tenté de démontrer en 3.1.5) : le premier est un principe d'unicité, à savoir

qu'un ensemble est déterminé par ses éléments ; le second est un principe d'existence, à savoir que l'on peut spécifier un ensemble soit en énumérant ses éléments, soit en donnant une propriété caractéristique de ceux-ci.

Définition (extensionnalité, extension, compréhension, système de Cantor).— On appelle *axiome d'extensionnalité* pour les objets de type τ l'assertion

$$\forall A, A' : \mathbf{Ens}_\tau \, (A = A' \Leftrightarrow \forall x : \tau \, (x \in A \Leftrightarrow x \in A')). \qquad (\mathsf{Ext}_\tau)$$

Pour $n \geqslant 1$, on appelle *axiome d'extension* (de taille n) l'assertion

$$\forall a_1, \ldots, a_n : \tau \; \exists A : \mathbf{Ens}_\tau \; \forall x : \tau \; (x \in A \Leftrightarrow (x = a_1 \text{ ou} \cdots \text{ou } x = a_n)). \qquad (\mathsf{Exs}_{n,\tau})$$

Si $\mathcal{P}(x)$ est une propriété pertinente pour les objets de type τ, on appelle *axiome de compréhension* pour $\mathcal{P}$ l'assertion

$$\exists A : \mathbf{Ens}_\tau \; \forall x : \tau \; (x \in A \Leftrightarrow \mathcal{P}(x) \text{ est vraie}). \qquad (\mathsf{Comp}_{\mathcal{P},\tau})$$

On appelle *système de Cantor* pour le type τ le système formé de tous les axiomes d'extensionnalité, d'extension, et de compréhension relatifs à τ.

3.2.3.— En présence de (Ext_τ), les ensembles dont $(\mathsf{Exs}_{n,\tau})$ et $(\mathsf{Comp}_{\mathcal{P},\tau})$ affirment l'existence sont notés, ainsi que déjà dit, respectivement $\{a_1, \ldots, a_n\}$ et $\{x : \tau \mid \mathcal{P}(x)\}$ (Figure 4). On peut s'affranchir des axiomes d'extension, mentionnés seulement pour suivre l'usage : une définition par extension est un cas particulier de définition par compréhension puisque, pour $a_1, \ldots, a_n$ de type τ, on a $\{a_1, \ldots, a_n\} = \{x : \tau \mid x = a_1 \text{ ou } \ldots \text{ ou } x = a_n\}$.

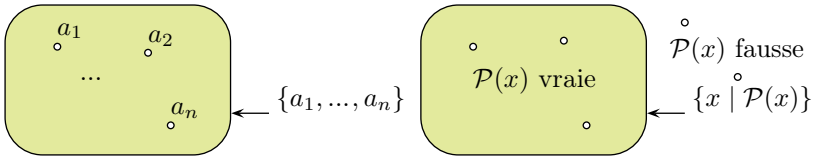


FIGURE 4.— Deux façons usuelles de spécifier un ensemble : par extension, en énumérant les éléments (supposés en nombre fini), et par compréhension, en donnant une propriété caractéristique des éléments.

3.2.4.— L'idée à ce point est donc de poser que, pour chaque type τ, les objets de type $\mathbf{Ens}_\tau$ obéissent aux axiomes d'extensionnalité, (d'extension) et de compréhension, et d'étudier les conséquences de ces axiomes.

3.3. Le paradoxe de Berry

▶ Résumé.— Le paradoxe de Berry rend le système de Cantor intenable. Dans le système de Frege, on restreint la compréhension aux propriétés exprimables formellement. ◀

3.3.1.— Le système de Cantor n'est pas tenable : le résultat suivant, qui est une variante due à G. Berry d'un énoncé de J. Richard, montre qu'il postule l'existence d'objets contradictoires.

Proposition (paradoxe de Berry).— *Si $\mathcal{P}(n)$ est la propriété « n peut être défini par une phrase française d'au plus cent caractères », il ne peut exister d'ensemble des entiers possédant la propriété $\mathcal{P}$.*

Démonstration. Notons **Ent** le type « nombre entier » (que toute théorie raisonnable doit inclure), et soit A l'ensemble $\{n{:}\mathbf{Ent} \mid \mathcal{P}(n)\}$, supposé exister. Il n'y a, en comptant les blancs, qu'au plus 27^{100} phrases françaises d'au plus 100 caractères, et chaque telle phrase ne définit qu'au plus un entier, puisque dire qu'une phrase définit n signifie que n est le seul entier satisfaisant la propriété exprimée. L'ensemble A a donc au plus 27^{100} éléments, et son complémentaire est non vide. L'ordre des entiers est un bon ordre, c'est-à-dire que tout ensemble non vide d'entiers possède un plus petit élément (*cf.* chapitre II), et donc le complémentaire de A possède un plus petit élément, soit n_0. Puisqu'il n'appartient pas à A, l'entier n_0 est non définissable par une phrase française d'au plus 100 caractères. Mais « je suis le plus petit entier non définissable par une phrase française d'au plus cent caractères » est une définition pour n_0, qui comporte 96 caractères. Cette contradiction montre que l'hypothèse que A existe est à rejeter. □

3.3.2.— Puisqu'il postule l'existence d'objets impossibles, le point de départ qui a été appelé système de Cantor ne peut être conservé, et on est donc amené à le modifier en espérant échapper aux contradictions.

▷ *Renoncer à considérer des ensembles d'entiers est difficile, dans la mesure où le type « entier » est l'un des premiers pour lequel on souhaite construire des ensembles. Renoncer aux définitions par compréhension, et se cantonner aux définitions par extension, est une solution drastique*[13] *qui ôte à la notion d'ensemble l'essentiel de son intérêt mathématique. Ne reste donc qu'à restreindre le champ des propriétés permises. On sent bien que le paradoxe de Berry tient à ce que la propriété « être définissable par une phrase française d'au plus cent caractères » n'est pas une propriété mathématique en ce qu'elle fait appel à la notion de phrase française, laquelle ne correspond à aucune définition précise. La solution naturelle est de restreindre le champ de la compréhension à des propriétés exprimables dans un langage assez souple pour laisser le plus de richesse d'expression possible, mais assez restrictif pour échapper au paradoxe de Berry.*

Par exemple, on tient à l'existence d'un ensemble des entiers qui sont somme de deux carrés. Or, une différence claire entre les propriétés « être définissable par une phrase française d'au plus cent caractères » et « être somme de deux carrés » est que la seconde s'exprime par la formule

$$\exists p, q\,(n = p{\times}p + q{\times}q), \qquad (\#2)$$

là où une traduction de la première est problématique. L'idée est de se restreindre désormais aux propriétés exprimables par des formules du type (#2). ◁

13. C'est plus ou moins le point de vue des langages de programmation impératifs.

3.3.3.— Il existe de nombreuses logiques formelles (voir partie B), et donc de nombreuses options sont possibles à ce stade. Pour le moment, on ne va pas entrer dans une discussion précise, mais simplement délimiter un peu le contexte, les définitions formelles étant renvoyées au chapitre VII.

▷ *Ce qui importe ici est de savoir quelles formules peuvent être légitimement utilisées dans des définitions par compréhension. Le principe retenu est de faire appel aux formules dites du premier ordre à un seul type d'objet. Ces formules sont essentiellement les formules mathématiques usuelles, écrites avec des variables et des quantificateurs divers, soumises à quelques contraintes additionnelles que l'on va décrire maintenant.* ◁

3.3.4.— Le cadre consiste à fixer une liste de symboles (« *signature* ») représentant des types, et des opérations et des relations susceptibles de relier des objets de ces types, puis à définir inductivement des *formules* comme des suites finies de symboles qui sont soit des variables avec indication de type, soit des opérations et relations, soit le signe =, soit des connecteurs logiques (non, et, ou, $\Rightarrow$, $\Leftrightarrow$), des quantificateurs ($\exists$, $\forall$), ou des parenthèses.

▷ *Les règles de construction seront données (ou rappelées : il s'agit ni plus ni moins des usages mathématiques) plus loin. Il est suffisant ici de mentionner que*

$$((\forall == n)))(+ + 01 \times p2 \Rightarrow\Rightarrow$$

n'est pas une formule, parce que les symboles n'y sont pas assemblés dans un ordre correct, alors que

$$\forall n{:}\mathbf{Ent}\ \exists p, q{:}\mathbf{Ent}\ (n = p{\times}p + q{\times}q) \qquad (\#3)$$

en est une vis-à-vis de la signature $\mathbf{\Sigma}_1$ comportant un unique type d'objet **Ent**, *et deux symboles d'opération binaires $+$ et $\times$.*

On notera que la formule ($\#3$) est considérée comme légitime alors que la propriété qu'elle exprime est fausse : il existe des entiers qui ne sont pas somme de deux carrés. On rencontre là une distinction importante dans la partie B, à savoir qu'une formule est un objet syntaxique (un mot), et que l'éventuelle valeur de vérité qui peut lui être attachée n'apparaît qu'avec un contexte extérieur d'évaluation non inscrit dans la formule : par exemple, ($\#3$) reçoit la valeur FAUX *lorsque* **Ent** *est le type « entier », et que $+$ et $\times$ réfèrent à l'addition et à la multiplication des entiers. En revanche, on pourra vérifier que la* même *formule ($\#3$) reçoit la valeur* VRAI *lorsque* **Ent** *réfère aux types « complexe » ou « entier modulo 5 », et $+$ et $\times$ aux opérations usuellement associées.* ◁

3.3.5.— On parle spécifiquement de formules *du premier ordre* lorsque les seules variables portent sur les éléments des types déclarés dans $\mathbf{\Sigma}$, à l'exclusion des ensembles de tels éléments.

▷ *Par opposition, on parle de formules* du second ordre *lorsque sont autorisées des variables et des quantifications de type τ et $\mathbf{Ens}_\tau$ et l'usage de $\in_\tau$, du troisième ordre si de même on autorise τ, $\mathbf{Ens}_\tau$, $\mathbf{Ens}_{\mathbf{Ens}_\tau}$ pour chaque type τ de $\mathbf{\Sigma}$, etc. Par exemple, la formule ($\#3$) est du premier ordre par rapport à la signature $\mathbf{\Sigma}_1$, alors que la formule*[14]

$$\forall A{:}\mathbf{Ens}_{\mathbf{Ent}}\ ((0 \in A \text{ et } \forall n{:}\mathbf{Ent}\ (n \in A \Rightarrow n{+}1 \in A)) \Rightarrow \forall n{:}\mathbf{Ent}\ (n \in A)) \qquad (\#4)$$

14. Qu'exprime cette formule ? (... le principe de récurrence)

est du second ordre par rapport à la signature Σ_2 *obtenue en ajoutant à* Σ_1 *les deux symboles de constante* 0 *et* 1. *En revanche, noter que* ($\#4$) *est du premier ordre par rapport à la signature* Σ_3 *comportant les deux types d'objets* **Ent** *et* $\mathbf{Ens}_{\mathbf{Ent}}$ *et, outre les symboles de* Σ_1, *le symbole de relation* $\in$ *entre objets de types* **Ent** *et* $\mathbf{Ens}_{\mathbf{Ent}}$. ◁

3.3.6.— Nous référant à la notion de formule du premier ordre relative à une signature (informellement) définie dans la discussion ci-dessus, et considérant comme intuitive (?) la notion de satisfaction d'une formule $\Phi(x)$ par un objet a de type τ, on revient à la construction des ensembles, et on réintroduit l'axiome de compréhension sous une forme restreinte.

Définition (compréhension restreinte, système de Frege).— Supposant $\Phi(x, x_1, ..., x_n)$ formule du premier ordre en une signature Σ pour un unique [15] type τ, on appelle *axiome de compréhension* en Φ l'assertion

$$\forall a_1, ..., a_n{:}\tau\ \exists A{:}\mathbf{Ens}_\tau\ (x \in A \Leftrightarrow \Phi(x, a_1, ..., a_n)), \qquad (\mathsf{Comp}_{\Phi,\tau})$$

et *système de Frege* [16] pour le type τ le système obtenu à partir du système de Cantor en restreignant les axiomes de compréhension aux formules du premier ordre en Σ.

▷ *Noter que l'on fait figurer explicitement dans l'axiome* ($\mathsf{Comp}_{\Phi,\tau}$) *des paramètres éventuels* $a_1, ..., a_n$ *figurant dans la formule* Φ *mais ne correspondant pas nécessairement à des symboles de constante de* Σ. *Par exemple, si nous considérons le type « entier » et si* Σ *est la signature réduite aux opérations arithmétiques de base, la formule* $\exists p\,(n = p + 3 \text{ ou } n = 5 \times p)$ *est une formule du premier ordre en* Σ *avec une variable libre, à savoir* n, *et deux paramètres, à savoir les entiers* 3 *et* 5. *L'axiome de compréhension associé permet alors d'affirmer l'existence de l'ensemble* $\{n{:}\mathbf{Ent} \mid \exists p\,(n = p + 3 \text{ ou } n = 5 \times p)\}$, *ainsi que le réclame l'usage.* ◁

3.3.7.— Le système de Frege est un sous-système du système initial de Cantor, et il échappe au paradoxe de Berry, tout au moins sous la forme où celui-ci a été énoncé : la conclusion de 3.3.1 devient simplement que la propriété d'être définissable par une phrase française d'au plus cent caractères n'est pas exprimable par une formule du premier ordre.

▷ *La phrase précédente reste vague car l'exprimabilité par une formule du premier ordre est relative au choix d'une signature. Ici, il s'agirait de tout choix d'opérations et de relations sur les entiers pour lequel le principe de récurrence s'applique, impliquant que tout ensemble non vide a un plus petit élément.* ◁

3.3.8.— On peut donc essayer d'aller de l'avant. Pour la suite, on fixe des notations pour les ensembles vides et pleins. Quelle que soit la signature choisie, les formules $x = x$ et $x \neq x$ (négation de $x = x$) sont des formules du premier ordre en cette signature. Appliquant les axiomes de compréhension associés, on obtient, pour chaque type τ, deux ensembles particuliers.

15. *A priori*, rien n'oblige à se restreindre ici à une signature à un seul type d'objet, mais, *de facto*, c'est l'option qui sera retenue dans la suite du texte.

16. Le nom est choisi ici pour le rôle fondateur joué par Frege dans la définition des formules du premier ordre, mais il ne correspond pas à un rôle particulier de celui-ci dans l'axiomatisation de la théorie des ensembles.

Définition (plein, vide).— Pour tout type τ, l'ensemble *plein* Ω_τ de type τ (*resp., vide* $\emptyset_\tau$) est $\{x{:}\tau \mid x = x\}$ (*resp.,* $\{x{:}\tau \mid x \neq x\}$).

Certaines notations sont traditionnelles : $\mathbb{N}$ pour l'ensemble $\Omega_{\mathbf{Ent}}$ de tous les entiers naturels, $\mathbb{R}$ pour l'ensemble $\Omega_{\mathbf{Reel}}$ de tous les réels, *etc.* Les définitions impliquent qu'être un objet de type τ équivaut à appartenir à l'ensemble Ω_τ. Par conséquent, la notation $\{x{:}\tau \mid \Phi(x)\}$ peut être remplacée par $\{x \in \Omega_\tau \mid \Phi(x)\}$, comme par exemple dans $\{n \in \mathbb{N} \mid \exists p, q\, (n = p^2{+}q^2)\}$.

3.4. Le paradoxe de Russell

▶ Résumé.— Le paradoxe de Russell rend le système de Frege intenable. On affaiblit les axiomes de compréhension en axiomes de séparation. ◀

3.4.1.— Le système de Frege se révèle à son tour contradictoire, à cause de ce qui est appelé le paradoxe de Russell. Le problème explicité en 3.4.2 naît de l'introduction d'un hypothétique type « ensemble » général.

▷ *Quel que soit le type τ, les objets de type* $\mathbf{Ens}_\tau$ *ont en commun d'être des ensembles, et, à ce titre, partagent un certain nombre de propriétés. De même, les relations d'appartenance relatives aux divers types peuvent être considérées comme restrictions d'une unique relation d'appartenance générale $\in$. Il apparaît donc naturel d'introduire un type « ensemble » général* **Ens** *englobant tous les types particuliers* $\mathbf{Ens}_\tau$*, en espérant en particulier qu'il permette d'uniformiser l'étude de divers types d'ensembles a priori distincts. On se trouverait ainsi en particulier libéré d'un contexte de type qui, pour intuitif qu'il soit, n'a pas à ce point été défini rigoureusement.* ◁

3.4.2.— Les problèmes surviennent rapidement. S'il existe un type **Ens** dont relèvent tous les ensembles, et si l'axiome de compréhension est valide pour les formules contenant la relation d'appartenance, alors il existe un objet $\Omega_{\mathbf{Ens}}$ qui est l'ensemble de tous les ensembles. De même, par compréhension, il existe un ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes.

Proposition (paradoxe de Russell).— *Supposer l'existence d'un type* **Ens** *général et d'un ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes est une hypothèse contradictoire.*

Démonstration. Supposons[17] $A = \{X{:}\mathbf{Ens} \mid X \notin X\}$, c'est-à-dire supposons que A est un ensemble tel que, pour tout ensemble X, on ait l'équivalence

$$X \in A \Leftrightarrow X \notin X. \qquad (\#5)$$

Pour chaque ensemble X, la relation $X \in A$ est alors soit vraie, soit fausse. En particulier, A étant lui-même un ensemble, l'assertion $A \in A$ doit être soit vraie, soit fausse. Or, par définition de A, suivant (#5), $A \in A$ entraîne $A \notin A$ et, de même, $A \notin A$ entraîne $A \in A$. Chacune des deux possibilités étant contradictoire, c'est que l'hypothèse que A existe est elle-même contradictoire. □

17. Dans toute la suite, $x \notin y$ est la négation de $x \in y$.

▷ *Une autre version du même problème apparaît pour le type* **Ens** *comparé avec le sous-type* $\mathbf{Ens}_{\mathbf{Ens}}$ *formé par les ensembles d'ensembles. Par construction, le type* $\mathbf{Ens}_{\mathbf{Ens}}$ *est un sous-type de* **Ens**, *ce qui revient à dire qu'il existe une injection de l'ensemble* $\Omega_{\mathbf{Ens}_{\mathbf{Ens}}}$, *qui est aussi* $\mathfrak{P}(\Omega_{\mathbf{Ens}})$, *dans l'ensemble* $\Omega_{\mathbf{Ens}}$, *et cela contredit* 1.3.13 (*théorème de Cantor*). ◁

3.4.3.— Comme dans le cas du paradoxe de Berry, on est donc conduit à chercher des solutions pour échapper au paradoxe de Russell. La solution retenue en théorie des ensembles, que nous allons explorer dans ce texte, consiste à restreindre à nouveau le champ d'application de la compréhension pour échapper au paradoxe de Russell. L'idée est d'attribuer le paradoxe au fait que l'ensemble de tous les ensembles est un objet trop grand pour être lui-même un ensemble, et de réserver l'appellation d'ensemble à ceux des objets définis par compréhension qui sont, en un sens à préciser, assez petits.

▷ *D'autres solutions existent et continuent à être explorées. Une des voies est d'attribuer le paradoxe de Russell à la forme syntaxique de la formule* $X \notin X$ *et de l'éviter soit en bannissant l'usage de la négation pour construire une théorie purement positive des ensembles* [108, 80, 30], *soit en limitant les définitions par compréhension à des formules « saines » échappant au risque d'autoréférence* [3]. *Une autre voie, proposée par B. Russell dans* [100], *est de renoncer à introduire un type « ensemble » général et de s'en tenir à un univers typé dans lequel on distingue des objets de base, puis des ensembles d'objets de base, puis des ensembles d'ensembles d'objets de base, etc. De la sorte, la relation d'appartenance ne fait sens qu'entre un objet de type* τ *et un objet de type* $\mathbf{Ens}_\tau$, *et des formules comme* $X \in X$ *ou* $X \notin X$ *ne sont pas définies. L'élaboration d'une théorie des fondements sur ces bases mène à un formalisme compliqué du fait de la diversité des objets introduits, et, au moins pour le moment, il ne semble pas adapté à des questions comme le problème du continu ou, plus généralement, à l'analyse de l'infini non dénombrable. Mais la théorie des types, notamment après les simplifications proposées par A. Church* [10] *et l'approche de P. Martin-Löf* [88], *connaît aujourd'hui un renouveau important dans l'étude des fondements en liaison avec l'informatique et la théorie de l'homotopie* [55] (*voir sous-section* XVI.1.3). ◁

3.4.4.— On renonce donc ici à la forme générale de l'axiome de compréhension : on ne postule plus l'existence d'un ensemble $\{x \mid \Phi(x, a_1, ..., a_n)\}$ pour chaque formule $\Phi(x, x_1, ..., x_n)$ et chaque choix de $a_1, ..., a_n$, et on ne le conserve que pour les formules du type « $x \in A$ et $\Phi(x, a_1, ..., a_n)$ », c'est-à-dire que l'on postule, pour chaque ensemble A et chaque formule, l'existence de l'ensemble $\{x \mid x \in A \text{ et } \Phi(x, a_1, ..., a_n)\}$.

▷ *Il ne s'agit donc plus de former un ensemble ex nihilo, mais simplement de* séparer [18] *à l'intérieur d'un ensemble A préexistant les éléments qui vérifient* Φ *de ceux qui ne vérifient pas* Φ *; on parlera donc d'*axiome de séparation *pour ce cas particulier d'axiome de compréhension.* ◁

18. À la façon dont on sépare le blanc du jaune d'un œuf en pâtisserie ...

Définition (séparation).— Pour $\Phi(x, x_1, ..., x_n)$ formule du premier ordre en une signature en un unique type τ, on appelle *axiome de séparation* en Φ l'assertion

$$\forall a_1, ..., a_n{:}\tau\ \forall A{:}\mathbf{Ens}_\tau\ \exists B{:}\mathbf{Ens}_\tau\ \forall x{:}\tau \\ (x \in B \Leftrightarrow (x \in A \text{ et } \Phi(x, a_1, ..., a_n))). \qquad (\mathsf{Sep}_{\Phi,\tau})$$

On note $\{x{\in}A|\Phi(x, a_1, ..., a_n)\}$ l'ensemble dont $(\mathsf{Sep}_{\Phi,\tau})$ affirme l'existence.

3.4.5.— Pour un type τ donné, deux situations sont alors possibles. Ou bien il existe un ensemble Ω_τ formé par tous les objets de type τ, et alors compréhension et séparation mènent aux mêmes définitions puisque tout ensemble $\{x{:}\tau \mid \Phi(x)\}$ défini par compréhension est aussi défini par séparation comme $\{x \in \Omega_\tau \mid \Phi(x)\}$. Ou bien un tel ensemble n'existe pas, et alors le champ des définitions est restreint. C'est le cas du type « ensemble ».

Proposition (ensemble de tous les ensembles).— *Les objets de type « ensemble » ne forment pas un ensemble.*

Démonstration. S'il existait un ensemble de tous les ensembles, alors, appliquant l'axiome de séparation associé à la formule $x \notin x$, on déduirait l'existence d'un ensemble de tous les ensembles qui ne sont pas éléments d'eux-mêmes, contredisant 3.4.2. □

3.4.6.— En prenant comme point de départ l'axiome d'extensionnalité et la famille infinie de tous les axiomes de séparation en chacune des formules du premier ordre (pour une signature et dans un contexte de type qui restent à spécifier), on se met à l'abri des paradoxes de Berry et de Russell. Mais une nouvelle difficulté apparaît : à la différence des axiomes de compréhension, les axiomes de séparation ne permettent pas de construire des ensembles *ex nihilo*.

▷ *Par exemple, l'existence des ensembles définis par extension, pourtant réclamée par l'intuition et la pratique mathématique, pose problème, et même celle d'un ensemble vide : l'axiome de séparation ne peut suffire puisqu'il ne construit un ensemble qu'à partir d'un autre ensemble préexistant.* ◁

3.4.7.— On est donc conduit à réintroduire explicitement les définitions par extension et, plus généralement, des axiomes garantissant que les opérations ensemblistes de base soient partout définies.

▷ *Plutôt que de poser un axiome pour chaque définition par extension, il est usuel de poser l'existence des paires, c'est-à-dire d'autoriser les définitions par extension d'ensembles à deux éléments au plus, et celle d'un axiome général pour la réunion d'une famille d'ensembles. Par ailleurs, à partir du moment où les axiomes de séparation sont adoptés, il suffit, pour garantir par exemple l'existence d'une paire $\{a, b\}$, d'être assuré de l'existence d'un ensemble A contenant a et b, puisqu'ensuite l'axiome de séparation associé à la formule $x = a$ ou $x = b$ permet de séparer dans A la paire $\{a, b\}$.* ◁

Définition (paire, réunion).— On appelle axiomes *de la paire* et *de la réunion* pour le type τ les assertions

$$\forall a, b{:}\tau\ \exists A{:}\mathbf{Ens}_\tau\ (a \in A \text{ et } b \in A), \qquad (\mathsf{Paire}_\tau)$$

$$\forall A{:}\mathbf{Ens}_{\mathbf{Ens}_\tau}\ \exists B{:}\mathbf{Ens}_\tau\ \forall x{:}\tau \\ (\exists X{:}\mathbf{Ens}_\tau (x \in X \text{ et } X \in A) \Rightarrow x \in B). \qquad (\mathsf{Un}_\tau)$$

En présence des axiomes d'extensionnalité, qui assurent l'unicité, et de séparation, qui permettent d'extraire les ensembles souhaités, on note respectivement $\{a, b\}$ et $\bigcup A$ l'unique ensemble dont les éléments sont a et b, et l'unique ensemble dont les éléments sont les éléments des éléments de A.

3.4.8.— Les axiomes précédents légitiment les définitions par extension dans le cas d'ensembles à un ou deux éléments. En appliquant l'axiome de la réunion à une paire d'ensembles $\{A, B\}$, on obtient la réunion $A \cup B$ de A et de B, c'est-à-dire l'ensemble des éléments qui sont dans A ou dans B. La formulation plus générale donnée ici permet d'introduire la réunion de familles quelconques d'ensembles, et pas seulement celle de deux ensembles. On peut alors légitimer les définitions par extension sans nouvel axiome.

Lemme.— *L'axiome d'extension pour le type τ est conséquence des axiomes d'extensionnalité, de la paire, de la réunion, et de séparation pour le type τ et de l'axiome de la paire pour le type $\mathbf{Ens}_\tau$.*

Démonstration. On montre d'abord par récurrence sur n que, quels que soient les objets $a_1, \ldots, a_n$ de type τ, il existe un ensemble contenant $a_1, \ldots, a_n$. Pour $n = 1$ et $n = 2$, cela résulte de l'axiome de la paire pour le type τ. Supposons $n \geqslant 3$. L'hypothèse de récurrence garantit l'existence d'un ensemble A de type $\mathbf{Ens}_\tau$ contenant $a_1, \ldots, a_{n-1}$, et l'axiome de la paire pour le type τ garantit celle d'un ensemble B de même type contenant a_n. L'axiome de la paire pour le type $\mathbf{Ens}_\tau$ garantit alors l'existence d'un ensemble C de type $\mathbf{Ens}_{\mathbf{Ens}_\tau}$ contenant A et B, puis l'axiome de la réunion pour le type τ garantit celle d'un ensemble D de type $\mathbf{Ens}_\tau$ contenant les éléments des éléments de C, donc en particulier les éléments de A et ceux de B, soit $a_1, \ldots, a_{n-1}$ d'une part et a_n d'autre part. Finalement, l'existence de l'ensemble $\{a_1, \ldots, a_n\}$ s'obtient en séparant dans l'ensemble D les éléments x vérifiant $x = a_1$ ou $\cdots$ ou $x = a_n$, et son unicité résulte de l'axiome d'extensionnalité pour le type τ. □

Noter que, pour autant qu'il existe au moins un objet a de type τ, l'axiome de la paire garantit l'existence du singleton $\{a\}$ (qui est la paire $\{a, a\}$), puis un axiome de séparation garantit l'existence de l'ensemble vide $\emptyset_\tau$, qui est par exemple $\{x \in \{a\} \mid x \neq x\}$.

3.4.9.— En revanche, si A est un ensemble, les axiomes de séparation ne permettent pas de sortir de A, et, en particulier, rien ne permet *a priori* d'affirmer l'existence d'un ensemble de toutes les parties de A. On ajoute donc un nouvel axiome affirmant l'existence d'un ensemble des parties pour tout ensemble A ou, ce qui revient au même en présence des axiomes de séparation, d'un ensemble contenant toutes les parties de A.

Définition (parties).— On appelle axiome *des parties* pour le type τ l'assertion

$$\forall A{:}\mathbf{Ens}_\tau\ \exists B{:}\mathbf{Ens}_{\mathbf{Ens}_\tau}\ \forall X{:}\mathbf{Ens}_\tau\ (X \subseteq A \Rightarrow X \in B). \qquad (\mathsf{Par}_\tau)$$

En présence des axiomes d'extensionnalité et de séparation, l'axiome des parties garantit l'existence d'un unique ensemble dont les éléments sont les parties de A ; comme dans la section 2, cet ensemble est noté $\mathfrak{P}(A)$.

▷ *En introduisant l'ensemble $\mathfrak{P}(A)$, on considère ici toutes les parties de A, qu'elles soient définies ou non par des formules ou tout autre moyen explicite. La distinction est importante, car, par exemple, on a déjà vu avec le théorème de Cantor que l'ensemble $\mathfrak{P}(\mathbb{N})$ de toutes les parties de $\mathbb{N}$ introduit ici est nécessairement non dénombrable. Comme l'ensemble des parties de $\mathbb{N}$ qui sont définissables, par exemple dans le langage de l'arithmétique, est dénombrable puisque la famille des formules pouvant servir de définition l'est, cela implique que l'ensemble $\mathfrak{P}(\mathbb{N})$ contient une infinité d'éléments qui sont des parties non définissables de $\mathbb{N}$. Autrement dit, on considère comme bien définis des ensembles dont certains des éléments échappent à toute définition. Plus subtilement, l'adoption d'un principe de séparation non limité mène à considérer comme légales des définitions autoréférentes : rien n'interdit de définir un ensemble d'entiers A pour une propriété qui met en jeu tous les ensembles d'entiers, donc A lui-même.* ◁

3.4.10.— Malgré les points (hautement) discutables de cette approche dite imprédicative [19], c'est celle-ci qui est ici retenue pour le développement d'une théorie des ensembles.

▷ *Ce faisant, il ne s'agit pas nécessairement de souscrire à des principes philosophiques — et encore moins de chercher à imposer ceux-ci comme un dogme indépassable — mais, plus humblement, d'explorer les conséquences d'une approche, celle où est acceptée la forme la plus faible d'existence pour les objets mathématiques, quitte à frôler le précipice. Il s'agit donc de construire une sorte de cadre maximal, à l'intérieur duquel peuvent être développées d'autres théories plus restrictives, en particulier une ou des théories prédicatives des ensembles où l'on se montre plus exigeant sur la qualité des définitions, cf.* [31, 14]*, ou encore la théorie dite descriptive des ensembles, basée sur les notions de complexité d'un ensemble de nombres réels* [96, 61] (*voir chapitre* IX). *Comme on le répétera au chapitre* IV *à propos de l'axiome du choix, il n'y a aucune raison d'opposer des approches complémentaires qui n'apparaissent souvent a posteriori que comme des moments distincts dans l'étude d'un même problème.* ◁

3.5. Ensembles purs et système de Zermelo

► Résumé.— Dans le système de Zermelo fini, les axiomes de séparation sont restreints aux ensembles purs et aux formules ensemblistes. ◄

19. De tels points ont conduit et conduisent certains mathématiciens à récuser la théorie des ensembles : adversaire résolu de celle-ci, Henri Poincaré écrivait « Mais si [Monsieur Zermelo] a bien fermé sa bergerie, je ne suis pas certain qu'il n'y ait pas enfermé le loup », *cf.* [98] ; voir aussi [114].

3.5.1.— En restreignant la compréhension au cas particulier des axiomes de séparation, on espère être à l'abri des paradoxes, et, en réintroduisant les axiomes de la paire, de la réunion et des parties, disposer de suffisamment d'ensembles pour que la (ou les) théorie(s) ainsi introduite(s) ai(en)t du corps. C'est sur ces bases que l'on se propose de développer dans la suite la théorie des ensembles. *A priori*, il existe une théorie des ensembles d'objets de type τ pour chaque type τ. Pour éviter la multiplication des théories, on va considérer un type unique, celui des ensembles dits *purs*.

▷ *Développer autant de théories des ensembles qu'il existe de signatures, par exemple développer une théorie pour les ensembles d'entiers et une autre pour les ensembles de réels, semble pénible et redondant, et il est naturel de chercher à l'éviter en choisissant une fois pour toutes un type d'objet permettant une théorie unifiée. Or, même l'introduction d'un type général « ensemble » dont relèverait tous les ensembles ne semble pas suffisant. L'intuition immédiate et la pratique mathématique suggèrent qu'il existe de nombreux objets mathématiques qui ne sont pas des ensembles, à commencer par les nombres entiers considérés individuellement, et on se retrouve avec au minimum deux types d'objets distincts, les ensembles et les non-ensembles. Une telle multiplicité des types limite les possibilités techniques, et rend plus difficile le recours à la méthode sémantique de démonstration qui est à la base des développements de la partie C : comme plus loin dans les chapitres* VII *et* VIII*, et même s'il ne s'agit pas d'obstructions de fond, les théorèmes de logique qui fondent une telle méthode sont souvent énoncés pour des logiques à un seul type d'objet. Il est donc naturel de privilégier la recherche d'un tel cadre.* ◁

3.5.2.— Il existe une solution pour sortir du dilemme entre ensembles et objets généraux et rétablir un contexte homogène où tous les objets sont de même type : se restreindre à un univers dont les objets soient des ensembles qui sont aussi ensembles d'ensembles, ensembles d'ensembles d'ensembles, et ainsi de suite. Appelant *purs* de tels ensembles [20], on est alors assuré que tout ensemble d'ensembles purs est lui-même pur et qu'inversement tout élément d'un ensemble pur est un ensemble pur. C'est ce type d'ensemble très particulier que l'on va considérer dans la suite.

▷ *Il semble clair que les ensembles purs, s'ils existent, sont clos par rapport à toutes les opérations ensemblistes précédemment considérées : réunion, intersection, ensemble des parties, etc. En revanche, il n'est pas a priori évident que de tels ensembles purs existent. En fait, il doit en exister au moins un, à savoir l'ensemble vide $\emptyset$: faute d'exister, tous ses éléments, éléments d'éléments, etc. sont des ensembles, et même des ensembles purs. De proche en proche, on en déduit qu'il existe une infinité d'ensembles purs, par exemple*

$$\{\{\emptyset\}\} \cup \mathfrak{P}(\emptyset), \quad \{\mathfrak{P}(\mathfrak{P}(\emptyset))\}, \quad \mathfrak{P}(\mathfrak{P}(\mathfrak{P}(\emptyset \cup \{\emptyset, \{\emptyset\}\}))) \cup \{\emptyset\},$$

et autres ensembles du même genre. ◁

3.5.3.— Si l'on se propose d'étudier, non pas les ensembles quelconques, mais seulement les ensembles purs, alors la question, laissée ouverte pour le moment, du choix de la signature mise en jeu dans les axiomes de séparation

20. Dont à ce point une définition formelle reste à donner ...

peut être aisément résolue. En effet, dès lors que les ensembles purs sont les objets considérés, il est naturel de choisir comme opérations et relations les restrictions aux dits ensembles purs des opérations et relations ensemblistes telles que $\in$, $\subseteq$, $\cup$, $\mathfrak{P}$, *etc.*

▷ *La dernière difficulté est que la liste précédente est mal délimitée, mais cette difficulté-là est aisée à résoudre. Toutes les relations et opérations ensemblistes considérées jusqu'à présent ont en effet la propriété de pouvoir être* définies *à partir de la seule relation d'appartenance $\in$. Une définition formelle sera donnée au chapitre* VII*, mais l'idée est simple et naturelle. Par exemple, la relation d'inclusion $\subseteq$ est définissable à partir de l'appartenance puisque $x \subseteq y$ équivaut à*

$$\forall t\,(t \in x \Rightarrow t \in y)\,;$$

de même l'opération de réunion $\bigcup$ l'est puisque $y = \bigcup x$ équivaut (le vérifier) à

$$\forall z\,(z \in y \Leftrightarrow \exists t\,(z \in t \text{ et } t \in x)).$$

Il est facile de montrer que, si l'on adopte les axiomes de séparation relativement à une certaine signature Σ, alors tous les axiomes de séparation relatifs à toute signature obtenue en étendant Σ par des opérations et relations définissables sont automatiquement valides. ◁

3.5.4.— Le choix dès lors est clair [21] : pour les formules légitimes dans les axiomes de séparation, on se restreindra à l'option minimale d'une signature réduite à la seule relation $\in$.

Définition (formule ensembliste).— On note Σ_{ens} la signature comportant un unique type d'objet $\mathbf{Ens}_{\text{pur}}$ et un unique symbole de relation binaire $\in$, et on appelle *formule ensembliste* toute formule du premier ordre en la signature Σ_{ens}.

Autrement dit, est appelée formule ensembliste toute formule obtenue en assemblant à l'aide de négations, conjonctions, disjonctions, implications et quantifications des formules de la forme $x = y$ et $x \in y$.

▷ *Notons que, dès lors qu'un seul type d'objet est concerné, il n'est plus nécessaire de typer les variables, qui, par défaut, sont considérées de type $\mathbf{Ens}_{\text{pur}}$. Ainsi,*

$$\forall x\,\exists y\,\forall z\,(z \in y \Leftrightarrow z \in x) \quad \textit{et} \quad z \in x$$

sont des formules ensemblistes, alors que

$$\forall x\,\exists y\,(x > y) \quad \textit{et} \quad \exists x\,\forall n{:}\mathbf{Ent}\,(n \in x)$$

n'en sont pas, puisque la relation $>$ et le type **Ent** *y interviennent.* ◁

3.5.5.— À l'ajout près de l'axiome de l'infini qui sera vu au chapitre III, le système obtenu est celui proposé par Zermelo.

Définition (système $\mathsf{Z}_{\mathsf{fini}}$).— Le système $\mathsf{Z}_{\mathsf{fini}}$ (« Zermelo fini ») comprend les axiomes d'extensionnalité, de la paire, de la réunion, des parties et, pour chaque formule ensembliste Φ, l'axiome de séparation en Φ.

21. Même si, pour le moment, il apparaît artificiel et éloigné de la pratique mathématique usuelle ...

Le système $\mathsf{Z}_{\mathsf{fini}}$ est donc la liste (infinie) des axiomes suivants [22] :

$\forall a, b\,(\,\forall x\,(x \in a \Leftrightarrow x \in b) \Rightarrow a = b)$, (Ext)

$\forall a, b\,\exists c\,(a \in c \text{ et } b \in c)$, (Paire)

$\forall a\,\exists b\,\forall x\,(\,\exists y(x \in y \text{ et } y \in a) \Rightarrow x \in b\,)$, (Un)

$\forall a\,\exists b\,\forall x\,(\,\forall y\,(y \in x \Rightarrow y \in a) \Rightarrow x \in b\,)$, (Par)

et, pour chaque formule ensembliste $\Phi(x, a_1, ..., a_n)$ où a et b n'apparaissent pas comme variables libres,

$\forall a, a_1, ..., a_n\,\exists b\,\forall x\,(x \in b \Leftrightarrow (x \in a \text{ et } \Phi(x, a_1, ..., a_n)))$. ($\mathsf{Sep}_\Phi$)

3.5.6.— Ce qui est proposé à ce point est d'utiliser le système $\mathsf{Z}_{\mathsf{fini}}$ comme point de départ axiomatique pour l'étude des ensembles purs. Quelques ajouts s'avéreront nécessaires en chemin, conduisant à l'enrichir en le système de Zermelo–Fraenkel ZFC (avec « C » pour « axiome du choix »).

▷ *Le système $\mathsf{Z}_{\mathsf{fini}}$ contient un grand nombre d'axiomes d'existence, et il affirme donc l'existence d'un grand nombre d'ensembles purs — dont on rappelle qu'aucune définition précise n'a été donnée pour le moment. Il doit être clair que l'analyse précédente n'est pas terminée puisque, au départ, le but n'était pas de se restreindre aux ensembles purs, mais de bâtir au contraire une théorie suffisamment générale pour éclairer le statut de questions comme le problème du continu, qui met en jeu des ensembles d'entiers et de réels, donc a priori des ensembles non purs. Il n'est donc pas clair que l'étude entamée ici ait une portée très vaste, ni qu'elle constitue autre chose qu'une première étape en direction d'une théorie plus générale restant à définir.* ◁

3.5.7.— En fait, un (petit) miracle va se produire. On montrera en effet dans les chapitres II et III qu'il existe une telle profusion d'ensembles purs qu'il est possible de représenter à l'intérieur de ceux-ci la plupart des objets mathématiques, qu'il s'agisse d'ensembles purs ou non, ou même d'objets qui, *a priori*, ne sont pas des ensembles. Du coup, l'étude des ensembles purs qui, au départ, paraissait restrictive et artificielle, devient le cadre naturel de la théorie des ensembles, voire même en un sens de toutes les mathématiques, et le système $\mathsf{Z}_{\mathsf{fini}}$ est alors un point de départ pertinent.

3.5.8.— En revanche, on constatera vite que ce système doit être complété par de nouveaux axiomes.

▷ *Typiquement, il s'agira d'étudier si le système axiomatique est suffisant pour rendre compte de l'existence et des propriétés de tous les ensembles (purs) dont l'intuition suggère l'existence, la situation rêvée étant celle d'un système suffisamment complet pour que toutes les propriétés envisageables puissent y être soit démontrées, soit réfutées. Quand ce n'est pas le cas, et que l'on échoue à trancher pour une certaine propriété, il s'agira de se demander s'il existe une évidence intuitive, et/ou des arguments techniques, recommandant d'en faire un nouvel axiome. Cela se produira à plusieurs reprises dans la suite, aux chapitres* III *et* IV*, pour des questions relativement élémentaires qui nous mèneront successivement aux systèmes de Zermelo* Z *et de Zermelo–Fraenkel* ZFC*, puis, beaucoup*

22. Il n'y a plus lieu d'utiliser plusieurs typographies différentes pour les variables puisqu'elles réfèrent toutes ici à un même type d'objet, à savoir les ensembles purs.

plus tard, au chapitre XV*, pour des questions bien plus sophistiquées qui nous mèneront aux développements récents de la théorie des ensembles et au système actuel* ZFC+DP. ◁

3.5.9.— On termine avec deux remarques. La première est que nous supposons comme une convention logique implicite l'existence d'au moins un ensemble, laquelle ensuite, par séparation et extensionnalité, implique celle d'un unique ensemble vide $\emptyset$.

▷ *Faute d'une telle convention, la théorie serait sans objet : comme la signature* Σ_{ens} *ne contient aucun nom, l'existence d'un ensemble ne peut pas être déduite des axiomes de séparation, et donc du système* $\mathsf{Z}_{\mathsf{fini}}$*. Cette convention est usuelle en logique formelle : lorsque sont introduites les réalisations d'une logique du premier ordre au chapitre* VII*, on requiert toujours que le domaine soit non vide, c'est-à-dire qu'il existe au moins un objet dans le domaine. De façon alternative, si l'on tient à éviter une convention, on adjoint parfois un axiome d'existence trivial du type* $\exists a\,(a = a)$*. Ce point est d'autant plus formel et mineur que sera introduit au chapitre* III *un axiome d'existence d'un ensemble infini, qui clôt définitivement la question.* ◁

3.5.10.— La dernière remarque est plus importante. On a écarté pour les ensembles la définition de 3.1.4 pour ce qu'elle requérait la préexistence des fonctions, et on a privilégié une approche axiomatique. Notons que, toute axiomatique qu'elle soit, l'approche développée ici requiert que les formules, quelle que soit leur définition, et les nombres entiers, sans lesquels celles-ci ne peuvent être construites, préexistent aux ensembles — ou plutôt existent à côté d'eux.

▷ *Le point de vue ainsi adopté est donc très éloigné de celui du traité de Bourbaki* [6]*, qui essaie de se libérer de toute contrainte en construisant simultanément ensembles et formules. On verra dans la partie C, et en particulier dans la sous-section* XVI.1.2*, que ce point de vue, en interdisant le recours à l'approche sémantique, entraîne des limitations inacceptables qui conduisent les spécialistes à le rejeter unanimement.* ◁

—==000==—

Exercices

Exercice 1 (Cantor–Bernstein).— (i) Décrire explicitement la bijection h construite dans la démonstration de 1.3.3 pour $A = B = \mathbb{N} \times \mathbb{N}$ avec $f((x_1, x_2)) = (x_1 + 1, x_2)$ et $g((y_1, y_2)) = (y_1, y_2 + 1)$. (ii) Même question pour $A = B = \mathbb{N}$ avec $f(x) = 2x$ et $g(y) = 3y$. [Notant $\nu_p(x)$ la p-valuation de x (exposant de p dans la décomposition en facteurs premiers de x), montrer que A_i est $\{x \in \mathbb{N} \mid \nu_2(x) \geqslant \nu_3(x) = i\}$ et déduire $h(x) = x/3$ pour $\nu_2(x) < \nu_3(x)$ et $h(x) = 2x$ sinon.] Rapport entre (i) et (ii) ?

Exercice 2 (treillis).— Montrer que, si $(X, \leqslant)$ est un treillis distributif possédant un minimum 0 et un maximum 1, alors, pour tout élément a de X, il existe au plus un élément b vérifiant $\inf(a, b) = 0$ et $\sup(a, b) = 1$. [Supposant $\inf(a, b) = 0$ et $\sup(a, b) = 1$,

et $\inf(a,c) = 0$ et $\sup(a,c) = 1$, poser $d = \sup(b,c)$, et utiliser la distributivité pour montrer $\inf(a,d) = 0$, puis $d = b$, donc $b \geqslant c$.]

Exercice 3 (algèbre de Boole).— Montrer que, pour tout ensemble A, l'ensemble $\mathfrak{P}_*(A)$ formé des parties de A qui sont soit finies, soit co-finies (c'est-à-dire de complémentaire fini) est une algèbre de Boole.

Exercice 4 (algèbre de Boole).— Montrer que, pour tout ensemble A, l'algèbre de Boole $(\mathfrak{P}(A), \subseteq)$ est complète, cela signifiant que toute partie (finie ou infinie) admet une borne supérieure et une borne inférieure.

Exercice 5 (algèbre de Boole).— Pour $f : B \to B'$ homomorphisme d'algèbres de Boole, le *noyau* de f est $\mathrm{Ker}(f) := \{x \in B \mid f(x) = 0\}$. (i) $\mathrm{Ker}(f)$ est-il stable par l'opération $\vee$? par $\wedge$? par complément ? (ii) Montrer que $x = y$ équivaut à $x \wedge \overline{y} = \overline{x} \wedge y = 0$. (iii) À l'aide de (ii), montrer que f est injectif si, et seulement si, $\mathrm{Ker}(f)$ est réduit à $\{0\}$. (iv) En déduire une nouvelle preuve pour l'injectivité de F dans 2.3.2.

Exercice 6 (formules de de Morgan).— Montrer que toute algèbre de Boole satisfait $\overline{a \vee b} = \overline{a} \wedge \overline{b}$ et $\overline{a \wedge b} = \overline{a} \vee \overline{b}$.

Exercice 7 (anneau de Boole).— (i) Montrer que tout anneau de Boole est de caractéristique 2. (ii) Démontrer 2.2.4. [Utiliser le cas des algèbres $\mathfrak{P}(A)$ pour deviner la définition des opérations d'anneau, et utiliser les lois de de Morgan de l'exercice 6]. (iii) Redémontrer le résultat de l'exercice 5(iii) avec les anneaux de Boole.

Repères chronologiques

▸ L'utilisation d'une terminologie ensembliste en mathématiques ne remonte guère au-delà de la fin du XIX$^{\text{e}}$ siècle.

▸ L'apparition d'une théorie de l'infini mathématique peut être datée précisément au moment où G. Cantor (1845–1918) établit la non-équipotence de $\mathbb{R}$ et $\mathbb{N}$ en 1873 [23].

▸ Ce qui a été appelé ici (de façon cavalière) « système de Cantor » correspond à la vision de Cantor vers 1890. L'introduction du symbole d'appartenance $\in$ est attribuée à G. Peano (1858–1932) en 1889.

▸ Les paradoxes qui portent leur nom ont été soulevés respectivement en 1901 par B. Russell (1872–1970), en 1906 [24] par G. Berry (1867–1928).

▸ Le système de Zermelo a été proposé par E. Zermelo (1871–1953) en 1908.

Résumé du chapitre I

▸ Nommer un ensemble, c'est proclamer l'existence d'un nouvel objet rassemblant des objets qui partagent une propriété.

▸ Introduire des ensembles est utile pour exprimer des propriétés collectives ne faisant pas sens pour des objets individuels.

23. La démonstration de 1873 était un peu plus compliquée que l'argument diagonal devenu classique ultérieurement, lui aussi dû à Cantor.

24. On pourra noter que le paradoxe de Russell a été formulé avant celui de Berry, à rebours de l'ordre dans lequel il a paru naturel de le mentionner dans ce texte.

▸ Comparer les ensembles (infinis) mène au problème du continu sur les tailles intermédiaires entre celles de $\mathbb{N}$ et de $\mathbb{R}$: l'absence d'une solution évidente motive l'élaboration d'une théorie.

▸ L'inclusion est une relation d'ordre dont la restriction à tout ensemble du type $\mathfrak{P}(A)$ est un treillis distributif et complémenté.

▸ Les algèbres de Boole peuvent être axiomatisées par les lois algébriques auxquelles obéissent leurs opérations sup et inf.

▸ Toute algèbre de Boole finie est isomorphe à une algèbre de la forme $(\mathfrak{P}(A), \subseteq)$.

▸ Tenter de définir les ensembles à partir de fonctions indicatrices tourne court.

▸ Suivant l'approche de Cantor, on axiomatise les ensembles par les axiomes d'extensionnalité et de compréhension.

▸ Le paradoxe de Berry rend le système de Cantor intenable. Dans le système de Frege, on restreint la compréhension aux propriétés exprimables formellement.

▸ Le paradoxe de Russell rend le système de Frege intenable. On affaiblit les axiomes de compréhension en axiomes de séparation.

▸ Dans le système de Zermelo fini, les axiomes de séparation sont restreints aux ensembles purs et aux formules ensemblistes.

—==000==—