CARDINALITÉ

Paul Rozière
Paris Diderot – Paris 7

version du 15 juin 2022– *(824)*

L'objet de la théorie de la cardinalité est d'étendre des ensembles finis aux ensembles infinis une notion de « taille » pour les ensembles. En particulier que veut dire « avoir autant d'éléments », « avoir plus d'éléments » pour des ensembles infinis ? Les choses ne sont pas si simples que pour les ensembles finis. Galilée remarquait déjà qu'il y a autant de carrés de nombres entiers que de nombres entiers, et donc qu'une partie (l'ensemble de tous les carrés parfaits) peut être aussi grande que le tout (l'ensemble de tous les nombres entiers naturels), ce qui n'est pas possible pour les ensembles finis. Galilée est d'ailleurs très loin d'être le premier à faire ce genre de remarque.

C'est Cantor qui est véritablement à l'origine de la théorie de la cardinalité des ensembles infinis, avec un article où il montre qu'il y a autant de nombres algébriques que de nombres entiers, mais strictement plus de nombres réels, en un sens que nous allons préciser.

1 Comparer les tailles des ensembles

1.1 Équipotence

Pour comparer les tailles des ensembles finis, on compte combien chacun ont d'éléments, et on compare les entiers obtenus. Pour les ensembles infinis on ne dispose pas de façon évidente de nombres qui permettraient de compter. Mais on peut quand même essayer d'abstraire la méthode utilisée pour les ensembles finis : compter les objets d'un ensemble E, c'est leur associer des entiers naturels de 1 jusqu'à n, appelé cardinal de l'ensemble. Plus mathématiquement c'est exhiber un entier n tel qu'il y ait une bijection entre E et $\{1,\dots,n\}$, l'ensemble des n premiers entiers naturels non nuls.

On revient en fait à une façon primitive de compter : un berger pouvait compter des moutons avec des caillous sans avoir besoin de numéroter ceux-ci, et cela lui permettait quand même de savoir s'il avait perdu des moutons.

On dira donc que deux ensembles E et F sont *équipotents* quand il existe une bijection entre E et F, et on notera $E \sim F$. On parlait autrefois de la puissance d'un ensemble, pour son cardinal, d'où le terme équipotent, qui signifie intuitivement avoir même cardinal, sachant qu'on on ne sait pas pour le moment ce qu'est le cardinal d'un ensemble infini.

La relation d'équipotence est définie sur tout l'univers ensembliste : ce n'est pas une relation au sens où on l'a défini dans le chapitre sur les ensembles parce qu'elle est définie sur une classe propre, et son graphe est aussi une classe propre. Mais en dehors de cela elle a toutes les propriétés d'une relation d'équivalence :

— elle est réflexive car un ensemble est équipotent à lui-même par l'identité ;
— elle est symétrique car une bijection f a une bijection réciproque f^{-1} de graphe symétrique ;
— elle est transitive car la composition de deux bijections est une bijection.

Une idée pour définir une notion de nombre qui s'étend aux nombres infinis pourraient être de considérer les classes d'équivalence pour cette relation. Mais ces classes d'équivalence, en dehors de celle de l'ensemble vide, sont toutes des classes propres : on l'a vu en exercice pour la classe des singletons (évidement deux singletons sont en bijection, et un ensemble en bijection avec un singleton est un singleton, c'est donc une classe d'équivalence pour l'équipotence). Ce n'est pas très difficile de généraliser la démonstration à une classe d'équipotence quelconque qui n'est pas réduite au seul ensemble vide. Si on procédait ainsi, les nombres ne seraient pas des objets, on ne pourrait pas parler d'ensembles de nombres : ce n'est pas une bonne façon de procéder, du moins dans le cadre de la théorie des ensembles tel qu'il a été introduit.

Une autre idée consiste à obtenir dans chaque classe d'équipotence un ensemble de référence, que l'on choisit comme étant le cardinal des ensembles de cette classe. Pour les ensembles finis, ce sont par exemple les ensembles d'entiers $\{1,\dots,n\}$, les $\{x \in \mathbb{N}^* \ / \ x \leqslant n\}$. On pourrait aussi choisir les $\{x \in N \ / \ x < n\}$, mais de toute façon il s'agit un ensemble caractérisé par l'entier n, et on retrouve alors la notion habituelle de cardinal pour les ensembles finis. On démontrera un peu plus loin qu'à deux entiers distincts correspondent bien deux classes d'équipotence distinctes, ce qui est une propriété arithmétique appelée théorème des tiroirs de Dirichlet.

La théorie des ensembles permet de construire de tels ensembles de référence pour les ensembles bien ordonnés et, avec l'axiome du choix, pour les ensembles en général, mais c'est hors sujet dans ce cours. On va donc se contenter de la relation d'équipotence et distinguer tout de même deux ensembles de référence infinis :

— l'ensemble $\mathbb{N}$ des entiers naturels : les ensembles équipotents à $\mathbb{N}$ sont appelé ensembles dénombrables, le cardinal correspondant, le dénombrable, est noté $\aleph_0$ (où $\aleph$ est la lettre hébraïque aleph) ;

— l'ensemble $\mathscr{P}(\mathbb{N})$ des parties de $\mathbb{N}$: on verra que $\mathbb{R}$ est équipotent à $\mathscr{P}(\mathbb{N})$, et le cardinal correspondant est appelé *cardinal du continu*, ou *puissance du continu*; il est noté $2^{\aleph_0}$.

Le théorème de Cantor (voir ci-dessous la section 1.4), assure que ces deux ensembles ne sont pas en bijection, mais aussi qu'il existe des ensembles qui ne sont en bijection avec aucun de ces deux ensembles.

On peut définir un cardinal noté $\aleph_1$, qui est celui de l'ensemble des classes d'isomorphismes de bons ordres qu'on peut définir sur $\mathbb{N}$ (intuitivement des classes d'isomorphisme de bons ordres dénombrables, mais les classes ainsi définies ne seraient pas des ensembles). On peut également montrer qu'il n'est pas en bijection avec $\mathbb{N}$, donc différent de $\aleph_0$. En un certain sens, qu'il faudrait préciser, c'est le cardinal successeur de $\aleph_0$ d'où son nom $\aleph_1$.

Cantor s'est posé la question de savoir si $\mathbb{R}$ est équipotent à $\aleph_1$, c'est-à-dire si $\aleph_1$ et $2^{\aleph_0}$ sont le même cardinal. C'est ce qu'on appelle *l'hypothèse du continu*. Gödel a démontré en 1938 que c'est possible (on ne peut pas démontrer qu'ils sont différents). Cohen a démontré en 1963 que ce n'est pas démontrable. Au final on peut ajouter comme axiome l'hypothèse du continu ou sa négation sans que la théorie ne soit contradictoire (du moins si elle ne l'est pas au départ). Pour tout ce qui suit on n'aura aucune raison de supposer que $\aleph_1$ et $2^{\aleph_0}$ sont égaux ou différents.

1.2 Subpotence

La subpotence permet de comparer des ensembles du point de vue de leur cardinal. Si $m \leqslant n$ il existe une injection évidente de $\{1,\dots,m\}$ dans $\{1,\dots,n\}$, et donc il existe une injection d'un ensemble cardinal m dans un ensemble de cardinal n par composition. On généralise.

Un ensemble E est dit *subpotent* à un ensemble F quand il existe une injection de E dans F, et on note $E \preccurlyeq F$.

À nouveau c'est une relation définie sur tout l'univers ensembliste, et dont le graphe est une classe propre. Mais en dehors de cela elle a les propriétés d'une relation de préordre, c'est-à-dire :

— qu'elle est réflexive, car un ensemble est subpotent à lui-même par l'identité ;

— qu'elle est transitive, car la composition de deux injections est une injection.

Pour qu'elle joue le rôle d'une relation d'ordre sur les cardinaux, on a besoin d'une propriété supplémentaire, qui correspond à ce que serait l'anti-symétrie sur les cardinaux. C'est le théorème de Cantor-Bernstein.

Théorème 1.1 (Cantor-Bernstein) *Étant donnés deux ensembles E et F, s'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection entre E et F, soit :*

$$(E \preccurlyeq F \text{ et } F \preccurlyeq E) \Rightarrow E \sim F\,.$$

Comme une injection est une bijection, la réciproque est évidente, et la relation de subpotence est compatible avec l'équipotence.

On remet à une section ultérieure la démonstration du théorème de Cantor-Bernstein. On peut aussi se poser la question de savoir si cette relation d'ordre est totale, c'est-à-dire si étant donné deux ensembles E et F, il existe toujours une injection de E dans F ou de F dans E. La réponse est oui, mais

demande une utilisation forte de l'axiome du choix. C'est hors du périmètre de ce cours, voir le polycopié de Jean-Louis Krivine si vous êtes intéressés. On peut même montrer qu'il n'est pas possible de le démontrer sans axiome du choix.

1.3 Subpotence stricte

Pour définir la subpotence stricte, il faut penser que l'on cherche à comparer les ensembles du point de vue de leur cardinalité : un ensemble E est dit *strictement subpotent* à un ensemble F quand il existe une injection de E dans F et il n'existe pas de bijection entre E et F, et on note $E \prec F$.

1.4 Le théorème de Cantor

1.4.1 Version ensembliste

Le théorème de Cantor énonce qu'un ensemble E n'est pas en bijection avec l'ensemble de ses parties $\mathscr{P}(E)$. Comme il y a une injection évidente de E dans $\mathscr{P}(E)$ en associant à un élément le singleton auquel il appartient :

$$\begin{array}{rccc} \varphi : & E & \to & \mathscr{P}(E) \\ & x & \mapsto & \{x\} \end{array}$$

le théorème de Cantor se reformule ainsi.

Théorème 1.2 (théorème de Cantor) *Pour tout ensemble E, E est strictement subpotent à $\mathscr{P}(E)$.*

La démonstration du théorème de Cantor est très courte mais utilise un raisonnement assez inhabituel, que l'on a appelé raisonnement diagonal. Nous avons déjà vu un exemple de raisonnement diagonal avec le paradoxe de Russell. Ce n'est pas étonnant car Russell s'est justement inspiré du théorème de Cantor et de cette démonstration pour son paradoxe.

Le théorème de Cantor est une conséquence immédiate du lemme suivant, qui énonce qu'aucune fonction de E dans $\mathscr{P}(E)$ n'est surjective : il n'existe donc pas de bijection de E dans $\mathscr{P}(E)$.

Lemme 1.3 *Soit E un ensemble et f une fonction définie sur E à valeur dans $\mathscr{P}(E)$. Alors il existe un sous-ensemble D de E tel que $D \notin \operatorname{Im} f$ (c'est-à-dire que f n'est pas surjective).*

Démonstration. On définit $D = \{x \in E \ / \ x \notin f(x)\}$. Montrons par l'absurde que $D \notin \operatorname{Im} f$: supposons $D \in \operatorname{Im} f$, et posons d tel que $D = f(d)$. On distingue deux cas suivant que $d \in f(d)$ ou $d \notin f(d)$ (tiers exclu) :

$d \in f(d)$ **:** comme $D = f(d)$, $d \notin f(d)$ par définition de D ; contradiction ;

$d \notin f(d)$ **:** alors par définition de D, $d \in D$, or $D = f(d)$: c'est à nouveau une contradiction.

Remarque : formellement il est possible d'enchaîner les deux cas, sans utiliser le tiers exclu. ■

Le nom de « raisonnement diagonal » vient de ce que l'on travaille sur la diagonale $\{(x, f(x) \ / \ x \in E\}$ du graphe de f.

Le théorème de Cantor est surtout intéressant quand l'ensemble E est infini : quand il est fini, il peut se ramener à un résultat d'arithmétique. Cependant la démonstration qui précède ne suppose rien sur E.

1.4.2 Version fonctionnelle

À un sous-ensemble A de E on associe sa fonction caractéristique :

$$\begin{array}{rccc} 1_A : & E & \to & \{0,1\} \\ & x \in A & \mapsto & 1 \\ & x \notin A & \mapsto & 0 \end{array}$$

Clairement la fonction $A \mapsto 1_A$ définit une bijection de $\mathscr{P}(E)$ dans $\{0,1\}^E$. On peut reformuler le lemme du raisonnement diagonal précédent ainsi.

Lemme 1.4 *Soit E un ensemble et $(f_i)_{i\in E}$ une famille de fonctions de $\{0,1\}^E$ ($f_i : E \to \{0,1\}$) indexée par E. Alors il existe une fonction $g : E \to \{0,1\}$ telle que pour tout $i \in E$, $g \neq f_i$ (c'est-à-dire que la fonction $: i \mapsto f_i$ n'est pas surjective).*

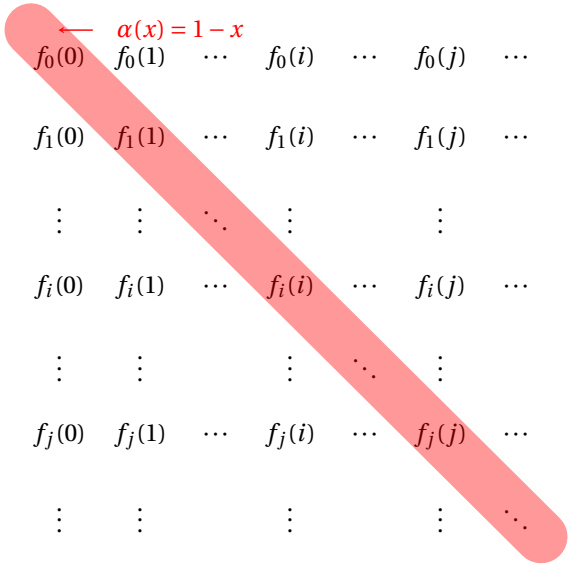


FIGURE 1 – Illustration (en prenant $E = \mathbb{N}$) ; la fonction α est composée avec la fonction diagonale $i \mapsto f_i(i)$ pour donner g

Démonstration. On définit g sur E par $g(x) = 1 - f_x(x)$, $x \in E$. Si $g = f_i$ pour un certain i, alors pour ce même i, $g(i) = 1 - f_i(i)$: contradiction. ■

Quand on l'examine de près, la démonstration est vraiment identique à la précédente, mais sous cette forme elle est plus adaptable à d'autres situations, par exemple à l'exercice suivant.

Exercice 1 Le but de l'exercice est de montrer directement que $\mathbb{R}$ n'est pas équipotent à $\mathbb{N}$ sans utiliser le théorème **??** (on obtient aussi le résultat en montrant que $\mathbb{R} \sim \mathscr{P}(\mathbb{N})$, voir la suite).

1. Soit Dec $:= \{0,1,\ldots,8,9\}^{\mathbb{N}}$ l'ensemble de toutes les suites $\bar{a} = (a_n)_{n\in\mathbb{N}}$ telles que $a_n \in \{0,1,\ldots,9\}$ pour tout n. Soit $\alpha : \{0,\ldots,9\} \to \{0,\ldots,9\}$, définie par

$$\alpha(i) = \begin{cases} 1 & \text{si } i \neq 1 \\ 2 & \text{si } i = 1. \end{cases}$$

   Soit $\left(\bar{a}^k\right)_{k\in\mathbb{N}}$ une famille d'éléments de Dec ($\bar{a}^k = (a_n^k)_{n\in\mathbb{N}}$ est une suite, l'exposant k est un indice haut, il ne désigne pas une puissance), et soit $\mathscr{A} \subset$ Dec l'ensemble des éléments de la famille. Montrer que $\left(\alpha(a_n^n)\right)_{n\in\mathbb{N}} \notin \mathscr{A}$.
2. Quel est l'ensemble des réels dont le développement décimal est $0,\bar{a}$ pour $\bar{a} \in$ Dec ? En utilisant le développement décimal des nombres réels, conclure que l'intervalle $[0,1]$ de $\mathbb{R}$ n'est pas dénombrable (faire attention au fait qu'un nombre décimal possède deux représentations décimales, par contre pour un nombre réel non décimal possède une unique représentation décimale).
3. En déduire que $\mathbb{R} \not\sim \mathbb{N}$.

1.5 Le théorème de Cantor-Bernstein

Soient A et B deux ensembles tels qu'il existe une injection f de A dans B et une injection g de B dans A. Pour simplifier l'expression du raisonnement, mais sans perte de généralité, On suppose que

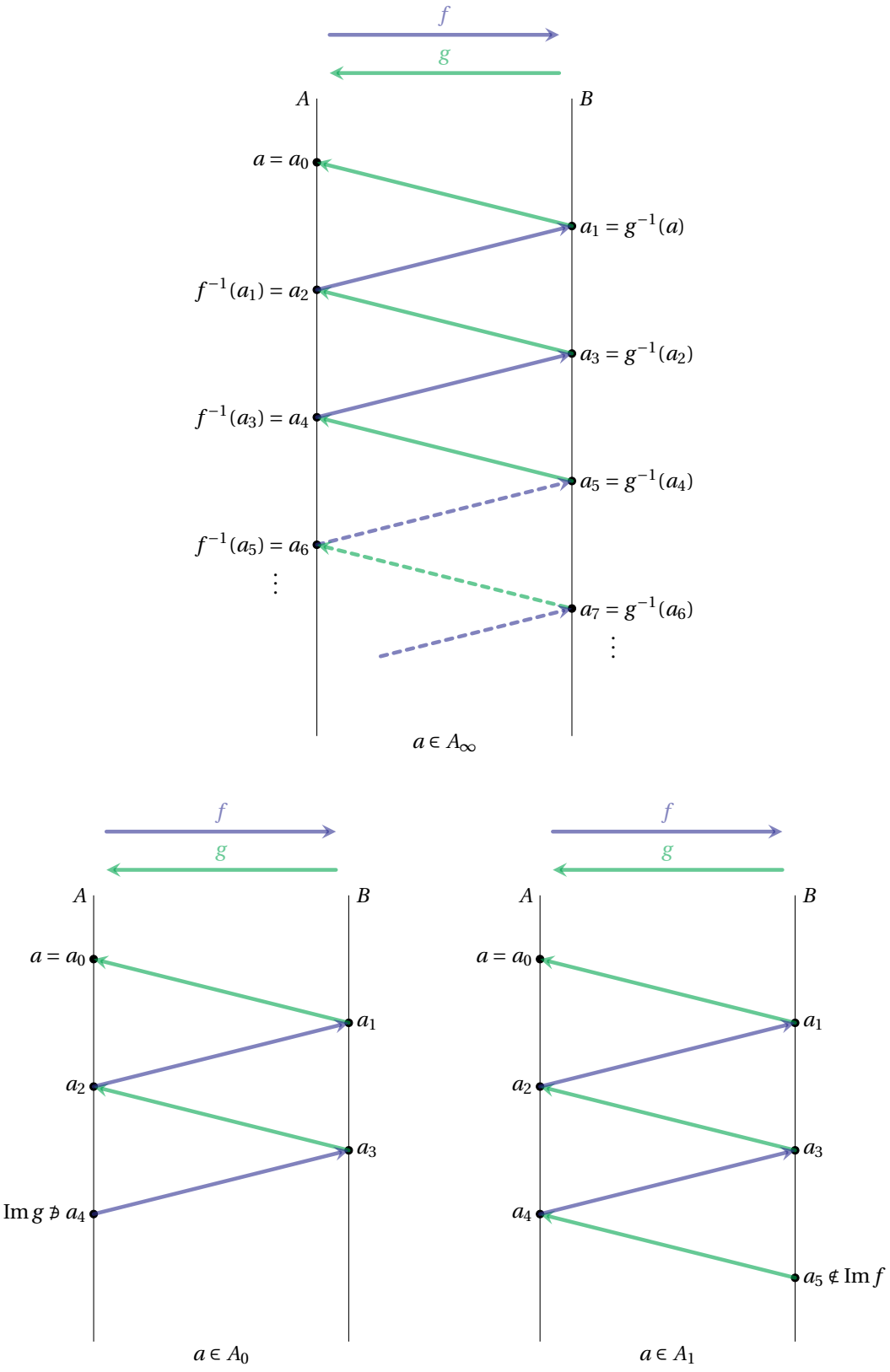


FIGURE 2 – A est partitionné en $A = A_\infty \cup A_0 \cup A_1$ et B de même en $B = B_\infty \cup B_0 \cup B_1$:
f est bijective de A_0 dans B_1, g^{-1} est bijective de A_1 dans B_0, f et g sont bijectives de A_∞ dans B_∞.

A et B sont disjoints. Il est facile d'en déduire le résultat général : prendre $A' = A \times \{0\}$, $B' = B \times \{1\}$, qui sont disjoints, et trivialement en bijection A' avec A, et B' avec B.

À chaque élément a de A on associe une suite $(a_n)_{n\in\mathbb{N}}$ définie par récurrence à partir de $a_0 = a$ en prenant à chaque fois l'unique antécédent par f (pour un élément de A, rang pair) ou par g (pour un élément de B, rang impair) s'il existe :

$$\begin{array}{lcl} a_0 & = & a \\ a_{2n+1} & = & g^{-1}(a_{2n}) \text{ si } a_{2n} \in \operatorname{Im} g \text{ non défini sinon} \\ a_{2n+2} & = & f^{-1}(a_{2n}) \text{ si } a_{2n+1} \in \operatorname{Im} f \text{ non défini sinon} \end{array}$$

Comme les fonctions f et g ne sont pas forcément surjectives, il est tout à fait possible de tomber à un moment sur un élément qui n'a pas d'antécédent, auquel cas la suite est finie, voire même le a de départ peut ne pas avoir d'antécédent, auquel cas la suite est même réduite à a. Mais la suite peut aussi être infinie.

On associe de façon analogue à chaque élément b de B une suite $(b_n)_{n\in\mathbb{N}}$.

On partitionne A en 3 parties $A_0,\ A_1,\ A_\infty$, soit $a \in A$:

— si la suite (a_n) associée à a s'arrête « du même côté» sur un élément de A, alors $a \in A_0$ (cela revient à dire que le dernier terme de la suite est de rang pair) ;

— si la suite (a_n) associée à a s'arrête « de l'autre côté » sur un élément de B, alors $a \in A_1$ (cela revient à dire que le dernier terme de la suite est de rang impair) ;

— si la suite (a_n) associée à a continue indéfiniment, alors $a \in A_\infty$.

Par exemple si $a \notin \operatorname{Im} g$, alors $a \in A_0$, si $a = f(b)$ mais $b \notin \operatorname{Im} f$, alors $a \in A_1$, etc. C'est bien une partition de A car, évidemment, au moins l'un des trois cas est réalisé, et ces trois cas sont exclusifs du fait que $A \cap B = \emptyset$ [1].

On définit de la même façon une partition de B en trois parties $B_0,\ B_1,\ B_\infty$, soit $b \in B$:

— si la suite (b_n) associée à b s'arrête « du même côté» sur un élément de B, alors $b \in B_0$;

— si la suite (b_n) associée à b s'arrête « de l'autre côté » sur un élément de B, alors $b \in B_1$;

— si la suite (b_n) associée à b continue indéfiniment, alors $b \in B_\infty$.

On observe maintenant que si $a \in A_0$, avec pour suite associée $(a_0, \ldots, a_{2n})$, alors la suite associée à $b = f(a)$ est $(b, a_0, \ldots, a_{2n})$, c'est-à-dire que $b \in B_1$ ($a_{2n} \in A$). Réciproquement, si $b \in B_1$, la suite associée à b est de rang impair, donc $b \in \operatorname{Im} f$, $b = f(b_1)$, et $b_1 \in A$ appartient à A_0 (car la suite associée est la suite associée à B sans le premier élement, et se termine donc de même sur A). L'injection f induit donc une bijection de A_0 dans B_1.

Par symétrie, le même raisonnement montre que l'injection g induit une bijection de B_0 dans A_1.

Par un raisonnement analogue il est clair que l'injection f induit une bijection de A_∞ dans B_∞ (on aurait pu aussi bien prendre g).

En regroupant ces trois bijections, on obtient une bijection de A dans B

$$\begin{array}{lcl} A_0 & \xrightarrow{f} & B_1 \\ A_1 & \xleftarrow{g^{-}1} & B_0 \\ A_\infty & \xrightarrow{f} & B_\infty \end{array}$$

■

Cette preuve est un exemple de preuve non constructive : elle donne l'existence d'une bijection, mais, en suivant la preuve on ne peut pas « construire effectivement » la bijection. Pour préciser : pour que cela ait un sens on peut supposer que l'on a les ensembles A et B énumérés chacun par un programme informatique, et que chacune des deux injections f et g peut également être calculée par un programme informatique. Par exemple pour la fonction f, être calculée par un programme signifie que si on fournit en entrée à ce programme un élément de A, il produit en sortie $f(a)$.

En utilisant ces programmes, on pourra écrire un nouveau programme qui, avec $a \in A$ en entrée, calcule la suite (a_n), jusqu'à un rang arbitraire. Mais cela ne donne pas de moyen systématique de savoir auquel des ensembles $A_0,\ A_1,\ A_\infty$ l'élément a appartient car la suite (a_n) peut être infinie : si elle est finie, on le saura un jour, mais tant que le calcul ne s'est pas arrêté on ne sait pas si c'est parce que la

1. Si on définit A_0 et A_1 uniquement en terme de partité du dernier élément de la suite, l'hypothèse $A \cap B = \emptyset$ n'est plus nécessaire.

suite (a_n) est réellement infinie, ou si c'est parce qu'elle est finie mais qu'on n'a pas encore trouvé le dernier élément.

Par comparaison, la démonstration du lemme du théorème de Cantor est constructive, au sens où, avec les hypothèses que les données sont calculables, la fonction diagonale est calculable.

2 Compatibilité avec les opérations ensemblistes

La relation d'équipotence est compatible avec certaines opérations ensemblistes, pas en général avec la réunion ni l'intersection, mais avec la réunion disjointe, le produit cartésien et l'exponentiation ensembliste. De plus on a des bijections « canoniques » qui donnent des relations d'équipotence bien utiles en cardinalité. On rappelle que $A \uplus B = A \times \{0\} \cup B \times \{1\}$.

Proposition 2.1 *Si les ensembles A, A', B et B' vérifient $A \sim A'$ et $B \sim B'$, alors :*

- $A \uplus B \sim A' \uplus B'$;
- $A \times B \sim A' \times B'$;
- $B^A \sim B'^{A'}$.

Soient des ensembles A, B et C, alors :

- *Si $A \cap B = \emptyset$, $A \cup B \sim A \uplus B$;*
- $A \uplus B \sim B \uplus A$;
- $A \times B \sim B \times A$;
- $\mathscr{P}(A) \sim \{0,1\}^A$;
- $C^{A \uplus B} \sim C^A \times C^B$;
- $C^{A \times B} \sim \left(C^B\right)^A$.

Démonstration. Pour les premières équipotences la bijection est immédiate. On a déjà mentionné $\mathscr{P}(A) \sim \{0,1\}^A$ (voir section 1.4.2). Voyons les deux dernières.

— Soient :

$$\begin{array}{rccc} \varphi : & C^{A \uplus B} & \to & C^A \times C^B \\ & f & \mapsto & (f_1, f_2) \end{array} \qquad \begin{array}{rccc} f_1 : & A & \to & C \\ & x & \mapsto & f(x,0) \end{array} \qquad \begin{array}{rccc} f_2 : & B & \to & C \\ & y & \mapsto & f(y,1) \, . \end{array}$$

Alors φ est évidemment bijective, f se définit par cas à partir de f_1 et f_2.

— Soient

$$\begin{array}{rccc} \varphi : & C^{A \times B} & \to & C^{B^A} \\ & f & \mapsto & \hat{f} \end{array} \qquad \begin{array}{rccc} \hat{f} : & A & \to & C^B \\ & x & \mapsto & f_x \end{array} \qquad \begin{array}{rccc} f_x : & B & \to & C \\ & y & \mapsto & f(x,y) \, . \end{array}$$

Alors φ est bijective de réciproque ψ :

$$\begin{array}{rccc} \psi : & C^{B^A} & \to & C^{A \times B} \\ & g & \mapsto & \check{g} \end{array} \qquad \begin{array}{rccc} \check{g} : & A \times B & \to & C \\ & (x,y) & \mapsto & g(x)(y) \, . \end{array}$$

■

3 Cardinalité finie

3.1 Définitions

On utilise dans ce qui suit $\{1, \dots, n\}$ comme notation pour $\{i \in \mathbb{N} \,/\, 1 \leqslant i \leqslant n\}$. En particulier si $n = 0$, $\{1, \dots, n\} = \emptyset$.

Un ensemble E est dit *fini* quand il existe un entier n tel que E est équipotent à $\{1, \dots, n\}$. Pour montrer qu'un tel entier est unique, on va passer par deux lemmes.

Lemme 3.1 *Soit E un ensemble fini non vide, c'est-à-dire que pour un certain entier n, E est en bijection avec $\{1, \dots, n\}$. Alors $n > 0$, et, pour $a \in E$, $E \setminus \{a\}$ est fini et en bijection avec $\{1, \dots, n-1\}$.*

Démonstration. On note g une bijection de E dans $\{1, \dots, n\}$. Comme E est non vide il ne peut être en bijection avec l'ensemble vide donc $n \neq 0$. Soit $a \in E$, on distingue alors deux cas.

$g(a) = n$ **:** alors, g définit par restriction une bijection de $E \setminus \{a\}$ dans $\{1, \dots, n-1\}$.

$g(a) \neq n$ **:** soit $b \in E$ tel que $g(b) = n$. La transposition t de E qui échange a et b :

$$\begin{array}{rccll} t: & E & \to & E & \\ & a & \mapsto & b & \\ & b & \mapsto & a & \\ & x & \mapsto & x & \text{si } x \notin \{a, b\} \end{array}$$

est bijective. La fonction $g \circ t : E \mapsto \{1, \ldots, n\}$ est alors bijective et on est ramené au cas précédent avec $g \circ t(a) = n$. ■

L'énoncé du lemme suivant est un peu contourné, justement car on n'a pas encore démontré l'unicité qui permettrait de parler *du* cardinal de E.

Lemme 3.2 *Soit E un ensemble tel qu'il existe une injection f de E dans $\{1, \ldots, n\}$, alors E est fini. De plus si E est équipotent à $\{1, \ldots, p\}$, alors $p \leqslant n$, et $p < n$ si f n'est pas surjective.*

Démonstration. La démonstration se fait par récurrence sur n.

$n = 0$ **:** Dans ce cas $\{1, \ldots, n\} = \emptyset$. l'injection f est de graphe vide (comme toute fonction à image dans $\emptyset$), donc $E = \emptyset$. Si $E = \emptyset$ est en bijection avec $\{1, \ldots, p\}$, c'est que $\{1, \ldots, p\} = \emptyset$, donc $p = 0$.

$n \to n+1$ **:** on suppose (hypothèse de récurrence) que pour tout ensemble E, s'il existe une injection h de E dans $\{1, \ldots, n\}$ alors :

— E est fini, c'est-à-dire en bijection avec $\{1, \ldots, q\}$ pour un certain entier q ;

— pour tout entier p, si E est en bijection avec $\{1, \ldots, p\}$, alors $p \leqslant n$, et si h n'est pas bijective $p < n$.

Soit $f : E \to \{1, \ldots, n+1\}$, f injective. On distingue alors deux cas suivant que $n+1$ est atteint par f ou non.

$n+1 \notin \operatorname{Im} f$ **:** alors, par restriction de l'ensemble d'arrivée, f définit une injection de E dans $\{1, \ldots, n\}$ et le résultat se déduit immédiatement de l'hypothèse de récurrence.

$n+1 \in \operatorname{Im} f$ **:** soit $a \in E$ tel que $f(a) = n+1$. Alors f définit par restriction une injection f_a de $E \setminus \{a\}$ dans $\{1, \ldots, n\}$, et donc par hypothèse de récurrence $E \setminus \{a\}$ est fini, et en bijection avec $\{1, \ldots, q\}$ pour un certain entier q par une certaine fonction g. On peut alors compléter g en une bijection $\overline{g}$ de E dans $\{1, \ldots, q+1\}$:

$$\begin{array}{rccll} \overline{g}: & E & \to & \{1, \ldots, q+1\} & \\ & a & \mapsto & q+1 & \\ & x & \mapsto & g(x) & \text{si } x \neq a \end{array}$$

C'est-à-dire que E est fini. Supposons maintenant que E soit en bijection avec $\{1, \ldots, p\}$. Le résultat et évident si $E = \emptyset$. On suppose donc $E \neq \emptyset$. D'après le lemme 3.1, $p > 0$ et il existe une bijection g de $E \setminus \{a\}$ dans $\{1, \ldots, p-1\}$. On peut appliquer l'hypothèse de récurrence pour f_a et $p-1$: $p-1 \leqslant n$ donc $p \leqslant n+1$. De plus si f n'est pas surjective, f_a non plus, donc par hypothèse de récurrence $p-1 < n$ d'où $p < n+1$. ■

Proposition 3.3 *Si E est un ensemble fini, alors il existe un unique entier n tel que E est équipotent à $\{1, \ldots, n\}$.*

Démonstration. Si E est équipotent à $\{1, \ldots, n\}$ et $\{1, \ldots, m\}$, alors d'après le lemme 3.2, $m \leqslant n$ et $n \leqslant m$, donc $m = n$. ■

On peut maintenant définir le *cardinal d'un ensemble fini E* comme l'unique entier n tel que E est équipotent à $\{1, \ldots, n\}$, et on note $\operatorname{card} E$ cet entier.

3.2 Comparaison des ensembles finis

Une fois que l'on a défini le cardinal d'un ensemble fini, il est possible de réénoncer le lemme 3.2 de façon plus familière.

Proposition 3.4 *Soient A et B deux ensembles tels que B est fini et tels qu'il existe une injection f de A dans B. Alors A est fini et $\operatorname{card} A \leqslant \operatorname{card} B$. Si de plus f n'est pas surjective, alors $\operatorname{card} A < \operatorname{card} B$. En particulier tout sous-ensemble strict d'un ensemble fini B est fini et de cardinal strictement inférieur à celui de B :*

$$\text{pour } B \text{ fini : } A \subseteq B \Rightarrow \operatorname{card} A \leqslant \operatorname{card} B \ ; \quad A \subsetneq B \Rightarrow \operatorname{card} A < \operatorname{card} B \ .$$

On obtient par contraposée (et totalité de l'ordre sur $\mathbb{N}$) le lemme des tiroirs de Dirichlet.

Corollaire 3.5 (lemme des tiroirs) *Soient A et B deux ensembles finis tels que $\operatorname{card} A > \operatorname{card} B$. Alors pour toute fonction $f : A \to B$, il existe deux éléments de A qui ont même image par f :*

$$\exists x, x' \in A \Big(x \neq x' \text{ et } f(x) = f(x') \Big) \ .$$

Démonstration. Par contraposée de la première partie de la proposition précédente, si $\operatorname{card} A > \operatorname{card} B$ aucune fonction $f : A \to B$ n'est injective ce qu'exprime la conclusion. ■

De façon imagée : quand on répartit n chaussettes (les éléments de A) dans m tiroirs (correspondant aux éléments de B), et que $n > m$, alors l'un au moins des tiroirs contient au minimum deux chaussettes, d'où le nom du lemme.
On peut aussi comparer des ensembles finis par surjection.

Proposition 3.6 *. Soit A un ensemble fini et f une fonction surjective de A dans B. ALors B est fini et $\operatorname{card} B \leqslant \operatorname{card} A$. De plus si f n'est pas injective $\operatorname{card} B < \operatorname{card} A$.*

Démonstration. Soit A fini, $n = \operatorname{card} A$, g une bijection de A dans $\{1, \dots, n\}$. Alors s'il existe une surjection f de A dans B, il existe une injection h de B dans A, donnée par $h(y) = g(\min\{n \in \mathbb{N} \ / \ f(g(n) = y\}$ (comme f est surjective $\{n \in \mathbb{N} \ / \ f(g(n) = y\}$ est non vide, et il possède un plus petit élément car $\mathbb{N}$ est bien ordonné. On a donc B fini, et $\operatorname{card} B \leqslant \operatorname{card} A$.

Si de plus f n'est pas injective, alors h n'est pas surjective (si y a plusieurs antécédents, seul celui dont l'image par g est minimale est atteint par h). Donc d'après la proposition 3.4 $\operatorname{card} B < \operatorname{card} A$.

On obtient le corollaire suivant par contraposée, à partir d'une part de la proposition 3.4, d'autre part de la proposition 3.6.

Corollaire 3.7 *Soit A et B deux ensembles finis équipotents ($\operatorname{card} A = \operatorname{card} B$). Alors :*
- *une fonction de A dans B est bijective si et seulement si elle est injective ;*
- *une fonction de A dans B est bijective si et seulement si elle est surjective.*

Les propriétés énoncées par ce corollaire font parties de celles qui sont tout à fait fausses pour les ensembles qui ne sont pas finis.

4 Le dénombrable

Dans ce cours on appelle ensemble dénombrable un ensemble en bijection avec $\mathbb{N}$ (cela correspond à la définition originale de Cantor). Faîtes attention que certains auteurs comprennent également les ensembles finis dans les ensembles dénombrables. Ce qui est appelé ici ensemble dénombrable est alors appelé ensemble infini dénombrable.

Bien-sûr $\mathbb{N}$ n'est pas fini : comme tout ensemble fini est évidemment subpotent à $\mathbb{N}$, si $\mathbb{N}$ était fini, on aurait par restriction un n pour lequel $\{1, \dots, n+1\}$ s'injecte dans $\{1, \dots, n\}$ ce qui contredit le lemme des tiroirs. Un ensemble dénombrable (en bijection avec $\mathbb{N}$) ne peut donc être fini.

4.1 Les sous-ensembles d'un ensemble dénombrable

Dans cette section on montre que, du point de vue de la cardinalité, il n'y a rien entre les ensembles finis et les ensembles dénombrables.

Proposition 4.1 *Tout sous-ensemble de $\mathbb{N}$ est soit fini soit dénombrable.*

Démonstration. Soit $E \subset \mathbb{N}$. On suppose que E n'est pas fini. On définit alors par récurrence une fonction f de $\mathbb{N}$ dans E, qui sera bijective par construction.

— $f(0) = \min E$ (existe car E n'étant pas fini, n'est pas vide) ;

— $f(n+1) = \min(E \cap \{x \in \mathbb{N} \,/\, x > f(n)\})$ (existe car si $E \subset \{x \in \mathbb{N} \,/\, x \leqslant f(n)\}$, E est fini).

Cette fonction est strictement croissante par définition, donc injective. Elle est surjective. En effet soit $y \in E$. Comme f est croissante il existe n tel que $f(n) < y \leqslant f(n+1)$. Alors par définition $f(n+1) = y$. ■

Corollaire 4.2 *Un ensemble subpotent à un ensemble dénombrable, est fini ou dénombrable. Dit autrement, s'il existe une injection d'un ensemble E dans un ensemble F dénombrable, alors E est dénombrable.*

Démonstration. S'il existe une injection d'un ensemble E dans F dénombrable, il existe une injection f de E dans $\mathbb{N}$ par composition, et E est en bijection avec $\operatorname{Im} f$ qui est fini ou dénombrable d'après la proposition précédente. ■

Ce résultat justifie que l'on parle parfois d'ensemble au plus dénombrable pour un ensemble fini ou dénombrable.

Corollaire 4.3 *S'il existe une surjection d'un ensemble dénombrable dans F, alors F est fini ou dénombrable.*

Démonstration. Par composition, on obtient une surjection f de $\mathbb{N}$ dans F. On a alors une injection de F dans $\mathbb{N}$ en associant à $y \in F$ le plus petit des antécédents de y (l'ensemble des antécédents de y est non vide car f est surjective). ■

4.2 Dénombrabilité et opérations ensemblistes

Voyons d'abord un résultat préliminaire.

Proposition 4.4

- $\mathbb{N} \uplus \mathbb{N} \sim \mathbb{N}$;
- $\mathbb{N} \uplus \{0, \dots, n-1\} \sim \mathbb{N}$
- $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Démonstration. Pour la première relation il suffit de vérifier que la fonction suivante est bijective :

$$\begin{array}{rccc} f : & \mathbb{N} \uplus \mathbb{N} & \to & \mathbb{N} \\ & (n, \varepsilon) & \mapsto & 2n + \varepsilon \end{array}$$

La seconde relation se déduit de la première et du théorème Cantor-Bernstein, ou se démontre facilement directement.

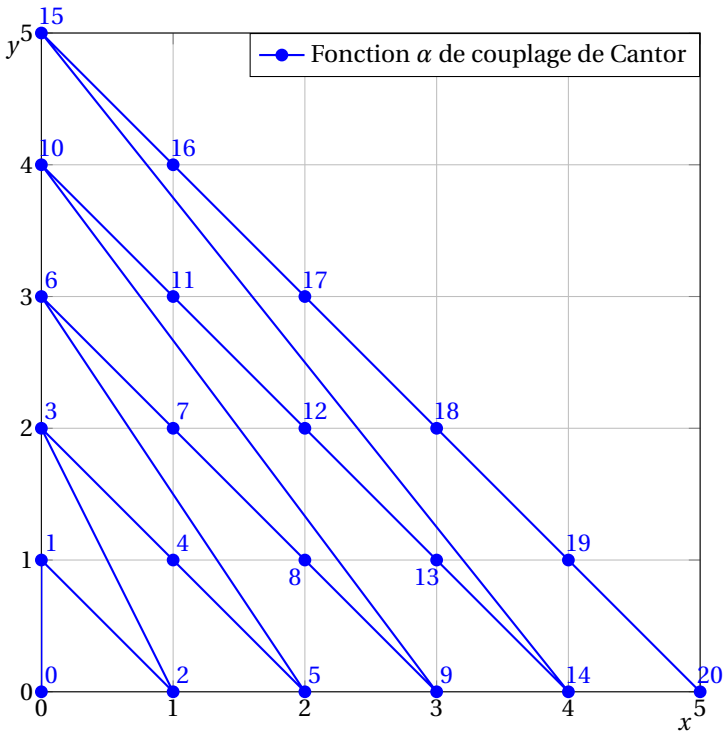
Pour la troisième relation, on peut utiliser la « fonction de couplage » de Cantor, qui est polynomiale et réalise une bijection de $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Le principe est que l'on énumère les couples d'entiers diagonale par diagonale. On a deux fonctions possibles suivant le sens que l'on suit pour parcourir la diagonale, ici on a va aller de gauche à droite. On a alors :

$$\begin{array}{rccc} \alpha : & \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ & (x, y) & \mapsto & \displaystyle\left(\sum_{i=1}^{(x+y)} i \right) + x = \frac{(x+y)(x+y+1)}{2} + x \end{array}$$

La fonction α est bien injective : soit (x, y) et (x', y') tels que $\alpha(x, y) = \alpha(x', y')$. Si $x + y \neq x' + y'$, par exemple $x + y < x' + y'$, alors :

$$\alpha(x, y) < (\sum_{i=1}^{x+y} i) + (x + y + 1) \leqslant \sum_{i=1}^{x'+y'} i \leqslant \alpha(x', y')$$

ce qui n'est pas possible, donc $x + y = x' + y'$. On déduit alors de $\alpha(x, y) = \alpha(x', y')$ que $x = x'$, puis comme $x + y = x' + y'$, $y = y'$.



$\alpha(0,0)$	=	0	$\alpha(1,3)$	=	11
$\alpha(0,1)$	=	1	$\alpha(2,2)$	=	12
$\alpha(1,0)$	=	2	$\alpha(3,1)$	=	13
$\alpha(0,2)$	=	3	$\alpha(4,0)$	=	14
$\alpha(1,1)$	=	4	$\alpha(0,5)$	=	15
$\alpha(2,0)$	=	5	$\alpha(1,4)$	=	16
$\alpha(0,3)$	=	6	$\alpha(2,3)$	=	17
$\alpha(1,2)$	=	7	$\alpha(3,2)$	=	18
$\alpha(2,1)$	=	8	$\alpha(4,1)$	=	19
$\alpha(3,0)$	=	9	$\alpha(5,0)$	=	20
$\alpha(0,4)$	=	10	$\cdots$		

La fonction f est bien surjective : soit $z \in \mathbb{N}$. Comme la fonction $n \mapsto \sum_{i=1}^{n} i$ est strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$, il existe $s \in \mathbb{N}$ tel que :

$$\sum_{i=1}^{s} i \leqslant z < \sum_{i=1}^{s+1} i \quad \text{d'où} \quad 0 \leqslant z - \sum_{i=1}^{s} i \leqslant s\,.$$

Posons $x = z - \sum_{i=1}^{s} i$, et $y = s - x$. Par choix de s, on a bien $x \in \mathbb{N}$ et $y \in \mathbb{N}$, et $z = \alpha(x,y)$. ■

Corollaire 4.5 *Le produit cartésien de deux ensembles dénombrables est dénombrable. La réunion de deux ensembles dénombrables est dénombrable, la réunion d'un ensemble fini et d'un ensemble dénombrable est dénombrable.*

Démonstration. C'est évident pour le produit par transitivité de la relation d'équipotence et compatibilité de celle-ci avec le produit cartésien. Pour la réunion : on a de la même façon que l'union disjointe de A est B dénombrable. Par ailleurs $A \cup B \preccurlyeq A \uplus B$, par exemple avec la fonction :

$$\begin{array}{rccll} f: & A \cup B & \to & A \oplus B & \\ & x & \mapsto & (x,0) & \text{si } x \in A \\ & x & \mapsto & (x,1) & \text{si } x \in B \text{ et } x \notin A \end{array}$$

qui est injective. D'après la proposition 4.2, $A \cup B$ est fini ou dénombrable, donc dénombrable car $A \subset A \cup B$, et A est dénombrable. ■

Proposition 4.6 *Une réunion finie d'ensembles dénombrables est dénombrable. Un produit cartésien fini d'ensembles dénombrables est dénombrable.*

Démonstration. Par récurrence sur p en utilisant la proposition précédente : toute réunion de p ensembles dénombrables est dénombrable, tout produit cartésien de p ensembles dénombrables est dénombrable. ■

La proposition suivante est commode, mais sa démonstration utilise l'axiome du choix (AC).

Proposition 4.7 (AC) *Une réunion dénombrable d'ensembles dénombrables est dénombrable.*

Démonstration. Soit $(A_i)_{i\in\mathbb{N}}$ une suite d'ensembles dénombrables. L'idée est d'utiliser que $\mathbb{N}\times\mathbb{N}\sim\mathbb{N}$. Chacun des A_i est dénombrable : cela signifie que pour tout i il existe une bijection de $\mathbb{N}$ dans A_i, c'est-à-dire que $\left\{f:\mathbb{N}\to A_i \ / \ f \text{ bijective}\right\}\neq\emptyset$. On en déduit par l'axiome du choix que :

$$\prod_{i\in\mathbb{N}}\left\{f:\mathbb{N}\to A_i \ / \ f \text{ bijective}\right\}\neq\emptyset$$

et un élément de ce produit est une suite $(f_i)_{i\in\mathbb{N}}$ de bijections, $f_i:\mathbb{N}\to A_i$. C'est pour le passage de : pour chaque i il existe une bijection $f_i:\mathbb{N}\to A_i$, à l'existence de cette suite $(f_i)_{i\in\mathbb{N}}$ de fonctions de $f_i:\mathbb{N}\to A_i$ que, formellement, on a besoin de l'axiome du choix. Le reste de la démonstration est simple : on définit $\varphi:\mathbb{N}\times\mathbb{N}\to\cup_{i\in\mathbb{N}}A_i$ par $\varphi(i,x)=f_i(x)$. Cette fonction est surjective, les f_i étant surjectives, donc, comme $\mathbb{N}\times\mathbb{N}$ est dénombrable, $\cup_{i\in\mathbb{N}}A_i$ est fini ou dénombrable, et comme il contient n'importe quel des A_i qui est dénombrable, il est dénombrable. ■

La démonstration de la proposition utilise l'axiome du choix, mais dans les applications de la proposition, il est courant que la suite (f_i) puisse être définie directement, sans utiliser l'axiome du choix.

4.3 Le plus petit infini

On démontre par récurrence qu'un ensemble qui n'est pas fini contient un ensemble fini de taille arbitraire. C'est même une caractérisation par le lemme des tiroirs : tout ensemble qui contient un ensemble fini de taille arbitraire n'est pas fini.

Proposition 4.8 *Un ensemble E n'est pas fini si et seulement si pour tout entier n, E contient un sous-ensemble fini de cardinal n.*

Démonstration. Soit E qui n'est pas fini. On montre par récurrence sur n que E contient un sous-ensemble de cardinal n. Pour 0, $\emptyset\subset E$. On suppose le résultat pour n. Soit alors A un sous-ensemble fini de cardinal n inclu dans E. Comme E n'est pas fini, $E\neq A$. Soit $b\in E\setminus A$. Alors $A\cup\{b\}\subset E$, et $A\cup\{b\}$ est fini de cardinal $n+1$. ■

Un ensemble qui contient un ensemble dénombrable n'est pas fini, puisqu'il contient des ensembles finis de taille arbitraire. Nous avons vu par ailleurs que les ensembles subpotents à un ensemble dénombrable sont finis ou dénombrables. Le dénombrable est donc candidat à être le plus petit ensemble qui n'est pas fini (au sens de la subpotence). Nous allons prendre ceci comme définition d'infini.

Définition 4.9 Un ensemble est dit *infini* s'il contient un ensemble dénombrable.

Cette définition est souvent plus maniable que de définir un ensemble infini simplement comme un ensemble qui n'est pas fini. Là le dénombrable est par définition le plus petit infini.

On pourrait imaginer qu'il existe des ensembles qui ne sont pas finis, mais qui ne sont pas comparables au dénombrable. En utilisant l'axiome du choix on démontre que ce n'est pas possible : un ensemble qui n'est pas fini contient un ensemble dénombrable.

Proposition 4.10 (AC) *Tout ensemble qui n'est pas fini contient un ensemble dénombrable, et donc est infini au sens de la définition précédente.*

Démonstration. Soit E un ensemble qui n'est pas fini. On a besoin d'une fonction f, dite fonction de choix sur $\mathscr{P}(E)\setminus\{\emptyset\}$ (les sous-ensembles non vides de E), qui associe à tout sous-ensemble A non vide de E un élément $f(A)$ de A ($f(A)\in A$). Cette fonction s'obtient par l'axiome du choix : pour se ramener à la formulation donnée, on peut prendre la famille des sous-ensembles non vide de E indexée par les sous-ensembles eux mêmes : $(A)_{A\in\mathscr{P}(E)\setminus\{\emptyset\}}$. Par l'axiome du choix, le produit cartésien de cette famille est non vide, et un élément du produit est bien une fonction de choix sur $\mathscr{P}(E)\setminus\{\emptyset\}$.

On définit alors par récurrence une fonction G de $\mathbb{N}$ dans $\mathscr{P}(E)$:

$$\begin{array}{lcl} G(0) & = & f(E) \\ G(n+1) & = & G(n)\cup\{f(E\setminus G(n))\}\,. \end{array}$$

Par récurrence, pour tout entier n, $G(n)$ est un sous-ensemble fini de E de cardinal n, et $G(n)\subset G(n+1)$. Donc $G(n+1)\setminus G(n)$ est un singleton. On définit $h:\mathbb{N}\to E$ par $h(n)=f(E\setminus G(n))$. Alors $G(n+1)\setminus G(n)=\{h(n)\}$. La fonction h est donc injective, d'où Im h est un ensemble dénombrable inclu dans E. ■