

Module 1

Ensembles, fonctions et cardinalité

Ce module fixe le vocabulaire ensembliste de tout le parcours et établit les trois résultats qui en délimitent le cadre. Il travaille dans la théorie naïve, dont il démontre d'abord qu'elle ne peut pas être prise telle quelle.

$$R = \{ x \mid x \notin x \}$$

L'ensemble de Russell. La même diagonale reparait au théorème de Cantor, puis à l'arrêt des machines et à l'incomplétude.

Sommaire

Objectifs	3
Prérequis supposés acquis	4
Corps du cours	4
Le cadre naïf et le paradoxe de Russell	4
Ensembles, opérations, parties	5
Relations et fonctions	8
Équipotence, subpotence et théorème de Cantor–Schröder–Bernstein	10
Le théorème de Cantor	13
Ensembles finis, dénombrables et au plus dénombrables	14
Résumé des résultats	18
Glossaire du module	20
Pièges fréquents	20
Notations introduites	21
Checklist d’auto-vérification	22

Notations hors Charte. Les cinq notations suivantes sont nécessaires à ce module et absentes de la Charte ; elles sont proposées ici conformément à la Charte § 1.

Notation	Lecture / signification	Justification
$E \preceq F$	subpotence : il existe une injection totale de E dans F	indispensable pour énoncer le théorème de Cantor–Schröder–Bernstein sans présupposer les cardinaux (module 17) ; même famille typographique que $\subseteq$ et $\approx$; le symbole $\preceq$ n’est pas retenu car la Charte § 6.2 le mentionne pour les ensembles ordonnés $(E, \preceq)$
f^{-1}	bijection réciproque d’une bijection f	la Charte ne fixe que l’image réciproque $f^{-1}[B]$; aucun conflit, les crochets distinguent les deux emplois
ε	mot vide, unique élément de E^0	la Charte § 6.2 fixe E^* mais ne nomme pas son élément neutre ; aucun conflit dans le parcours
$[n]$	segment initial $\{k \in \mathbb{N} \mid k < n\}$	nécessaire pour définir la finitude sans recourir aux ordinaux (module 16) ; les crochets ne sont employés ailleurs que pour $f[A]$ et $[x]_R$, dont l’argument n’est jamais un entier
$[a, b], [a, b[$	intervalles réels fermé, semi-ouvert	notation française usuelle ; aucun conflit, l’argument est un couple de réels ; la variante anglo-saxonne $[a, b)$ n’est pas retenue

Objectifs

À l’issue de ce module, le lecteur saura :

- énoncer le principe de compréhension non restreinte et démontrer qu’il est contradictoire (paradoxe de Russell) ;
- manipuler avec rigueur les opérations ensemblistes, les images directes et réciproques, et réfuter par contre-exemple les identités fausses qui les concernent ;
- démontrer qu’une fonction est injective, surjective ou bijective, et identifier les énoncés dont la preuve exige l’axiome du choix ;
- démontrer deux ensembles équipotents en construisant une bijection, ou en exhibant deux injections et en invoquant le théorème de Cantor–Schröder–Bernstein ;
- démontrer le théorème de Cantor par l’argument diagonal et expliquer sa parenté avec le paradoxe de Russell ;
- établir qu’un ensemble est au plus dénombrable au moyen d’un codage explicite, et calculer de tels codages pour $\mathbb{N} \times \mathbb{N}$, $\mathbb{Q}$ et E^* .

Prérequis supposés acquis

Ce module est le premier du parcours : aucune notion issue d'un module antérieur n'est mobilisée, et par conséquent aucun renvoi externe au sens de la Charte § 2.4 ne figure dans cette section. Toutes les notions logiques et ensemblistes employées sont redéfinies ici.

Sont en revanche supposées acquises les connaissances mathématiques générales suivantes, extérieures au parcours et non redémontrées :

1. Le raisonnement par récurrence sur $\mathbb{N}$, sous sa forme simple et sous sa forme forte, ainsi que le principe du bon ordre : toute partie non vide de $\mathbb{N}$ possède un plus petit élément, noté $\min$.
2. La définition de suites par récurrence sur $\mathbb{N}$: étant donnés une valeur initiale et une loi de passage de l'étape n à l'étape $n + 1$, il existe une unique suite les vérifiant. Ce principe est admis ici ; il sera démontré dans le cadre général du théorème de définition par induction structurelle (module 3) et du théorème de récursion transfinie (module 16).
3. L'arithmétique élémentaire de $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$: opérations, ordre, existence et unicité de l'écriture irréductible p/d d'un rationnel avec $d \in \mathbb{N}^*$.
4. Les propriétés élémentaires des ensembles finis, démontrables par récurrence et admises ici sans démonstration : toute partie d'un ensemble fini est finie ; toute partie majorée de $\mathbb{N}$ est finie ; il n'existe pas de bijection entre $\{k \in \mathbb{N} \mid k < n\}$ et $\{k \in \mathbb{N} \mid k < m\}$ lorsque $n \neq m$ (principe des tiroirs).
5. Les propriétés d'ordre et de valeur absolue sur $\mathbb{R}$, utilisées uniquement dans la proposition 1.32 et dans l'exercice 1.34.

Aucune axiomatique ensembliste n'est supposée : le module travaille dans le cadre *naïf*, dont il établit précisément les limites, et prépare l'axiomatisation traitée au module 16.

Corps du cours

Le cadre naïf et le paradoxe de Russell

La théorie des ensembles sert ici de métathéorie : c'est le langage dans lequel on parlera plus tard des formules, des structures et des dérivations. Il importe donc de savoir dès maintenant ce que ce langage autorise et ce qu'il interdit.

Définition 1.1 (Compréhension non restreinte). Le **principe de compréhension non restreinte** est l'énoncé suivant : pour toute propriété P exprimable, il existe un ensemble

$$\{x \mid P(x)\}$$

dont les éléments sont exactement les objets x vérifiant $P(x)$. Autrement dit, pour tout objet a , on a $a \in \{x \mid P(x)\}$ lorsque $P(a)$ est vraie, et $a \notin \{x \mid P(x)\}$ lorsque $P(a)$ est fausse.

C'est ce principe, implicite chez Cantor et explicite chez Frege, qui donne à la théorie naïve sa souplesse. Il est contradictoire.

Théorème 1.2 (Paradoxe de Russell). Le principe de compréhension non restreinte (définition 1.1) est contradictoire.

Preuve. *Par l'absurde.* Supposons le principe de compréhension non restreinte valide. Appliqué à la propriété « x n'est pas élément de lui-même », il fournit un ensemble

$$R := \{x \mid x \notin x\}.$$

Par la définition 1.1, pour tout objet a : $a \in R$ lorsque $a \notin a$, et $a \notin R$ lorsque $a \in a$. L'objet R étant lui-même un ensemble, on peut prendre $a := R$, et l'on distingue deux cas.

Premier cas : $R \in R$. Alors, par la caractérisation ci-dessus appliquée à $a := R$, la propriété définissant R est vraie de R , c'est-à-dire $R \notin R$: contradiction avec l'hypothèse du cas.

Second cas : $R \notin R$. Alors la propriété définissant R est vraie de R , donc R appartient à R , c'est-à-dire $R \in R$: contradiction avec l'hypothèse du cas.

Les deux cas sont exhaustifs et chacun conduit à une contradiction. L'hypothèse absurde posée au départ — la validité du principe de compréhension non restreinte — est donc réfutée. ■

Remarque 1.3. Le paradoxe ne met en cause ni la logique employée, ni la notion d'ensemble, mais la seule liberté de former $\{x \mid P(x)\}$ pour une propriété P arbitraire. La réponse standard consiste à n'admettre la compréhension que sous forme *restreinte* : on ne sépare des éléments qu'à l'intérieur d'un ensemble déjà donné (notation 1.7). C'est l'option retenue dans tout le parcours, et c'est le schéma d'axiomes de séparation de ZF, étudié au module 16. Deux conséquences immédiates de ce choix : la collection de tous les ensembles n'est pas un ensemble (exercice 1.4), et $x \in x$ n'est pas contradictoire en soi, mais devient impossible sous l'axiome de fondation (module 16).

Exercice 1.4. Sous le principe de compréhension restreinte (notation 1.7) et lui seul, démontrer qu'il n'existe aucun ensemble U tel que tout ensemble soit élément de U . On formera $\{x \in U \mid x \notin x\}$ et l'on reprendra l'argument du théorème 1.2.

Exercice 1.5. On appelle *hétérologique* un adjectif qui ne se décrit pas lui-même (« long » est hétérologique, « court » ne l'est pas). Analyser le statut de l'adjectif « hétérologique » et préciser en quoi la difficulté obtenue diffère du théorème 1.2 : quel est ici l'ensemble dont l'existence est illégitimement supposée, et quelle hypothèse supplémentaire, absente de la définition 1.1, est en jeu ?

Ensembles, opérations, parties

Définition 1.6 (Égalité et inclusion). Deux ensembles A et B sont **égaux**, ce qui s'écrit $A = B$, lorsqu'ils ont exactement les mêmes éléments : pour tout objet x , $x \in A$

précisément lorsque $x \in B$. C'est le principe d'**extensionnalité**. On dit que A est **inclus** dans B , ce qui s'écrit $A \subseteq B$, lorsque tout élément de A est élément de B ; l'inclusion est dite **stricte**, ce qui s'écrit $A \subsetneq B$, lorsque de plus $A \neq B$. L'ensemble sans aucun élément est noté $\emptyset$; il est unique par extensionnalité.

L'extensionnalité fournit la méthode standard de preuve d'une égalité d'ensembles : la double inclusion, employée ci-dessous dans la preuve de la proposition 1.9.

Notation 1.7 (Compréhension restreinte). Étant donné un ensemble E et une propriété P , on note

$$\{x \in E \mid P(x)\}$$

l'ensemble des éléments de E vérifiant P . Cette notation, contrairement à celle de la définition 1.1, est légitime dans tout le parcours : elle ne crée aucun ensemble nouveau, elle sépare une partie d'un ensemble déjà disponible.

Définition 1.8 (Opérations booléennes). Soient A, B des ensembles et E un ensemble tel que $A \subseteq E$. On pose

$$A \cup B := \{x \mid x \in A \text{ ou } x \in B\}, \quad A \cap B := \{x \in A \mid x \in B\}, \quad A \setminus B := \{x \in A \mid x \notin B\},$$

et $\complement_E A := E \setminus A$, le **complémentaire** de A dans E . Pour une famille $(A_i)_{i \in I}$ d'ensembles indexée par un ensemble I non vide, on pose de même $\bigcup_{i \in I} A_i$, l'ensemble des objets appartenant à au moins un A_i , et $\bigcap_{i \in I} A_i$, l'ensemble des objets appartenant à tous les A_i .

L'hypothèse « I non vide » n'est pas une commodité : pour $I = \emptyset$, l'intersection indexée serait la collection de tous les objets, qui n'est pas un ensemble (exercice 1.4). L'union indexée sur $I = \emptyset$ vaut en revanche $\emptyset$ sans difficulté.

Proposition 1.9 (Lois de De Morgan). Soient E un ensemble, I un ensemble non vide et $(A_i)_{i \in I}$ une famille de parties de E . Alors

$$\complement_E \left(\bigcup_{i \in I} A_i \right) = \bigcap_{i \in I} \complement_E A_i \quad \text{et} \quad \complement_E \left(\bigcap_{i \in I} A_i \right) = \bigcup_{i \in I} \complement_E A_i.$$

Preuve. *Par double inclusion, pour chacune des deux égalités.*

Première égalité, inclusion directe. Soit $x \in \complement_E (\bigcup_{i \in I} A_i)$. Par la définition 1.8, $x \in E$ et x n'appartient à aucun A_i . Soit $i \in I$ quelconque : de $x \in E$ et $x \notin A_i$ on tire $x \in \complement_E A_i$. Ceci valant pour tout $i \in I$, on a $x \in \bigcap_{i \in I} \complement_E A_i$.

Première égalité, inclusion réciproque. Soit $x \in \bigcap_{i \in I} \complement_E A_i$. Comme I est non vide, choisissons $i_0 \in I$; de $x \in \complement_E A_{i_0}$ on tire $x \in E$. Par ailleurs, pour tout $i \in I$, $x \in \complement_E A_i$, donc $x \notin A_i$; ainsi x n'appartient à aucun A_i , c'est-à-dire $x \notin \bigcup_{i \in I} A_i$. De $x \in E$ et $x \notin \bigcup_{i \in I} A_i$ on conclut $x \in \complement_E (\bigcup_{i \in I} A_i)$.

Seconde égalité, inclusion directe. Soit $x \in \complement_E (\bigcap_{i \in I} A_i)$, donc $x \in E$ et $x \notin \bigcap_{i \in I} A_i$. Il existe donc $j \in I$ tel que $x \notin A_j$; alors $x \in \complement_E A_j$, donc $x \in \bigcup_{i \in I} \complement_E A_i$.

Seconde égalité, inclusion réciproque. Soit $x \in \bigcup_{i \in I} \complement_E A_i$: il existe $j \in I$ tel que $x \in \complement_E A_j$, d'où $x \in E$ et $x \notin A_j$. De $x \notin A_j$ on tire $x \notin \bigcap_{i \in I} A_i$, et donc $x \in \complement_E (\bigcap_{i \in I} A_i)$. ■

Définition 1.10 (Ensemble des parties). Pour tout ensemble E , on note $\mathcal{P}(E)$ l'ensemble dont les éléments sont exactement les parties de E : pour tout ensemble A , on a $A \in \mathcal{P}(E)$ précisément lorsque $A \subseteq E$.

Exemple 1.11. On a $\mathcal{P}(\emptyset) = \{\emptyset\}$, ensemble à un élément, et $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, ensemble à deux éléments. Plus généralement, pour $a \neq b$, $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. On prendra garde à ne pas confondre $\emptyset$ et $\{\emptyset\}$: le premier n'a aucun élément, le second en a un.

Définition 1.12 (Couple, produit cartésien). Pour deux objets a et b , le **couple** (a, b) est défini par $(a, b) := \{\{a\}, \{a, b\}\}$. Le **produit cartésien** de deux ensembles est $A \times B := \{z \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \text{il existe } a \in A \text{ et } b \in B \text{ tels que } z = (a, b)\}$. Les **n -uplets** sont définis par récurrence sur n : $(a_1) := a_1$ et $(a_1, \dots, a_{n+1}) := ((a_1, \dots, a_n), a_{n+1})$; on pose $E^n := E \times \dots \times E$ (n facteurs), et E^* désigne l'ensemble des suites finies d'éléments de E , dont le **mot vide** ε , unique élément de E^0 .

La définition du produit cartésien par la notation 1.7 à l'intérieur de $\mathcal{P}(\mathcal{P}(A \cup B))$ n'est pas une coquetterie : elle évite le recours à la définition 1.1, puisque $\{a\}$ et $\{a, b\}$ sont des parties de $A \cup B$, donc (a, b) est une partie de $\mathcal{P}(A \cup B)$.

Lemme 1.13 (Propriété caractéristique du couple). Pour tous objets a, b, c, d , on a $(a, b) = (c, d)$ exactement lorsque $a = c$ et $b = d$.

Preuve. *Par double implication, la seconde par analyse de cas sur l'égalité $a = b$.*

Sens réciproque. Si $a = c$ et $b = d$, les deux couples sont le même objet par substitution, donc $(a, b) = (c, d)$.

Sens direct. Supposons $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$.

Cas 1 : $a = b$. Alors $\{a, b\} = \{a\}$, donc $(a, b) = \{\{a\}\}$: ce couple a un unique élément. Par extensionnalité (définition 1.6), $\{\{c\}, \{c, d\}\}$ a donc lui aussi $\{a\}$ pour unique élément, d'où $\{c\} = \{a\}$ et $\{c, d\} = \{a\}$. De $\{c\} = \{a\}$ on tire $c = a$; de $\{c, d\} = \{a\}$ on tire $d = a$, et comme $b = a$ par l'hypothèse du cas, $d = b$. Les deux égalités voulues sont établies.

Cas 2 : $a \neq b$. Comme $\{a\}$ est élément du membre de gauche, il est élément du membre de droite : ou bien $\{a\} = \{c\}$, ou bien $\{a\} = \{c, d\}$. De même, $\{a, b\}$ est égal à $\{c\}$ ou à $\{c, d\}$.

Écartons d'abord $\{a, b\} = \{c\}$: cette égalité donnerait $a = c$ et $b = c$, donc $a = b$, ce qui contredit l'hypothèse du cas. Donc $\{a, b\} = \{c, d\}$.

Écartons ensuite $\{a\} = \{c, d\}$: cette égalité donnerait $c = a$ et $d = a$, donc $\{c, d\} = \{a\}$; joint à $\{a, b\} = \{c, d\}$, cela donnerait $\{a, b\} = \{a\}$, donc $b = a$, ce qui contredit encore l'hypothèse du cas. Donc $\{a\} = \{c\}$, c'est-à-dire $a = c$.

Il reste à établir $b = d$. De $\{a, b\} = \{c, d\}$ et $a = c$ on tire $\{a, b\} = \{a, d\}$. Comme $b \in \{a, b\}$, on a $b \in \{a, d\}$, donc $b = a$ ou $b = d$; le premier membre de l'alternative est exclu par l'hypothèse du cas, donc $b = d$. ■

Exercice 1.14. Démontrer que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ et que $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, par double inclusion dans les deux cas.

Exercice 1.15. Démontrer que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$, puis exhiber deux ensembles A et B pour lesquels $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$. Préciser laquelle des deux inclusions subsiste dans le second cas.

Relations et fonctions

Définition 1.16 (Relation binaire). Une **relation binaire** sur un ensemble E est une partie $R \subseteq E \times E$; on écrit $x R y$ pour $(x, y) \in R$. La relation R est dite **réflexive** lorsque $x R x$ pour tout $x \in E$; **symétrique** lorsque, pour tous $x, y \in E$, $x R y$ entraîne $y R x$; **transitive** lorsque, pour tous $x, y, z \in E$, $x R y$ et $y R z$ entraînent $x R z$; **antisymétrique** lorsque $x R y$ et $y R x$ entraînent $x = y$.

Définition 1.17 (Relation d'équivalence). Une relation binaire R sur E est une **relation d'équivalence** lorsqu'elle est réflexive, symétrique et transitive. Pour $x \in E$, la **classe d'équivalence** de x est $[x]_R := \{y \in E \mid x R y\}$, et l'**ensemble quotient** est $E/R := \{C \in \mathcal{P}(E) \mid \text{il existe } x \in E \text{ tel que } C = [x]_R\}$.

Proposition 1.18 (Le quotient est une partition). Soit R une relation d'équivalence sur E . Alors :

1. pour tout $x \in E$, $x \in [x]_R$; en particulier toute classe est non vide et E est la réunion de ses classes;
2. pour tous $x, y \in E$: $x R y$ exactement lorsque $[x]_R = [y]_R$;
3. pour tous $x, y \in E$, ou bien $[x]_R = [y]_R$, ou bien $[x]_R \cap [y]_R = \emptyset$.

Preuve. *Construction directe pour le point 1, par double implication pour le point 2, par analyse de cas pour le point 3.*

Point 1. Soit $x \in E$. Par réflexivité de R (définition 1.17), $x R x$, donc $x \in [x]_R$ par définition de la classe. Toute classe contient donc au moins l'élément dont elle est la classe, et tout $x \in E$ appartient à la classe $[x]_R$, laquelle est élément de E/R .

Point 2, sens direct. Supposons $x R y$. Soit $z \in [x]_R$, c'est-à-dire $x R z$. Par symétrie, $y R x$; par transitivité appliquée à $y R x$ et $x R z$, on obtient $y R z$, donc $z \in [y]_R$: ainsi $[x]_R \subseteq [y]_R$. L'inclusion inverse s'obtient de même en partant de $z \in [y]_R$, c'est-à-dire $y R z$, et en appliquant la transitivité à $x R y$ et $y R z$. Par double inclusion, $[x]_R = [y]_R$.

Point 2, sens réciproque. Supposons $[x]_R = [y]_R$. Par le point 1, $y \in [y]_R$, donc $y \in [x]_R$, c'est-à-dire $x R y$.

Point 3. Soient $x, y \in E$. Si $[x]_R \cap [y]_R = \emptyset$, la conclusion est acquise. Sinon, il existe $z \in [x]_R \cap [y]_R$, donc $x R z$ et $y R z$. Par symétrie, $z R y$; par transitivité appliquée à $x R z$ et $z R y$, on obtient $x R y$, d'où $[x]_R = [y]_R$ par le point 2. ■

Définition 1.19 (Fonction). Une **fonction partielle** de E dans F , ce qui s'écrit $f : E \rightarrow F$, est une partie $f \subseteq E \times F$ telle que, pour tout $x \in E$, il existe au plus un $y \in F$ vérifiant $(x, y) \in f$; on note alors $y = f(x)$. Son **domaine** est $\text{dom}(f) := \{x \in E \mid \text{il existe } y \in F \text{ tel que } (x, y) \in f\}$ et son **image** est $\text{im}(f) := \{y \in F \mid \text{il existe } x \in E \text{ tel que } (x, y) \in f\}$. La fonction est **totale**, ce qui s'écrit $f : E \rightarrow F$, lorsque $\text{dom}(f) = E$.

Dans ce module, « fonction » sans qualificatif signifie « fonction totale »; la convention inverse prévaudra en calculabilité (modules 11 et 12), où l'on qualifiera systématiquement.

Notation 1.20 (Opérations sur les fonctions). Soit $f : E \rightarrow F$. Pour $A \subseteq E$ et $B \subseteq F$, on note $f[A] := \{y \in F \mid \text{il existe } x \in A \text{ tel que } y = f(x)\}$ l'**image directe** de

A , et $f^{-1}[B] := \{x \in E \mid f(x) \in B\}$ l'**image réciproque** de B . La **restriction** de f à A est $f \upharpoonright A := \{(x, y) \in f \mid x \in A\}$. Pour $g : F \rightarrow G$, la **composée** est $g \circ f : E \rightarrow G$, $x \mapsto g(f(x))$. L'**identité** de E est $\text{id}_E : E \rightarrow E$, $x \mapsto x$.

La notation $f^{-1}[B]$ a un sens pour toute fonction f , bijective ou non : elle ne présuppose aucune réciproque. On la distinguera soigneusement de la bijection réciproque f^{-1} introduite à la proposition 1.22, qui n'existe que si f est bijective ; les crochets marquent la différence.

Définition 1.21 (Injection, surjection, bijection). Une fonction totale $f : E \rightarrow F$ est **injective** lorsque, pour tous $x, y \in E$, $f(x) = f(y)$ entraîne $x = y$; **surjective** lorsque $\text{im}(f) = F$, c'est-à-dire lorsque, pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$; **bijjective** lorsqu'elle est à la fois injective et surjective.

Proposition 1.22 (Inverses). Soit $f : E \rightarrow F$ une fonction totale.

1. Si $E \neq \emptyset$, alors f est injective exactement lorsqu'il existe $g : F \rightarrow E$ telle que $g \circ f = \text{id}_E$.
2. f est bijective exactement lorsqu'il existe $g : F \rightarrow E$ telle que $g \circ f = \text{id}_E$ et $f \circ g = \text{id}_F$. Une telle g est alors unique ; on la note f^{-1} et elle est elle-même bijective.
3. S'il existe $s : F \rightarrow E$ telle que $f \circ s = \text{id}_F$, alors f est surjective.

Preuve. *Par double implication pour les points 1 et 2, construction directe pour le point 3.*

Point 1, sens direct. Supposons f injective et $E \neq \emptyset$; fixons $e_0 \in E$. Pour $y \in F$, deux cas se présentent. Si $y \in \text{im}(f)$, il existe $x \in E$ tel que $f(x) = y$, et cet x est unique par injectivité de f ; on pose $g(y) := x$. Sinon, on pose $g(y) := e_0$. La fonction $g : F \rightarrow E$ ainsi définie est totale et, pour tout $x \in E$, $f(x) \in \text{im}(f)$ et l'unique antécédent de $f(x)$ est x , donc $g(f(x)) = x$: ainsi $g \circ f = \text{id}_E$.

Point 1, sens réciproque. Supposons qu'il existe g telle que $g \circ f = \text{id}_E$, et soient $x, y \in E$ avec $f(x) = f(y)$. En appliquant $g : x = g(f(x)) = g(f(y)) = y$. Donc f est injective.

Point 2, sens direct. Supposons f bijective. Pour $y \in F$, la surjectivité fournit un $x \in E$ tel que $f(x) = y$, et l'injectivité assure son unicité ; on pose $g(y) := x$. La fonction $g : F \rightarrow E$ est totale. Pour $y \in F$, $f(g(y)) = y$ par construction, donc $f \circ g = \text{id}_F$; pour $x \in E$, $g(f(x))$ est l'unique antécédent de $f(x)$, à savoir x , donc $g \circ f = \text{id}_E$.

Point 2, sens réciproque. Supposons $g \circ f = \text{id}_E$ et $f \circ g = \text{id}_F$. La première égalité donne l'injectivité de f par le point 1 (sens réciproque, dont la preuve n'utilise pas $E \neq \emptyset$). La seconde donne la surjectivité : pour $y \in F$, $y = f(g(y))$ est dans $\text{im}(f)$.

Point 2, unicité. Soient g et g' vérifiant toutes deux les deux égalités. Pour $y \in F$: $g(y) = g(f(g'(y)))$, car $f \circ g' = \text{id}_F$, et $g(f(g'(y))) = g'(y)$, car $g \circ f = \text{id}_E$. Donc $g = g'$. Enfin f^{-1} est bijective, car f elle-même joue pour f^{-1} le rôle que f^{-1} joue pour f dans les deux égalités, ce qui permet d'appliquer le sens réciproque du point 2 à f^{-1} .

Point 3. Supposons $f \circ s = \text{id}_F$ et soit $y \in F$. Alors $y = f(s(y))$, donc $y \in \text{im}(f)$. Ceci valant pour tout $y \in F$, f est surjective. ■

La réciproque du point 3 — toute surjection admet un inverse à droite — n'est *pas* démontrable sans hypothèse supplémentaire : elle équivaut à l'axiome du choix (module 17, AC et lemme de Zorn). Aucune preuve du présent module ne l'utilise ; les seuls

énoncés du module dont la démonstration requerrait le choix sont signalés explicitement (remarque suivant la proposition 1.46).

Contre-exemple 1.23 (L'image directe ne commute pas à l'intersection).

Posons $E := \{0, 1\}$, $F := \{0\}$ et $f : E \rightarrow F$ la fonction constante $x \mapsto 0$, puis $A := \{0\}$ et $B := \{1\}$. Alors $A \cap B = \emptyset$, donc $f[A \cap B] = \emptyset$, tandis que $f[A] = f[B] = \{0\}$, donc $f[A] \cap f[B] = \{0\}$. Ainsi $f[A \cap B] \neq f[A] \cap f[B]$. Seule l'inclusion $f[A \cap B] \subseteq f[A] \cap f[B]$ est générale ; l'image *reciproque*, en revanche, commute à toutes les opérations booléennes (exercice 1.24).

Exercice 1.24. Démontrer que, pour toute $f : E \rightarrow F$ et toutes parties $B, B' \subseteq F$: $f^{-1}[B \cup B'] = f^{-1}[B] \cup f^{-1}[B']$, $f^{-1}[B \cap B'] = f^{-1}[B] \cap f^{-1}[B']$ et $f^{-1}[\mathbb{C}_F B] = \mathbb{C}_E f^{-1}[B]$.

Exercice 1.25. Soient $f : E \rightarrow F$, $A \subseteq E$ et $B \subseteq F$. Démontrer que $A \subseteq f^{-1}[f[A]]$ et $f[f^{-1}[B]] \subseteq B$, puis démontrer que la première inclusion est une égalité pour tout A exactement lorsque f est injective, et que la seconde l'est pour tout B exactement lorsque f est surjective.

Équipotence, subpotence et théorème de Cantor–Schröder–Bernstein

Définition 1.26 (Équipotence). Deux ensembles E et F sont **équipotents**, ce qui s'écrit $E \approx F$, lorsqu'il existe une bijection de E sur F .

L'équipotence est la notion primitive : elle compare des ensembles sans supposer construit un objet « cardinal ». Le cardinal $|E|$ lui-même, défini comme le plus petit ordinal équipotent à E , ne sera disponible qu'au module 17 ; jusque-là, l'écriture $|E| = |F|$ doit être lue comme une abréviation de $E \approx F$.

Proposition 1.27. Pour tous ensembles E, F, G : $E \approx E$; si $E \approx F$ alors $F \approx E$; si $E \approx F$ et $F \approx G$ alors $E \approx G$.

Preuve. *Construction directe, dans les trois cas.*

Réflexivité. La fonction id_E est injective (si $x = y$ alors $x = y$) et surjective (tout $x \in E$ est l'image de x), donc bijective, donc $E \approx E$.

Symétrie. Soit $f : E \rightarrow F$ une bijection. Par la proposition 1.22, point 2, la fonction $f^{-1} : F \rightarrow E$ existe et est bijective, donc $F \approx E$.

Transitivité. Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ bijectives. La composée $g \circ f$ est injective : si $g(f(x)) = g(f(y))$, l'injectivité de g donne $f(x) = f(y)$, puis celle de f donne $x = y$. Elle est surjective : pour $z \in G$, la surjectivité de g fournit $y \in F$ tel que $g(y) = z$, puis celle de f fournit $x \in E$ tel que $f(x) = y$, d'où $g(f(x)) = z$. Donc $g \circ f$ est bijective et $E \approx G$. ■

Notation 1.28 (Subpotence). On écrit $E \preccurlyeq F$, et l'on dit que E est **subpotent** à F , lorsqu'il existe une fonction totale injective de E dans F . Cette notation ne figure pas dans la Charte (voir l'encadré de tête).

Proposition 1.29. Pour tous ensembles E, F, G : (i) $E \preccurlyeq E$; (ii) si $E \preccurlyeq F$ et $F \preccurlyeq G$ alors $E \preccurlyeq G$; (iii) si $E \subseteq F$ alors $E \preccurlyeq F$; (iv) si $E \approx F$ alors $E \preccurlyeq F$ et $F \preccurlyeq E$.

Preuve. *Construction directe, dans les quatre cas.*

(i) id_E est injective, comme vu dans la preuve de la proposition 1.27.

(ii) Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ injectives. La composée $g \circ f$ est injective, par l'argument déjà donné dans la preuve de la transitivité à la proposition 1.27.

(iii) Si $E \subseteq F$, la fonction $j : E \rightarrow F$, $x \mapsto x$, est totale et injective.

(iv) Si $f : E \rightarrow F$ est bijective, elle est en particulier injective, donc $E \preccurlyeq F$; et $f^{-1} : F \rightarrow E$ est bijective par la proposition 1.22, point 2, donc injective, d'où $F \preccurlyeq E$. ■

La réciproque du point (iv) est le théorème suivant. Elle n'a rien d'évident : rien ne dit *a priori* que de deux injections opposées on puisse fabriquer une bijection.

Théorème 1.30 (Théorème de Cantor–Schröder–Bernstein). Soient A et B deux ensembles. Si $A \preccurlyeq B$ et $B \preccurlyeq A$, alors $A \approx B$.

Preuve. *Construction directe, à partir d'une suite de parties définie par récurrence sur $\mathbb{N}$.*

Soient $f : A \rightarrow B$ et $g : B \rightarrow A$ injectives. Définissons par récurrence sur $n \in \mathbb{N}$ (prérequis 2) la suite de parties de A :

$$C_0 := A \setminus g[B], \quad C_{n+1} := g[f[C_n]], \quad C := \bigcup_{n \in \mathbb{N}} C_n.$$

Définissons ensuite $h : A \rightarrow B$ en posant, pour $x \in A$:

$$h(x) := \begin{cases} f(x) & \text{si } x \in C, \\ g^{-1}(x) & \text{si } x \notin C. \end{cases}$$

La fonction h est bien définie et totale. Le seul point à vérifier concerne le second cas. Soit $x \notin C$. Comme $C_0 \subseteq C$, on a $x \notin C_0$, c'est-à-dire $x \notin A \setminus g[B]$; or $x \in A$, donc $x \in g[B]$: il existe $b \in B$ tel que $g(b) = x$. Cet élément b est unique par injectivité de g ; on le note $g^{-1}(x)$. La disjonction des deux cas est exclusive et exhaustive, donc h est une fonction totale de A dans B .

La fonction h est injective. Soient $x, y \in A$ avec $h(x) = h(y)$. Trois configurations sont possibles.

Si $x \in C$ et $y \in C$, alors $f(x) = f(y)$, d'où $x = y$ par injectivité de f .

Si $x \notin C$ et $y \notin C$, alors $g^{-1}(x) = g^{-1}(y)$; en appliquant g aux deux membres et en utilisant $g(g^{-1}(x)) = x$ et $g(g^{-1}(y)) = y$, on obtient $x = y$.

Si l'un est dans C et l'autre non, on peut supposer $x \in C$ et $y \notin C$ (le cas symétrique s'obtient en échangeant les noms de x et y). Alors $f(x) = g^{-1}(y)$, donc, en appliquant g , $y = g(f(x))$. Comme $x \in C$, il existe $n \in \mathbb{N}$ tel que $x \in C_n$; alors $f(x) \in f[C_n]$, donc $y = g(f(x)) \in g[f[C_n]] = C_{n+1} \subseteq C$, ce qui contredit $y \notin C$. Cette configuration est donc impossible.

La fonction h est surjective. Soit $b \in B$, et posons $a := g(b) \in A$. Deux cas.

Si $a \notin C$, alors $h(a) = g^{-1}(a) = g^{-1}(g(b)) = b$ par injectivité de g , donc $b \in \text{im}(h)$.

Si $a \in C$, il existe $n \in \mathbb{N}$ tel que $a \in C_n$. On a $n \neq 0$: en effet $a = g(b) \in g[B]$, alors que $C_0 = A \setminus g[B]$ ne contient aucun élément de $g[B]$. Donc $n = m + 1$ pour un $m \in \mathbb{N}$, et $a \in C_{m+1} = g[f[C_m]]$: il existe $x \in C_m$ tel que $a = g(f(x))$. De $g(b) = a = g(f(x))$ et de l'injectivité de g on tire $b = f(x)$. Comme $x \in C_m \subseteq C$, on a $h(x) = f(x) = b$, donc $b \in \text{im}(h)$.

Dans les deux cas $b \in \text{im}(h)$, donc h est surjective. Étant injective et surjective, h est bijective, et $A \approx B$. ■

Cette démonstration n'utilise pas l'axiome du choix : les objets $g^{-1}(x)$ et $x \in C_m$ y sont obtenus par unicité ou par existence explicite, jamais par sélection simultanée dans une famille.

Corollaire 1.31 (Encadrement). Soient $A \subseteq B \subseteq C$ trois ensembles tels que $A \approx C$. Alors $A \approx B$ et $B \approx C$.

Preuve. *Construction directe, puis application du théorème 1.30.* De $B \subseteq C$ et de la proposition 1.29 (iii) on tire $B \preccurlyeq C$. Par hypothèse il existe une bijection $u : C \rightarrow A$; elle est injective, et la fonction $j : A \rightarrow B$, $x \mapsto x$, est injective par la proposition 1.29 (iii) puisque $A \subseteq B$. Donc $j \circ u : C \rightarrow B$ est injective par la proposition 1.29 (ii), c'est-à-dire $C \preccurlyeq B$. Le théorème 1.30 appliqué à B et C donne $B \approx C$. Enfin $A \approx C$ et $C \approx B$ donnent $A \approx B$ par symétrie et transitivité (proposition 1.27). ■

Proposition 1.32. Les ensembles $\mathbb{R}$ et $[0, 1] := \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ sont équipotents.

Preuve. *Construction directe de deux injections, puis application du théorème 1.30.*

L'inclusion $[0, 1] \subseteq \mathbb{R}$ donne $[0, 1] \preccurlyeq \mathbb{R}$ par la proposition 1.29 (iii).

Réciproquement, posons $u : \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto \frac{x}{1 + |x|}$, puis $v : \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto \frac{1}{2} + \frac{u(x)}{2}$. Le dénominateur $1 + |x|$ est strictement positif, donc u est bien définie et totale, et v aussi.

Les valeurs de v sont dans $[0, 1]$. Pour tout x , $|u(x)| = \frac{|x|}{1 + |x|} < 1$, car $|x| < 1 + |x|$. Donc $-1 < u(x) < 1$, d'où $0 < v(x) < 1$ et en particulier $v(x) \in [0, 1]$.

La fonction v est injective. Il suffit de le démontrer pour u , puisque $v(x) = v(y)$ entraîne $u(x) = u(y)$. Or, pour tout x , on a $|u(x)| = \frac{|x|}{1 + |x|}$, donc

$$1 - |u(x)| = \frac{1 + |x| - |x|}{1 + |x|} = \frac{1}{1 + |x|},$$

quantité strictement positive, et par conséquent

$$\frac{u(x)}{1 - |u(x)|} = \frac{x}{1 + |x|} \cdot (1 + |x|) = x.$$

Ainsi x se récupère à partir de $u(x)$ par une expression ne dépendant que de $u(x)$: si $u(x) = u(y)$, alors $x = \frac{u(x)}{1 - |u(x)|} = \frac{u(y)}{1 - |u(y)|} = y$. Donc u , puis v , sont injectives.

La fonction v , vue comme fonction de $\mathbb{R}$ dans $[0, 1]$, est donc une injection totale, d'où $\mathbb{R} \preccurlyeq [0, 1]$. Le théorème 1.30 conclut : $\mathbb{R} \approx [0, 1]$. ■

Exercice 1.33. Démontrer que $\mathbb{N} \approx \mathbb{N} \setminus \{0\}$ et, plus généralement, que $\mathbb{N} \approx \mathbb{N} \setminus P$ pour toute partie finie $P \subseteq \mathbb{N}$. Commenter : l'inclusion stricte $\mathbb{N} \setminus \{0\} \subsetneq \mathbb{N}$ interdit-elle l'équipotence ?

Exercice 1.34. En utilisant le théorème 1.30, démontrer que $[0, 1] \approx [0, 1[$ puis que $\mathbb{R} \approx \mathbb{R} \setminus \mathbb{Q}$. Pour la seconde équipotence, on pourra utiliser la proposition 1.32 et le corollaire 1.48.

Le théorème de Cantor

Théorème 1.35 (Théorème de Cantor). Pour tout ensemble E , il n'existe aucune surjection de E sur $\mathcal{P}(E)$.

Preuve. *Par l'absurde, au moyen de l'argument diagonal.*

Supposons qu'il existe une surjection $f : E \rightarrow \mathcal{P}(E)$. Comme $f(x)$ est, pour chaque $x \in E$, une partie de E , on peut poser, par compréhension restreinte (notation 1.7) :

$$D := \{x \in E \mid x \notin f(x)\}.$$

C'est une partie de E , donc $D \in \mathcal{P}(E)$. Par surjectivité de f , il existe $a \in E$ tel que $f(a) = D$. Distinguons deux cas.

Premier cas : $a \in D$. Par définition de D , cela signifie $a \notin f(a)$; or $f(a) = D$, donc $a \notin D$: contradiction avec l'hypothèse du cas.

Second cas : $a \notin D$. Comme $a \in E$, la définition de D impose que la propriété « $a \notin f(a)$ » soit fausse, c'est-à-dire $a \in f(a)$; or $f(a) = D$, donc $a \in D$: contradiction avec l'hypothèse du cas.

Les deux cas sont exhaustifs et chacun conduit à une contradiction. L'hypothèse absurde — l'existence d'une surjection de E sur $\mathcal{P}(E)$ — est donc réfutée. ■

Corollaire 1.36 (Hiérarchie stricte). Pour tout ensemble E : $E \prec \mathcal{P}(E)$, mais $\mathcal{P}(E) \not\preceq E$; en particulier E et $\mathcal{P}(E)$ ne sont pas équipotents.

Preuve. *Construction directe pour la première assertion, par l'absurde pour la seconde.*

Première assertion. La fonction $s : E \rightarrow \mathcal{P}(E)$, $x \mapsto \{x\}$, est totale et injective : si $\{x\} = \{y\}$, alors $x \in \{y\}$, donc $x = y$. Donc $E \prec \mathcal{P}(E)$.

Seconde assertion. Supposons qu'il existe une injection totale $j : \mathcal{P}(E) \rightarrow E$. Construisons $f : E \rightarrow \mathcal{P}(E)$ ainsi : pour $x \in E$, si $x \in \text{im}(j)$, il existe un unique $A \in \mathcal{P}(E)$ tel que $j(A) = x$ (unicité par injectivité de j) et l'on pose $f(x) := A$; sinon on pose $f(x) := \emptyset$, ce qui est licite puisque $\emptyset \in \mathcal{P}(E)$. Alors f est surjective : pour $A \in \mathcal{P}(E)$, l'élément $x := j(A)$ vérifie $f(x) = A$. L'existence d'une telle surjection contredit le théorème 1.35. Donc $\mathcal{P}(E) \not\preceq E$.

Conséquence. Si l'on avait $E \approx \mathcal{P}(E)$, la proposition 1.29 (iv) donnerait $\mathcal{P}(E) \prec E$, ce qui vient d'être exclu. ■

Remarque 1.37 (La diagonale et Russell). Les théorèmes 1.2 et 1.35 sont un seul et même argument. Si l'on applique la construction de la preuve du théorème 1.35 à un hypothétique ensemble U de tous les ensembles et à la fonction $f := \text{id}_U$, l'ensemble diagonal $D = \{x \in U \mid x \notin f(x)\}$ devient exactement l'ensemble de Russell $\{x \mid x \notin x\}$. Ce schéma diagonal se retrouvera, sous des habillages différents, à l'indécidabilité du problème de l'arrêt (module 12), au lemme de diagonalisation (module 14) et au théorème de Tarski (module 14). Il vaut la peine d'en retenir la forme : *étant donné un procédé qui prétend énumérer tous les objets d'une espèce, fabriquer un objet de cette espèce qui diffère du x -ième en son x -ième trait.*

Exercice 1.38. Démontrer directement, sans passer par le corollaire 1.36, qu'il n'existe pas d'injection de $\mathcal{P}(\mathbb{N})$ dans $\mathbb{N}$, en supposant une telle injection donnée et en construisant une partie diagonale.

Exercice 1.39. Soit E un ensemble et $f : E \rightarrow \mathcal{P}(E)$ une fonction totale quelconque. Démontrer que la partie $D := \{x \in E \mid x \notin f(x)\}$ n'appartient pas à $\text{im}(f)$, et en déduire une nouvelle preuve du théorème 1.35 qui ne procède pas par l'absurde.

Ensembles finis, dénombrables et au plus dénombrables

Définition 1.40 (Finitude et dénombrabilité). Pour $n \in \mathbb{N}$, on pose $[n] := \{k \in \mathbb{N} \mid k < n\}$. Un ensemble E est **fini** lorsqu'il existe $n \in \mathbb{N}$ tel que $E \approx [n]$; il est **infini** dans le cas contraire. Il est **dénombrable** lorsque $E \approx \mathbb{N}$, et **au plus dénombrable** lorsqu'il est fini ou dénombrable.

Conformément à la Charte § 7, « dénombrable » signifie ici *infini dénombrable* : un ensemble fini n'est pas dénombrable. L'usage anglo-saxon de *countable*, qui inclut le fini, correspond à « au plus dénombrable ».

Lemme 1.41 (Parties infinies de $\mathbb{N}$). Toute partie infinie $A \subseteq \mathbb{N}$ est dénombrable.

Preuve. *Construction directe d'une énumération par récurrence sur $\mathbb{N}$, puis vérification de la bijectivité.*

Comme A est infini, il est en particulier non vide, et aucune partie finie de A n'épuise A : pour toute partie finie S , l'ensemble $A \setminus S$ est non vide, faute de quoi $A \subseteq S$ serait fini (prérequis 4). Le principe du bon ordre (prérequis 1) permet donc de définir par récurrence (prérequis 2) la suite

$$e(0) := \min A, \quad e(n+1) := \min (A \setminus \{e(0), \dots, e(n)\}),$$

chaque minimum portant sur une partie non vide de $\mathbb{N}$ par la remarque précédente.

Assertion auxiliaire. Pour tout $n \in \mathbb{N}$, on a $e(0) < e(1) < \dots < e(n)$ et

$$\{a \in A \mid a \leq e(n)\} = \{e(0), \dots, e(n)\}.$$

Preuve de l'assertion auxiliaire. *Par récurrence sur n .*

Cas de base. $e(0) = \min A$ appartient à A et minore A , donc tout $a \in A$ vérifiant $a \leq e(0)$ vérifie $a = e(0)$; l'égalité annoncée est acquise, et la condition de croissance est vide pour $n = 0$.

Hérédité. Supposons l'assertion vraie au rang n . Par l'hypothèse de récurrence, les éléments de A inférieurs ou égaux à $e(n)$ sont exactement $e(0), \dots, e(n)$, donc

$$A \setminus \{e(0), \dots, e(n)\} = \{a \in A \mid a > e(n)\},$$

et par conséquent $e(n+1)$ est le plus petit élément de A strictement supérieur à $e(n)$. En particulier $e(n+1) > e(n)$, ce qui, joint à l'hypothèse de récurrence, donne $e(0) < \dots < e(n) < e(n+1)$. Soit maintenant $a \in A$ avec $a \leq e(n+1)$. Si $a \leq e(n)$, alors $a \in \{e(0), \dots, e(n)\}$ par hypothèse de récurrence. Sinon $a > e(n)$, et comme $e(n+1)$ est le plus petit élément de A strictement supérieur à $e(n)$, on a $a \geq e(n+1)$, donc $a = e(n+1)$. Réciproquement, chaque $e(k)$ pour $k \leq n+1$ appartient à A et vérifie $e(k) \leq e(n+1)$ par croissance. L'égalité au rang $n+1$ est donc établie. $\square$

La fonction $e : \mathbb{N} \rightarrow A$ est injective. Soient $m \neq n$, par exemple $m < n$; la stricte croissance établie par l'assertion auxiliaire donne $e(m) < e(n)$, donc $e(m) \neq e(n)$.

La fonction e est surjective. La stricte croissance entraîne $e(n) \geq n$ pour tout n , comme on le voit par récurrence immédiate : $e(0) \geq 0$, et $e(n+1) > e(n) \geq n$ donne $e(n+1) \geq n+1$. Soit $a \in A$. Alors $e(a) \geq a$, donc l'ensemble $\{n \in \mathbb{N} \mid e(n) \geq a\}$ est non vide ; soit n_0 son plus petit élément (prérequis 1). On a $a \leq e(n_0)$ et $a \in A$, donc, par l'assertion auxiliaire, $a \in \{e(0), \dots, e(n_0)\}$: a est bien dans $\text{im}(e)$.

Ainsi e est une bijection de $\mathbb{N}$ sur A , donc $A \approx \mathbb{N}$ par la proposition 1.27 (symétrie), c'est-à-dire A est dénombrable. ■

Corollaire 1.42 (Caractérisation). Un ensemble E est au plus dénombrable exactement lorsque $E \preccurlyeq \mathbb{N}$.

Preuve. *Par double implication.*

Sens direct. Si E est fini, il existe n et une bijection $b : E \rightarrow [n]$; comme $[n] \subseteq \mathbb{N}$, la proposition 1.29 (iii) et (ii) donnent $E \preccurlyeq \mathbb{N}$. Si E est dénombrable, $E \approx \mathbb{N}$ donne $E \preccurlyeq \mathbb{N}$ par la proposition 1.29 (iv).

Sens réciproque. Soit $j : E \rightarrow \mathbb{N}$ injective et $A := \text{im}(j) \subseteq \mathbb{N}$. La fonction j , vue comme fonction de E dans A , est bijective : elle est injective par hypothèse et surjective sur son image par définition de A . Donc $E \approx A$. Deux cas. Si A est fini, il existe n tel que $A \approx [n]$, donc $E \approx [n]$ par transitivité (proposition 1.27) et E est fini. Si A est infini, le lemme 1.41 donne $A \approx \mathbb{N}$, donc $E \approx \mathbb{N}$ par transitivité et E est dénombrable. Dans les deux cas E est au plus dénombrable. ■

Notation 1.43 (Codage des couples). On note $\langle \cdot, \cdot \rangle : \mathbb{N}^2 \rightarrow \mathbb{N}$ la fonction de couplage de Cantor

$$\langle m, n \rangle := \frac{(m+n)(m+n+1)}{2} + n.$$

C'est la fonction de codage retenue dans tout le parcours (Charte § 6.7).

Proposition 1.44. La fonction $\langle \cdot, \cdot \rangle$ de la notation 1.43 est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$.

Preuve. *Construction directe, à partir des nombres triangulaires.*

Pour $k \in \mathbb{N}$, posons $T_k := \frac{k(k+1)}{2}$. Comme k et $k+1$ sont deux entiers consécutifs, l'un des deux est pair, donc $T_k \in \mathbb{N}$. On a $T_0 = 0$ et, pour tout k ,

$$T_{k+1} - T_k = \frac{(k+1)(k+2) - k(k+1)}{2} = \frac{(k+1) \cdot 2}{2} = k+1 > 0,$$

donc la suite (T_k) est strictement croissante ; une récurrence immédiate donne alors $T_k \geq k$, si bien que (T_k) n'est pas majorée. Avec ces notations, en posant $s := m+n$:

$$\langle m, n \rangle = T_s + n, \quad \text{avec} \quad 0 \leq n \leq s.$$

Assertion auxiliaire. Pour tout $N \in \mathbb{N}$, il existe un unique $s \in \mathbb{N}$ tel que $T_s \leq N < T_{s+1}$.

Preuve de l'assertion auxiliaire. *Construction directe pour l'existence, par l'absurde pour l'unicité.* L'ensemble $K := \{k \in \mathbb{N} \mid T_k \leq N\}$ contient 0, car $T_0 = 0 \leq N$, et il est majoré par N , car $T_k \geq k$; il est donc fini et non vide (prérequis 4), et possède un plus grand élément s . Par définition de s , $T_s \leq N$, et $s+1 \notin K$, c'est-à-dire

$N < T_{s+1}$. Pour l'unicité, supposons $s \neq s'$ conviennent tous deux, par exemple $s < s'$; alors $s + 1 \leq s'$, donc $T_{s+1} \leq T_{s'}$ par croissance, d'où $N < T_{s+1} \leq T_{s'} \leq N$: contradiction obtenue sur la comparaison de N à lui-même. $\square$

Surjectivité. Soit $N \in \mathbb{N}$ et soit s l'unique entier fourni par l'assertion auxiliaire. Posons $n := N - T_s$, qui est un entier naturel puisque $T_s \leq N$. De $N < T_{s+1} = T_s + s + 1$ on tire $n < s + 1$, donc $0 \leq n \leq s$. Posons $m := s - n$, entier naturel. Alors $m + n = s$ et $\langle m, n \rangle = T_s + n = N$.

Injectivité. Soient (m, n) et (m', n') tels que $\langle m, n \rangle = \langle m', n' \rangle =: N$. Posons $s := m + n$ et $s' := m' + n'$. Comme $0 \leq n \leq s$, on a $T_s \leq T_s + n = N$ et $N = T_s + n \leq T_s + s < T_s + s + 1 = T_{s+1}$, donc $T_s \leq N < T_{s+1}$; le même calcul donne $T_{s'} \leq N < T_{s'+1}$. L'unicité de l'assertion auxiliaire impose $s = s'$. Alors $n = N - T_s = N - T_{s'} = n'$, puis $m = s - n = s' - n' = m'$. Donc $(m, n) = (m', n')$ par le lemme 1.13. $\blacksquare$

Corollaire 1.45. $\mathbb{N}^2 \approx \mathbb{N}$, et plus généralement $\mathbb{N}^k \approx \mathbb{N}$ pour tout entier $k \geq 1$.

Preuve. Par récurrence sur k , le cas $k = 2$ étant la proposition 1.44.

Cas de base $k = 1$. $\mathbb{N}^1 = \mathbb{N}$ et $\text{id}_{\mathbb{N}}$ est bijective.

Hérédité. Supposons $\mathbb{N}^k \approx \mathbb{N}$, au moyen d'une bijection $b : \mathbb{N}^k \rightarrow \mathbb{N}$. La fonction

$$c : \mathbb{N}^{k+1} \rightarrow \mathbb{N}, \quad (a_1, \dots, a_{k+1}) \mapsto \langle b(a_1, \dots, a_k), a_{k+1} \rangle$$

est bijective. Elle est injective : si $c(\vec{a}) = c(\vec{a}')$, la proposition 1.44 donne $b(a_1, \dots, a_k) = b(a'_1, \dots, a'_k)$ et $a_{k+1} = a'_{k+1}$, puis l'injectivité de b donne $(a_1, \dots, a_k) = (a'_1, \dots, a'_k)$, d'où l'égalité des deux $(k+1)$ -uplets par le lemme 1.13. Elle est surjective : pour $N \in \mathbb{N}$, la proposition 1.44 fournit (u, v) tel que $\langle u, v \rangle = N$, puis la surjectivité de b fournit $(a_1, \dots, a_k)$ tel que $b(a_1, \dots, a_k) = u$, et $c(a_1, \dots, a_k, v) = N$. $\blacksquare$

Proposition 1.46 (Réunion au plus dénombrable). Soient I un ensemble, $(A_i)_{i \in I}$ une famille d'ensembles, $u : I \rightarrow \mathbb{N}$ une injection et, pour chaque $i \in I$, une injection $g_i : A_i \rightarrow \mathbb{N}$, la famille $(g_i)_{i \in I}$ étant elle aussi donnée. Alors $\bigcup_{i \in I} A_i$ est au plus dénombrable.

Preuve. Construction directe d'une injection dans $\mathbb{N}$, puis application du corollaire 1.42.

Si $I = \emptyset$, la réunion est vide, donc finie, donc au plus dénombrable. Supposons I non vide et posons $U := \bigcup_{i \in I} A_i$. Soit $x \in U$. L'ensemble $M_x := \{u(i) \mid i \in I \text{ et } x \in A_i\}$ est une partie non vide de $\mathbb{N}$; soit $m(x) := \min M_x$ (prérequis 1). Il existe un unique $i \in I$ tel que $u(i) = m(x)$, par injectivité de u ; notons-le $i(x)$. On a $x \in A_{i(x)}$ par construction de M_x . On pose

$$h : U \rightarrow \mathbb{N}, \quad h(x) := \langle m(x), g_{i(x)}(x) \rangle.$$

Cette définition ne fait intervenir aucune sélection arbitraire : $m(x)$ est un minimum, $i(x)$ est unique, et $g_{i(x)}$ est un membre de la famille donnée.

Injectivité de h . Soient $x, y \in U$ avec $h(x) = h(y)$. Par injectivité de $\langle \cdot, \cdot \rangle$ (proposition 1.44), $m(x) = m(y)$ et $g_{i(x)}(x) = g_{i(y)}(y)$. De $m(x) = m(y)$ et de l'injectivité de u on tire $i(x) = i(y) =: i$. Alors $g_i(x) = g_i(y)$, donc $x = y$ par injectivité de g_i .

Ainsi $U \preccurlyeq \mathbb{N}$, et le corollaire 1.42 conclut. $\blacksquare$

L'hypothèse selon laquelle la famille d'injections $(g_i)_{i \in I}$ est *donnée* est essentielle et ne peut être remplacée par la seule hypothèse « chaque A_i est au plus dénombrable ». Savoir que chaque A_i admet une injection dans $\mathbb{N}$ ne fournit pas une manière d'en choisir une simultanément pour tous les i : ce passage est exactement l'axiome du choix dénombrable. L'énoncé « toute réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable » n'est pas démontrable dans ZF seul (module 17, AC et lemme de Zorn ; module 18 pour les techniques d'indépendance). Dans les applications de ce parcours, les injections sont toujours explicitement construites, et l'hypothèse est donc satisfaite.

Proposition 1.47 (Mots sur un alphabet au plus dénombrable). Si E est au plus dénombrable, alors E^* est au plus dénombrable.

Preuve. *Construction directe d'une injection dans $\mathbb{N}$, la famille des codages étant définie par récurrence sur la longueur.*

Par le corollaire 1.42, il existe une injection $g : E \rightarrow \mathbb{N}$. Définissons par récurrence sur $n \in \mathbb{N}$ (prérequis 2) une fonction $j_n : E^n \rightarrow \mathbb{N}$:

$$j_0(\varepsilon) := 0, \quad j_{n+1}(a_0, \dots, a_n) := \langle j_n(a_0, \dots, a_{n-1}), g(a_n) \rangle.$$

Chaque j_n est injective. Par récurrence sur n . Pour $n = 0$, $E^0 = \{\varepsilon\}$ n'a qu'un élément, donc toute fonction de source E^0 est injective. Supposons j_n injective et soient deux éléments de E^{n+1} ayant même image par j_{n+1} . Par injectivité de $\langle \cdot, \cdot \rangle$ (proposition 1.44), leurs préfixes de longueur n ont même image par j_n et leurs dernières lettres ont même image par g ; l'hypothèse de récurrence donne l'égalité des préfixes, l'injectivité de g celle des dernières lettres, et le lemme 1.13 conclut à l'égalité des deux mots.

Codage global. Tout $w \in E^*$ appartient à E^n pour un unique n , sa longueur ; on pose $h(w) := \langle n, j_n(w) \rangle$. Si $h(w) = h(w')$, la proposition 1.44 donne d'abord l'égalité des longueurs, $n = n'$, puis $j_n(w) = j_n(w')$, d'où $w = w'$ par injectivité de j_n . Donc h est une injection de E^* dans $\mathbb{N}$, et le corollaire 1.42 conclut. ■

Ce résultat est le seul du module qui sera utilisé de façon constante par la suite : c'est lui qui garantit que l'ensemble des formules d'un langage au plus dénombrable est au plus dénombrable, hypothèse du théorème de complétude de Gödel (module 9) et du théorème de Löwenheim–Skolem descendant (module 9).

Corollaire 1.48. Les ensembles $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.

Preuve. *Construction directe d'injections, puis application du corollaire 1.42 et de la définition 1.40.*

Cas de $\mathbb{Z}$. La fonction $\zeta : \mathbb{Z} \rightarrow \mathbb{N}$ définie par $\zeta(n) := 2n$ si $n \geq 0$ et $\zeta(n) := -2n - 1$ si $n < 0$ est totale et injective : les valeurs prises sur les entiers positifs ou nuls sont paires, celles prises sur les entiers strictement négatifs sont impaires, donc deux entiers de signes distincts ont des images distinctes ; et sur chacun des deux domaines, ζ est injective car $n \mapsto 2n$ et $n \mapsto -2n - 1$ le sont. Donc $\mathbb{Z} \preccurlyeq \mathbb{N}$.

Cas de $\mathbb{Q}$. Tout $q \in \mathbb{Q}$ s'écrit de manière unique $q = p/d$ avec $p \in \mathbb{Z}$, $d \in \mathbb{N}^*$ et p, d premiers entre eux (prérequis 3). La fonction $\rho : \mathbb{Q} \rightarrow \mathbb{N}$, $q \mapsto \langle \zeta(p), d \rangle$, où p/d est l'écriture irréductible de q , est donc bien définie et totale ; elle est injective, car $\rho(q) = \rho(q')$ donne, par injectivité de $\langle \cdot, \cdot \rangle$ (proposition 1.44), $\zeta(p) = \zeta(p')$ et $d = d'$, donc $p = p'$ par injectivité de ζ , donc $q = p/d = p'/d' = q'$. Donc $\mathbb{Q} \preccurlyeq \mathbb{N}$.

Ces ensembles sont infinis. La fonction $\mathbb{N} \rightarrow \mathbb{Z}$, $n \mapsto n$, est injective, donc $\mathbb{N} \preccurlyeq \mathbb{Z}$ et de même $\mathbb{N} \preccurlyeq \mathbb{Q}$. Par le théorème 1.30 appliqué à chacun de ces deux ensembles et à $\mathbb{N}$, on obtient $\mathbb{Z} \approx \mathbb{N}$ et $\mathbb{Q} \approx \mathbb{N}$: ces ensembles sont dénombrables au sens de la définition 1.40. ■

Proposition 1.49. L'ensemble $\mathcal{P}(\mathbb{N})$ n'est pas au plus dénombrable. De plus, pour tout ensemble E , l'application $A \mapsto \chi_A$ est une bijection de $\mathcal{P}(E)$ sur l'ensemble des fonctions totales de E dans $\{0, 1\}$, où $\chi_A(x) := 1$ si $x \in A$ et $\chi_A(x) := 0$ sinon.

Preuve. *Par l'absurde pour la première assertion, construction directe pour la seconde.*

Première assertion. Supposons $\mathcal{P}(\mathbb{N})$ au plus dénombrable. Par le corollaire 1.42, $\mathcal{P}(\mathbb{N}) \preccurlyeq \mathbb{N}$, ce qui contredit le corollaire 1.36 appliqué à $E := \mathbb{N}$. La contradiction est obtenue sur l'existence d'une injection de $\mathcal{P}(\mathbb{N})$ dans $\mathbb{N}$.

Seconde assertion. Notons $\Phi : A \mapsto \chi_A$. Elle est injective : si $\chi_A = \chi_B$, alors pour tout $x \in E$, $x \in A$ exactement lorsque $\chi_A(x) = 1$, c'est-à-dire lorsque $\chi_B(x) = 1$, c'est-à-dire lorsque $x \in B$; par extensionnalité (définition 1.6), $A = B$. Elle est surjective : soit $\theta : E \rightarrow \{0, 1\}$ totale, et posons $A := \theta^{-1}[\{1\}] = \{x \in E \mid \theta(x) = 1\}$, qui est une partie de E . Pour $x \in E$, si $\theta(x) = 1$ alors $x \in A$ donc $\chi_A(x) = 1$; si $\theta(x) = 0$ alors $x \notin A$ donc $\chi_A(x) = 0$. Dans les deux cas $\chi_A(x) = \theta(x)$, donc $\chi_A = \theta$ et $\theta \in \text{im}(\Phi)$. ■

Remarque 1.50 (Portée logique et hypothèse du continu). Deux conséquences méritent d'être retenues dès maintenant.

D'une part, la proposition 1.47 assure que les objets syntaxiques du parcours — formules, dérivations, théories axiomatisées — forment des ensembles au plus dénombrables dès que le langage l'est ; c'est ce qui rend possibles le codage arithmétique des formules (module 13) et les constructions de modèles dénombrables (module 9).

D'autre part, la proposition 1.49 établit qu'il existe strictement plus de parties de $\mathbb{N}$ que d'entiers. Savoir s'il existe un ensemble de cardinal strictement compris entre celui de $\mathbb{N}$ et celui de $\mathcal{P}(\mathbb{N})$ est l'hypothèse du continu HC : elle n'est ni réfutable dans ZFC (théorème de Gödel sur la constructibilité, module 18), ni démontrable dans ZFC (théorème de Cohen (indépendance de HC), module 18). Il ne s'agit donc pas d'une question laissée ouverte faute de travail, mais d'un énoncé indécidable dans la théorie usuelle.

Exercice 1.51. Démontrer que l'ensemble des parties finies de $\mathbb{N}$ est dénombrable. On pourra coder une partie finie par un mot fini strictement croissant et invoquer la proposition 1.47.

Exercice 1.52. On appelle *nombre algébrique* tout réel racine d'un polynôme non nul à coefficients rationnels. Démontrer que l'ensemble des nombres algébriques est dénombrable, en admettant qu'un polynôme non nul de degré d possède au plus d racines réelles. En déduire, à l'aide de la proposition 1.49 et de l'exercice 1.34, qu'il existe des réels non algébriques, sans en exhiber aucun.

Exercice 1.53. Soit E un ensemble infini. Démontrer que E n'est pas au plus dénombrable exactement lorsque, pour toute fonction totale $f : \mathbb{N} \rightarrow E$, on a $\text{im}(f) \neq E$. Identifier précisément le point de la démonstration où une hypothèse de choix serait requise si l'on voulait établir que tout ensemble infini contient une partie dénombrable.

Résumé des résultats

Numéro	Nom	Énoncé abrégé	Dépendances
1.2	Paradoxe de Russell	la compréhension non restreinte est contradictoire	définition 1.1
1.9	Lois de De Morgan	le complémentaire échange union et intersection indexées	définitions 1.6, 1.8
1.13	Propriété caractéristique du couple	$(a, b) = (c, d)$ équivaut à la conjonction $a = c$ et $b = d$	définitions 1.6, 1.12
1.18	Le quotient est une partition	les classes d'une équivalence sont non vides, égales ou disjointes, et recouvrent E	définition 1.17
1.22	Inverses	injectivité équivaut à inverse à gauche ; bijectivité à inverse bilatère unique f^{-1}	définitions 1.19, 1.21
1.27	Équipotence : réflexivité, symétrie, transitivité	$\approx$ se comporte comme une équivalence	proposition 1.22, définition 1.26
1.29	Subpotence : préordre	$\preccurlyeq$ est réflexive, transitive, compatible avec $\subseteq$ et $\approx$	proposition 1.22, notation 1.28
1.30	Théorème de Cantor–Schröder–Bernstein	$A \preccurlyeq B$ et $B \preccurlyeq A$ entraînent $A \approx B$	définitions 1.21, 1.26, notation 1.28, prérequis 2
1.31	Encadrement	$A \subseteq B \subseteq C$ et $A \approx C$ entraînent $A \approx B \approx C$	propositions 1.27, 1.29, théorème 1.30
1.32	Équipotence de $\mathbb{R}$ et de $[0, 1]$	$\mathbb{R} \approx [0, 1]$	proposition 1.29, théorème 1.30, prérequis 5
1.35	Théorème de Cantor	aucune surjection de E sur $\mathcal{P}(E)$	définitions 1.10, 1.21, notation 1.7
1.36	Hiérarchie stricte	$E \preccurlyeq \mathcal{P}(E)$ et $\mathcal{P}(E) \not\preccurlyeq E$	théorème 1.35, proposition 1.29
1.41	Parties infinies de $\mathbb{N}$	toute partie infinie de $\mathbb{N}$ est dénombrable	définition 1.40, prérequis 1, 2, 4
1.42	Caractérisation de « au plus dénombrable »	E au plus dénombrable équivaut à $E \preccurlyeq \mathbb{N}$	lemme 1.41, propositions 1.27, 1.29
1.44	Bijectivité du couplage de Cantor	$\langle \cdot, \cdot \rangle$ est une bijection de $\mathbb{N}^2$ sur $\mathbb{N}$	notation 1.43, lemme 1.13, prérequis 1, 4
1.45	Puissances de $\mathbb{N}$	$\mathbb{N}^k \approx \mathbb{N}$ pour tout $k \geq 1$	proposition 1.44, lemme 1.13
1.46	Réunion au plus dénombrable	une réunion indexée d'ensembles munis d'injections données est au plus dénombrable	propositions 1.44, corollaire 1.42, prérequis 1
1.47	Mots sur un alphabet au plus dénombrable	E au plus dénombrable entraîne E^* au plus dénombrable	propositions 1.44, corollaire 1.42, lemme 1.13, prérequis 2
1.48	Dénombrabilité de $\mathbb{Z}$ et de $\mathbb{Q}$	$\mathbb{Z} \approx \mathbb{N}$ et $\mathbb{Q} \approx \mathbb{N}$	proposition 1.44, théorème 1.30, corollaire 1.42, prérequis 3
1.49	Non-dénombrabilité de $\mathcal{P}(\mathbb{N})$	$\mathcal{P}(\mathbb{N})$ n'est pas au plus dénombrable ; $\mathcal{P}(E)$ s'identifie aux fonctions de E dans $\{0, 1\}$	corollaires 1.36, 1.42, définition 1.6

Glossaire du module

Terme	Définition en une phrase	Numéro de la définition formelle
principe de compréhension non restreinte	principe affirmant que toute propriété détermine un ensemble	1.1
égal (ensembles)	ayant exactement les mêmes éléments	1.6
extensionnalité	principe selon lequel un ensemble est déterminé par ses éléments	1.6
inclus, inclusion	tout élément du premier est élément du second, l'égalité étant exclue dans le cas strict	1.6
stricte		
complémentaire	ensemble des éléments de l'ambient qui n'appartiennent pas à la partie	1.8
couple	objet $\{\{a\}, \{a, b\}\}$ codant la donnée ordonnée de a puis b	1.12
produit cartésien	ensemble des couples formés d'un élément de chaque facteur	1.12
n -uplet	couple itéré à gauche, défini par récurrence sur n	1.12
mot vide	unique suite finie de longueur nulle	1.12
relation binaire	partie du produit cartésien d'un ensemble par lui-même	1.16
réflexive, symétrique, transitive, antisymétrique	quatre propriétés élémentaires d'une relation binaire	1.16
relation d'équivalence	relation binaire réflexive, symétrique et transitive	1.17
classe d'équivalence, ensemble quotient	ensemble des éléments équivalents à un élément donné ; ensemble de toutes les classes	1.17
fonction partielle, fonction totale	graphe fonctionnel ; graphe fonctionnel défini partout	1.19
domaine, image	ensemble des arguments où la fonction est définie ; ensemble des valeurs prises	1.19
image directe, image réciproque	ensemble des valeurs prises sur une partie de la source ; ensemble des arguments dont la valeur tombe dans une partie du but	1.20
restriction, composée, identité	fonction limitée à une partie ; application successive de deux fonctions ; fonction laissant tout élément inchangé	1.20
injective, surjective, bijective	valeurs distinctes en des arguments distincts ; toute valeur atteinte ; les deux à la fois	1.21
équipotents	reliés par une bijection	1.26
subpotent	source d'une injection totale vers l'autre ensemble	1.28
fini, infini	équipotent à un segment initial de $\mathbb{N}$; non fini	1.40
dénombrable, au plus dénombrable	équipotent à $\mathbb{N}$; fini ou dénombrable	1.40

Pièges fréquents

Confondre appartenance et inclusion. Les relations $x \in E$ et $\{x\} \subseteq E$ sont équivalentes,

mais $x \subseteq E$ et $\{x\} \in E$ disent tout autre chose. L'exemple 1.11 est le test minimal : $\emptyset \subseteq E$ pour tout E , alors que $\emptyset \in E$ est une assertion sur les éléments de E , fautive par exemple pour $E := \{\{\emptyset\}\}$. Cette confusion devient dévastatrice au module 16, où l'appartenance est le seul symbole primitif du langage.

Croire que le paradoxe de Russell interdit $x \in x$. Le théorème 1.2 ne réfute pas l'énoncé « il existe un ensemble élément de lui-même » : il réfute le principe de compréhension non restreinte. C'est un axiome supplémentaire, la fondation, qui exclura les appartenances circulaires (module 16). Le paradoxe porte sur la formation des ensembles, pas sur leur contenu.

Écrire « dénombrable » pour « au plus dénombrable ». La Charte § 7 réserve « dénombrable » au cas infini. La littérature anglo-saxonne emploie *countable* dans les deux sens, ce qui rend ambigus des énoncés tels que « toute théorie sur un langage dénombrable admet un modèle dénombrable ». Dans tout le parcours, écrire « au plus dénombrable » lorsque le cas fini est admis.

Transporter au cas infini les intuitions du cas fini. Un ensemble infini est équipotent à certaines de ses parties strictes (exercice 1.33), ce qui n'arrive jamais pour un ensemble fini. L'inclusion stricte $A \subsetneq B$ n'entraîne donc jamais, à elle seule, la non-équipotence de A et B ; seul un argument diagonal (théorème 1.35) ou une comparaison par le théorème 1.30 permet de conclure.

Employer le théorème de Cantor–Schröder–Bernstein comme un principe de comparabilité. Le théorème 1.30 dit que deux injections opposées produisent une bijection. Il ne dit pas que, de deux ensembles quelconques, l'un est toujours subpotent à l'autre : cette comparabilité universelle est équivalente à l'axiome du choix (module 17). Le théorème 1.30, lui, ne requiert aucune forme de choix.

Utiliser l'axiome du choix sans le voir. Trois formulations en apparence anodines le dissimulent : « toute surjection admet un inverse à droite » (contre-exemple à la réciproque de la proposition 1.22, point 3), « toute réunion au plus dénombrable d'ensembles au plus dénombrables est au plus dénombrable » (remarque suivant la proposition 1.46) et « tout ensemble infini contient une partie dénombrable » (exercice 1.53). Le signal d'alarme est toujours le même : une infinité de sélections simultanées, sans règle uniforme qui désigne l'élément choisi.

Confondre la bijection réciproque et l'image réciproque. L'écriture $f^{-1}[B]$ a un sens pour toute fonction, y compris non injective, tandis que f^{-1} seul n'a de sens que pour une bijection (notation 1.20, proposition 1.22). Écrire $f^{-1}(y)$ pour désigner l'ensemble des antécédents de y est une faute de notation dans ce parcours : il faut écrire $f^{-1}[\{y\}]$.

Traiter l'hypothèse du continu comme une question ouverte. La proposition 1.49 établit une inégalité stricte, non l'absence d'intermédiaire. L'existence d'un cardinal intermédiaire est indécidable dans ZFC (remarque 1.50) : c'est un résultat démontré, non une lacune de la recherche.

Notations introduites

Les notations suivantes sont introduites ou fixées dans ce module. Celles qui *ne figurent pas dans la Charte* sont signalées par une mention explicite dans la dernière colonne, conformément à la Charte § 1 ; elles sont reprises dans l'encadré de tête.

Notation	Lecture / signification	Variantes rencontrées dans la littérature
$\{x \mid P(x)\}$	compréhension non restreinte, illégitime hors de la définition 1.1 et du théorème 1.2	$\{x : P(x)\}, \{x; P(x)\}$
$\{x \in E \mid P(x)\}$	compréhension restreinte à un ensemble donné (notation 1.7)	$\{x \in E : P(x)\}, \{x \in E; P(x)\}$
$A \subseteq B, A \subsetneq B$	inclusion large, inclusion stricte	$A \subset B$ (ambigu), $A \subsetneq B$
$\emptyset$	ensemble vide	$\emptyset, \{\}$
$\complement_E A$	complémentaire de A dans E	$A^c, \bar{A}, E \setminus A$
$\mathcal{P}(E)$	ensemble des parties de E	$\mathfrak{P}(E), 2^E, \text{Pow}(E)$
(a, b)	couple de Kuratowski $\{\{a\}, \{a, b\}\}$	$\langle a, b \rangle$
E^n, E^*	puissance cartésienne ; suites finies d'éléments de E	$E^{<\omega}, \text{Seq}(E), \text{List}(E)$
ε	mot vide, unique élément de E^0	λ, Λ , mot vide noté 1 — <i>hors Charte</i> (encadré de tête)
$x R y, [x]_R, E/R$	relation infix, classe d'équivalence, ensemble quotient	$x R y, \bar{x}, E/\sim$
$f : E \rightarrow F, f : E \rightharpoonup F$	fonction totale, fonction partielle	application ; $f : \subseteq E \rightarrow F$
$f[A], f^{-1}[B]$	image directe, image réciproque	$f(A), f''A; f^{-1}(B), f^*(B)$
$f \upharpoonright A, g \circ f, \text{id}_E$	restriction, composée, identité	$f _A; gf; \text{Id}_E, 1_E$
f^{-1}	bijection réciproque d'une bijection	$f^{\leftarrow}, \bar{f}$ — <i>hors Charte</i> (encadré de tête)
$E \approx F$	équipotence	$E \sim F, E \cong F, E = F $
$E \preccurlyeq F$	subpotence : existence d'une injection totale	$E \preceq F, E \leq F, E \leq F $ — <i>hors Charte</i> (encadré de tête)
$[n]$	segment initial $\{k \in \mathbb{N} \mid k < n\}$	$\{1, \dots, n\}$ (décalage à proscrire ici), n (au sens ordinal, module 16) — <i>hors Charte</i> (encadré de tête)
$[a, b], [a, b[$	intervalles réels fermé, semi-ouvert	$[a, b)$ (usage anglo-saxon) — <i>hors Charte</i> (encadré de tête)
$\langle m, n \rangle$	couplage de Cantor $\frac{(m+n)(m+n+1)}{2} + n$	$\pi(m, n), J(m, n), [m, n]$
χ_A	fonction caractéristique de A	$\mathbf{1}_A, c_A$

Checklist d'auto-vérification

- ✓ **Unicité des notations** — chaque concept est noté d'une seule façon dans tout le module, conformément à la § 6 ; aucune notation concurrente n'a été introduite en cours de route.
- ✓ **Notations hors Charte** — toute notation absente de la Charte est signalée dans l'encadré de tête et reprise dans la section « Notations introduites ».
- ✓ **Séparation objet / méta** — $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, \perp, \top, =$ n'apparaissent qu'à l'intérieur de formules du langage objet ; $\implies, \iff, :=$ et les quantifications en français n'apparaissent que dans le métalangage ; aucune phrase de preuve n'utilise un connecteur objet comme articulation logique.

- ✓ **Démonstration vs dérivation** — le vocabulaire distingue partout démonstration (métathéorie) et dérivation (système formel).
- ✓ **Format des environnements** — en-têtes en gras conformes au modèle ****Théorème 9.4 (Complétude)****, aucun environnement hors de la liste admise.
- ✓ **LaTeX systématique** — aucun symbole mathématique en Unicode brut ; aucun | littéral dans une cellule de tableau ; aucune formule

...

dans un tableau.

- ✓ **Numérotation** — compteur unique, continu et croissant sur tout le module, préfixé par le numéro du module.
- ✓ **Renvois** — tous les renvois sont numérotés et au format de la § 2.4 ; les renvois externes mentionnent le module ; aucun renvoi vague.
- ✓ **Preuves complètes** — toutes les hypothèses utilisées sont nommées, tous les cas d'induction sont traités, la méthode est annoncée en italique, la preuve se clôt par ■ ; toute étape déléguée renvoie à un exercice numéroté existant.
- **Dérivations formelles** — format linéaire à quatre colonnes, dépendances explicites, décharges signalées, conditions de variable propre vérifiées et mentionnées. (*Sans objet : ce module ne contient aucune dérivation formelle, le système de déduction n'étant introduit qu'au module 5.*)
- ✓ **Résultats nommés** — les résultats de la § 8 portent exactement leur nom canonique.
- ✓ **Glossaire** — les termes ambigus de la § 7 sont employés dans le sens retenu ; la section « Glossaire du module » couvre tous les termes nouveaux introduits en gras.
- ✓ **Gabarit** — les sept sections de la § 3 sont présentes, dans l'ordre, avec leurs titres exacts.