RUDIMENTS SUR LA CARDINALITE

Introduction. Pour comparer la “taille” de deux ensembles finis, on a une notion naturelle de “nombre d'éléments” (on compte les moutons). Dans ce cas, dire que deux ensembles ont le même nombre d'éléments équivaut à dire que l'on peut associer à chacun des éléments du premier un élément unique du second, et réciproquement. En clair, deux ensembles finis ont le même nombre d'éléments si et seulement s'il existe une bijection entre eux. Cette façon de mesurer la “taille” ou le “peuplement” d'un ensemble fini est compatible avec l'inclusion, au sens que si $A \subset B$ et $A \neq B$, alors le nombre d'éléments de A est $<$ au nombre d'éléments de B.

Les choses se compliquent dès que l'on considère des ensembles infinis. On n'a plus de façon intuitive de compter les éléments (on peut encore comprendre ce que signifie énumérer les éléments de $\mathbb{N}$, ou de $\mathbb{Z}$, mais comment compter les points d'un plan ? ou les réels de l'intervalle $[0, 1]$?). Ce qui demeure, c'est le fait de pouvoir définir deux ensembles “de même taille” ou “également peuplés” par le fait qu'il existe (au moins) une bijection entre les deux (c'est la notion d'ensembles équipotents, ou de même puissance). Mais le comportement vis à vis de l'inclusion est plus délicat. L'ensemble $2\mathbb{N}$ des entiers positifs pairs est strictement inclus dans $\mathbb{N}$ (en ce sens il y a “moins” d'entiers pairs que d'entiers puisque tous les entiers ne sont pas pairs), mais il est équipotent à $\mathbb{N}$ via par exemple la bijection $n \mapsto 2n$ (en ce sens il y a “autant” d'entiers pairs que d'entiers). En fait, on verra que cette propriété d'avoir un sous-ensemble strict qui soit équipotent à l'ensemble tout entier est une caractérisation des ensembles infinis.

Elles se compliquent plus encore si l'on veut comparer les différentes façons d'être infini. On peut numéroter les entiers naturels en une suite infinie, mais en est-il de même des nombres rationnels ? (on verra que oui) ou des nombres réels (on verra que non) ? En clair, $\mathbb{Q}$ est équipotent à $\mathbb{N}$, mais pas $\mathbb{R}$. Y a-t-il “plus de points” dans un plan que dans une droite ? (oui intuitivement au sens de l'inclusion, mais non au sens de l'équipotence, car on verra que $\mathbb{R}^2$ est équipotent à $\mathbb{R}$). Il semble clair qu'un ensemble fini a toujours “moins d'éléments” que l'ensemble infini $\mathbb{N}$, mais existe-t-il des ensembles infinis qui aient “moins d'éléments” que $\mathbb{N}$? (au sens de l'équipotence, on verra que non). Existe-t-il des ensembles infinis qui (toujours au sens de l'équipotence) aient “plus d'éléments” que $\mathbb{N}$ mais “moins d'éléments” que $\mathbb{R}$? (on verra que la réponse est plus délicate).

Le traitement rigoureux de ces questions conduit (entre autres) à dégager la notion de cardinal. On se limite ici à quelques énoncés (les plus élémentaires et les plus utiles dans la pratique mathématique quotidienne), ne concernant que LE FINI, LE DÉNOMBRABLE ET LA PUISSANCE DU CONTINU, et sans insister sur les questions de théorie des ensembles qui les sous-tendent, et qui sont pourtant indissociables de leur développement historique à la fin du XIXème et au début du XXème siècle.

Le point de vue retenu pour cet exposé n'est pas celui de l'axiomatique:
[théorie des ensembles] $\to$ [cardinaux] $\to$ [cardinaux finis] $\to$ [$\mathbb{N}$] $\to$ [$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$,...]

On suppose connus les ensembles de nombres $\mathbb{N}$ (par exemple par les axiomes de Péano), $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, tels qu'ils ont été introduits et étudiés en S1. On y reviendra au chapitre 2.

Définition préliminaire. Un ensemble E est dit ÉQUIPOTENT à un ensemble F lorsqu'il existe au moins une bijection de E sur F.
Il est clair qu'il existe alors au moins une bijection de F sur E (réciproque d'une bijection de E sur F); on dira donc simplement que *les ensembles E et F sont équipotents.*
Il est clair que tout ensemble est équipotent à lui-même (via par exemple l'identité de E), et que: si E est équipotent à F et F est équipotent à G, alors E est équipotent à G. On a donc les propriétés d'une relation d'équivalence, mais dans la classe de tous les ensembles, qui n'est pas un ensemble (mais dont les éléments sont tous les ensembles.)

I. ENSEMBLES FINIS

1.1 Segments de $\mathbb{N}$.

a) Notation. Pour tout $n \in \mathbb{N}^*$, on note: $[\![1, n]\!] = \{1, 2, \dots, n\}$.

b) Premier lemme fondamental. *Soient $p, q \in \mathbb{N}^*$. On a les propriétés suivantes:*

(i) *Il existe une injection de $[\![1, p]\!]$ dans $[\![1, q]\!]$ si et seulement si $p \leq q$.*
(ii) *S'il existe une surjection de $[\![1, p]\!]$ sur $[\![1, q]\!]$, alors $p \geq q$.*
(iii) *Il existe une bijection de $[\![1, p]\!]$ sur $[\![1, q]\!]$ si et seulement si $p = q$.*

Preuve. Montrons d'abord (i). Supposons d'abord $p \leq q$. Alors $[\![1, p]\!] \subseteq [\![1, q]\!]$, de sorte que l'injection canonique f de $[\![1, p]\!]$ dans $[\![1, q]\!]$, définie par $f(x) = x$ pour tout $x \in [\![1, p]\!]$, répond à la question.
Pour la réciproque, on va montrer par récurrence sur p la propriété $(*)_p$ suivante:
$(*)_p$: pour tout $q \in \mathbb{N}^*$, s'il existe une injection de $[\![1, p]\!]$ dans $[\![1, q]\!]$, alors $p \leq q$.
Pour $p = 1$, il n'y a rien à montrer puisque $[\![1, p]\!] = \{1\}$; donc $(*)_1$ est vraie.
Supposons (hypothèse de récurrence) que $(*)_p$ soit vraie, pour un entier $p \in \mathbb{N}^*$. Donnons-nous $q \in \mathbb{N}^*$ quelconque et une injection f de $[\![1, p+1]\!]$ dans $[\![1, q]\!]$. Il est clair que $q \geq 2$ (en effet, sinon $[\![1, q]\!]$ serait un singleton, donc l'injectivité de f impliquerait que $[\![1, p+1]\!]$ serait un singleton, d'où $1 = p + 1$, ce qui contredirait $p \geq 1$.)
Premier cas: si $f(p + 1) = q$. Alors par injectivité de f, tout $x \in [\![1, p]\!]$ est tel que $f(x) \in [\![1, q-1]\!]$. Donc la restriction f' de f à $[\![1, p]\!]$ est une injection de $[\![1, p]\!]$ dans $[\![1, q-1]\!]$. En appliquant l'hyp. de récurrence, on déduit $p \leq q - 1$, donc $p + 1 \leq q$.
Second cas: si $1 \leq f(p + 1) < q$, définissons une bijection g de $[\![1, q]\!]$ sur $[\![1, q]\!]$ en posant: $g(q) = f(p + 1)$, $g(f(p + 1)) = q$,
et $g(x) = x$ pour tout $x \in [\![1, p]\!]$, $x \neq f(p + 1)$, $x \neq q$.
Alors $g \circ f$ est une application de $[\![1, p+1]\!]$ dans $[\![1, q]\!]$, qui est injective (composée de deux injections) et qui vérifie $(g \circ f)(p + 1) = q$. En appliquant le premier cas, il vient $p + 1 \leq q$.
Ceci prouve la propriété $(*)_{p+1}$, ce qui par récurrence achève la preuve de (i).

- Pour (ii), soit f une surjection de $[\![1, p]\!]$ sur $[\![1, q]\!]$. Pour chaque $k \in [\![1, q]\!]$, l'ensemble $E_k = \{x \in [\![1, p]\!]\,;\, f(x) = k\}$ est une partie non-vide de $[\![1, p]\!]$. Elle admet donc un (unique) plus petit élément x_k. On a ainsi construit une application $k \mapsto x_k$ de $[\![1, q]\!]$

dans $[\![1,p]\!]$. Elle est injective (car si $x_k = x_m$, alors $f(x_k) = f(x_m)$, donc $k = m$). En appliquant le point (i), on déduit que $q \leq p$.

- Pour (iii), si $p = q$, l'identité est une bijection de $[\![1,p]\!] = [\![1,q]\!]$ sur lui-même. Pour l'implication réciproque, il suffit d'appliquer (i) et (ii). $\square$

c) <u>Second lemme fondamental.</u> *Soit $p \in \mathbb{N}^*$. Soit f une application de $[\![1,p]\!]$ dans $[\![1,p]\!]$. Les assertions suivantes sont équivalentes:*

(i) *f est injective,* (ii) *f est surjective,* (iii) *f est bijective.*

Preuve. Comme (iii)⇒(i), il suffit de raisonner en deux étapes.

- Montrons (i)⇒(ii). Supposons f injective. Par l'absurde, supposons que f n'est pas surjective. Il existe alors $a \in [\![1,p]\!]$ tel que $a \notin \{f(1), f(2), \ldots, f(p)\}$. Ceci implique que $[\![1,p]\!]$ n'est pas un singleton, donc $p \geq 2$. Définissons alors une application g de $[\![1,p]\!]$ dans $[\![1,p-1]\!]$ de la façon suivante:
  soit $n \in [\![1,p]\!]$; comme $f(n) \neq a$, deux cas seulement sont possibles:
  si $f(n) < a$, on pose $g(n) = f(n)$, (on a bien $g(n) \in [\![1,p-1]\!]$ puisque $g(n) < a \leq p$),
  si $f(n) > a$, on pose $g(n) = f(n) - 1$, (on a bien $g(n) \in [\![1,p-1]\!]$ puisque $f(n) \leq p$).
  Mais alors g est injective; (en effet, si $g(n) = g(m)$, on a :
  ou bien $f(n) < a$ et $f(m) < a$, donc $f(n) = f(m)$ donc $n = m$ car f injective,
  ou bien $f(n) > a$ et $f(m) > a$, donc $f(n) - 1 = f(m) - 1$ donc de même $n = m$,
  ou bien $f(n) < a$ et $f(m) > a$, donc $a > f(n) = f(m) - 1 > a - 1$ impossible).
  L'existence d'une injection de $[\![1,p]\!]$ dans $[\![1,p-1]\!]$ contredit le lemme b).
- Montrons (ii)⇒(iii). Supposons f surjective de $[\![1,p]\!]$ sur $[\![1,p]\!]$. Comme dans la preuve du lemme b, pour tout $k \in [\![1,p]\!]$, soit x_k le plus petit élément de la partie non-vide $E_k = \{x \in [\![1,p]\!]\,;\, f(x) = k\}$ de $[\![1,p]\!]$. Soit g l'application $k \mapsto x_k$ de $[\![1,p]\!]$ dans $[\![1,p]\!]$. Elle est injective comme on l'a vu, donc surjective d'après l'étape précédente, et finalement bijective. Par définition de g, on a $f \circ g = \mathrm{id}_{[\![1,p]\!]}$, d'où $f = g^{-1}$ bijective. $\square$

1.2 Notion d'ensemble fini.

a) <u>Définition.</u> Un ensemble non-vide E est dit FINI lorsqu'il existe un entier naturel $p \in \mathbb{N}^*$ tel que E soit équipotent à $[\![1,p]\!]$. Par convention, on dit aussi que l'ensemble vide est fini.
b) <u>Lemme.</u> *Soit E est un ensemble non-vide. E est fini si et seulement s'il existe un* UNIQUE *entier naturel $p \in \mathbb{N}^*$ tel que E soit équipotent à $[\![1,p]\!]$.*

Preuve. Le seul point à montrer est l'unicité de p.
Supposons donc E fini. D'après a), il existe $p \in \mathbb{N}^*$ tel que E est équipotent à $[\![1,p]\!]$. Soit $q \in \mathbb{N}^*$ tel que E est équipotent à $[\![1,q]\!]$. Alors $[\![1,p]\!]$ est équipotent à $[\![1,q]\!]$. En appliquant 1.1.b (iii), on conclut $p = q$. $\square$

c) <u>Définition.</u> Soit E un ensemble fini. Si E est non-vide, on appelle CARDINAL de E (ou encore nombre d'éléments de E) l'unique entier $p \in \mathbb{N}^*$ tel que E soit équipotent à $[\![1,p]\!]$. On convient que le cardinal de l'ensemble vide est 0.
On note: $p = \operatorname{card} E$, ou encore $p = \#E$, ou encore parfois $p = |E|$.

On peut alors résumer les principales propriétés découlant directement de ces définitions et des lemmes 1.1.b et 1.1.c sous la forme du théorème de synthèse suivant:

1.3 Théorème. (ce qu'il faut retenir)

(i) *Soient E et F deux ensembles finis. Alors:*
$\operatorname{card} E \leq \operatorname{card} F$ *ssi il existe une injection de E dans F.*
$\operatorname{card} E \geq \operatorname{card} F$ *ssi il existe une surjection de E sur F.*
$\operatorname{card} E = \operatorname{card} F$ *ssi il existe une bijection de E sur F.*

(ii) *Soient E et F deux ensembles finis de même cardinal, et f une application $E \to F$. Alors: f injective ssi f surjective ssi f bijective.*
(Notons que ceci s'applique en particulier au cas où $E = F$.)

(iii) *Soient E et F deux ensembles, et f une application $E \to F$. Alors:*
(F fini et f injective) $\Rightarrow$ (E fini et $\operatorname{card} E \leq \operatorname{card} F$).
(E fini et f surjective) $\Rightarrow$ (F fini et $\operatorname{card} E \geq \operatorname{card} F$).
(E fini et f bijective) $\Rightarrow$ (F fini et $\operatorname{card} E = \operatorname{card} F$).

(iv) *Si F est fini, tout sous-ensemble $E \subseteq F$ est fini et vérifie $\operatorname{card} E \leq \operatorname{card} F$.*

(v) *Si F est fini, et si $E \subseteq F$, alors $\operatorname{card} E = \operatorname{card} F$ ssi $E = F$.*

Preuve. Résulte immédiatement des définitions et de 1.1. Rédaction en exercice. □

On résume sous forme d'exercice (à faire en T.D.) certains procédés pour construire des ensembles finis à partir d'autres ensembles finis.

1.4 Exercice.

Soient E et F deux ensembles finis; montrer que:
a) la réunion $E \cup F$ est fini, et: $\operatorname{card}(E \cup F) = \operatorname{card}(E) + \operatorname{card}(F) - \operatorname{card}(E \cap F)$;
b) le produit cartésien $E \times F$ est fini, et: $\operatorname{card}(E \times F) = \operatorname{card}(E)\operatorname{card}(F)$;
c) l'ensemble $\mathcal{F}(E, F)$ des applications $E \to F$ est fini, de cardinal $\operatorname{card}(F)^{\operatorname{card}(E)}$;
d) l'ensemble $\mathcal{P}(E)$ des sous-ensembles de E est fini, et: $\operatorname{card}(\mathcal{P}(E)) = 2^{\operatorname{card}(E)}$.

1.5 Ensembles infinis.

a) Définition. Un ensemble est dit INFINI lorsqu'il n'est pas fini.

b) Remarques et exemples.
1) *S'il existe une application $E \to E$ qui est surjective sans être injective, ou injective sans être surjective, alors E est infini* [d'après 1.3.(ii)].
Par exemple, $\mathbb{N}$ est infini (puisque l'application $\mathbb{N} \to \mathbb{N}$ de succession $n \mapsto n + 1$ est injective non surjective: c'est le fameux "hôtel d'Hilbert"...)
2) *S'il existe une application $E \to F$ qui est injective et si E est infini, alors F est infini. En particulier tout ensemble contenant un sous-ensemble infini est infini.*
Par exemple, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont infinis car ils contiennent $\mathbb{N}$.
3) *Tout ensemble équipotent à un ensemble infini est infini,* [d'après le 2), ou 1.3.(iii)].

c) Exercice. Montrer que:
Si E est infini, alors $E \times E$ est infini. (et donc E^p est infini pour tout $p \in \mathbb{N}^*$.)
Si E est infini, alors $\mathcal{P}(E)$ est infini.
Si F est infini, alors $\mathcal{F}(E, F)$ est infini.

Les deux théorèmes suivants donnent deux caractérisations utiles des ensembles infinis.

d) Théorème.
Un ensemble F est infini si et seulement s'il existe une injection de $\mathbb{N}$ dans F.

Preuve. Supposons qu'il existe une injection de $\mathbb{N}$ dans F.

Comme $\mathbb{N}$ est infini, il résulte du 2) du b) ci-dessus que F est infini. Réciproquement, supposons F infini. Soit $a_0 \in F$ fixé. Soit $X_0 = F \setminus \{a_0\}$. On a $X_0 \neq \emptyset$ puisque F n'est pas un singleton. Choisissons un élément a_1 quelconque dans X_0, et posons $X_1 = F \setminus \{a_0, a_1\}$. On a $X_1 \neq \emptyset$ puisque F n'est pas de cardinal 2. Supposons que l'on ait construit n éléments distincts $a_0, a_1, \ldots, a_n$ dans F. Comme F n'est pas fini, l'ensemble $X_n = F \setminus \{a_0, a_1, \ldots, a_n\}$ est non vide. On choisit (axiome du choix) un élément a_{n+1} dans X_n, de sorte qu'il est distinct de chacun des éléments $a_0, a_1, \ldots, a_n$. Par récurrence, on construit ainsi une application $f : \mathbb{N} \to F$ définie par $f(n) = a_n$, qui est injective puisque $f(n) = f(m) \Rightarrow n = m$. □

e) Théorème. *Un ensemble F est infini si et seulement s'il existe un sous-ensemble E de F qui est équipotent à F et distinct de F.*

Preuve. Supposons que $E \subset F$ avec $E \neq F$ et E équipotent à F.

Si F était fini, E serait fini d'après 1.3.(iv). Mais alors l'équipotence de E et F impliquerait d'après 1.3.(v) que $E = F$. On conclut donc que F est infini.

Réciproquement, supposons F infini. D'après d), il existe une injection $f : \mathbb{N} \to F$. Posons $E = F \setminus \{f(0)\}$ et définissons une application $g : F \to E$ de la façon suivante:

$$g(x) = \begin{cases} x & \text{si } x \notin f(\mathbb{N}) \\ f(n+1) & \text{si } x = f(n) \in f(\mathbb{N}) \end{cases}$$

Il est clair que g est une bijection de F sur E, avec $E \subset F$ et $E \neq F$. □

1.6 Exercice.

1) Montrer que tout intervalle de $\mathbb{R}$ (non vide et non singleton) est infini. (Utiliser d.)
2) Montrer qu'un ensemble E est fini si et seulement si toute partie non-vide de $\mathcal{P}(E)$ possède un élément maximal pour l'inclusion. (Utiliser d.)

II. Ensembles dénombrables

2.1 Lemme fondamental.

Tout sous-ensemble infini de $\mathbb{N}$ *est équipotent à* $\mathbb{N}$.

Preuve. Soit $A \subseteq \mathbb{N}$ infini; on sait que A admet un plus petit élément a_0.

Comme A n'est pas un singleton, $A_1 = A \setminus \{a_0\}$ est non-vide donc admet un plus petit élément a_1, qui vérifie $a_0 < a_1$. Comme A n'est pas de cardinal 2, $A_2 = A \setminus \{a_0, a_1\}$ admet un plus petit élément a_2, qui vérifie $a_0 < a_1 < a_2$. Supposons que l'on ait construit n éléments $a_0 < a_1 < \cdots < a_n$ dans A. Comme A n'est pas fini, l'ensemble $A_{n+1} = A \setminus \{a_0, a_1, \ldots, a_n\}$ est non vide et admet donc un plus petit élément a_{n+1}, qui vérife $a_n < a_{n+1}$. Par récurrence, on construit ainsi une suite $a_0 < a_1 < \cdots < a_n < a_{n+1} < \cdots$, c'est-à-dire une application $f : \mathbb{N} \to A$ définie par $f(n) = a_n$, qui est strictement croissante, donc injective.

Montrons que f est surjective. Par l'absurde, supposons qu'il existe $y \in A$ tel que $y \neq f(n)$ pour tout $n \in \mathbb{N}$. Il existe alors $m \in \mathbb{N}$ tel que $a_m < y < a_{m+1}$. Comme $a_m < y$, on a $y \in A_{m+1} = A \setminus \{a_0, a_1, \ldots, a_m\}$. Comme a_{m+1} est le plus petit élément de A_{m+1}, on doit alors avoir $a_{m+1} \leq y$, d'où la contradiction.

En résumé, on a contruit une bijection (strictement croissante) de $\mathbb{N}$ sur A. Donc A est équipotent à $\mathbb{N}$. □

Remarque. On peut préciser un peu en montrant que, pour toute partie infinie A de $\mathbb{N}$, il existe une unique bijection strictement croissante de A sur $\mathbb{N}$. L'existence a été établie ci-dessus, l'unicité repose sur le simple fait que l'unique bijection strictement croissante de $\mathbb{N}$ sur $\mathbb{N}$ est l'identité (laissée en exercice).

2.2 Notion d'ensemble dénombrable.

a) Définitions. Un ensemble E est dit DÉNOMBRABLE lorsqu'il est équipotent à $\mathbb{N}$. Un ensemble E est dit AU PLUS DÉNOMBRABLE lorsqu'il est dénombrable ou fini.
Attention: la terminologie peut varier d'un auteur à l'autre; en particulier, pour nous, un ensemble dénombrable est infini.
Il est clair que tout ensemble équipotent à un ensemble dénombrable (resp. au plus dénombrable) est lui-même dénombrable (resp. au plus dénombrable).

b) Propriétés immédiates.

1) *Si F est dénombrable, alors tout sous-ensemble infini $E \subseteq F$ est dénombrable.*
En effet: Soit g une bijection de F sur $\mathbb{N}$. Donc $g(E)$ est un sous-ensemble de $\mathbb{N}$, qui est bien sûr équipotent à E, donc infini [d'après 1.5.b.3)]. D'après le lemme 2.1, $g(E)$ est équipotent à $\mathbb{N}$, donc E est équipotent à $\mathbb{N}$. $\square$

2) *Si F est au plus dénombrable, alors tout sous-ensemble $E \subseteq F$ est au plus dénombrable.*
En effet: Résulte évidemment du 1) ci-dessus et de [1.3.(iv)]. $\square$

3) *Soit $f : E \to F$;*
si f est injective et si F est au plus dénombrable, alors E est au plus dénombrable;
si f est surjective et si E est au plus dénombrable, alors F est au plus dénombrable.

En effet: Le premier point résulte du 2) car $f(E) \subseteq F$ est équipotent à E via f. Pour le second point, rappelons que la surjectivité de f implique qu'il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ (pour tout $y \in F$, on définit $x = g(y)$ en choisissant dans $f^{-1}(\{y\})$ qui est non-vide). Mais alors $f \circ g$ injective implique g injective, ce qui permet d'appliquer le premier point pour conclure que F est au plus dénombrable dès lors que E l'est. $\square$

4) *Un ensemble E est au plus dénombrable si et seulement s'il existe une injection de E dans $\mathbb{N}$.*
En effet: Un sens résulte du 3) ci-dessus. Pour la réciproque, supposons que E est au plus dénombrable. Si E est infini (donc dénombrable), il existe une bijection $E \to \mathbb{N}$, a fortiori injective. Si E est fini non-vide, il existe d'après 1.2.b un unique $p \in \mathbb{N}$ et une bijection $f : E \to [\![1, p]\!]$; il suffit de composer f avec l'injection canonique $[\![1, p]\!] \to \mathbb{N}$ $\square$

c) Remarque (Ecriture sous forme de suites)

• Un ensemble E est dénombrable si et seulement si ses éléments peuvent être écrits comme les termes deux à deux distincts d'une suite infinie (pour toute bijection f de $\mathbb{N}$ sur E, on peut noter $f(n) = x_n$ et $E = \{x_n\,;\, n \in \mathbb{N}\}$).

• D'après le théorème 1.5.d, un ensemble F est infini si et seulement s'il contient un sous-ensemble dénombrable E (il suffit de prendre $E = f(\mathbb{N})$ pour une injection $f : \mathbb{N} \to E$), c'est-à-dire s'il contient les termes deux à deux distincts d'une suite infinie.

2.3 Produit d'ensembles dénombrables.

a) Lemme (fondamental lui aussi): *L'ensemble* $\mathbb{N} \times \mathbb{N}$ *est dénombrable.*

Preuve. On peut construire explicitement une bijection $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ en "numérotant" les couples de $\mathbb{N} \times \mathbb{N}$ suivant le schéma ci-contre; φ est définie par: $\varphi(i,j) = \frac{(i+j)(i+j+1)}{2} + i$.

(0,3) ●	(1,3) ●	(2,3) ●	(3,3)●
(0,2) ●	(1,2) ●	(2,2) ●	(3,2)●
(0,1) ●	(1,1) ●	(2,1) ●	(3,1)●
(0,0) ●	(1,0) ●	(2,0) ●	(3,0)●

Une preuve plus rapide repose sur l'unicité de la décomposition en facteurs premiers de tout entier naturel non-nul. On suppose connu ce résultat, (dont la preuve est bien sûr indépendante de la notion d'ensemble dénombrable). L'application $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par $(n,m) \mapsto 2^n 3^m$ est alors injective. Il résulte alors de 2.2.b.4) que $\mathbb{N} \times \mathbb{N}$ est au plus dénombrable. Or $\mathbb{N} \times \mathbb{N}$ est infini d'après 1.5.c. $\square$

b) Proposition *Si E et F sont dénombrables, alors $E \times F$ est dénombrable. Plus généralement, le produit d'un nombre fini d'ensembles dénombrables est dénombrable.*

Preuve. Par récurrence, il suffit de le montrer pour deux ensembles.
Soient donc E, F tels qu'il existe deux bijections $f : \mathbb{N} \to E$ et $g : \mathbb{N} \to F$. Considérons l'application $h : \mathbb{N} \times \mathbb{N} \to E \times F$, définie par $h(n,m) = (f(n), g(m))$. Il est clair qu'elle est bijective. Donc $E \times F$ est équipotent à $\mathbb{N} \times \mathbb{N}$, qui est dénombrable d'après le lemme a. $\square$

2.4 Réunion d'ensembles dénombrables.

a) Proposition. *Si E et F sont dénombrables, alors $E \cup F$ est dénombrable. Plus généralement, la réunion d'un nombre fini d'ensembles dénombrables est dénombrable.*

Preuve. Par récurrence, il suffit de le montrer pour deux ensembles.
Soient donc E, F tels qu'il existe deux bijections $f : \mathbb{N} \to E$ et $g : \mathbb{N} \to F$. Considérons l'application $h : \mathbb{N} \to E \cup F$, définie par $h(2n) = f(n)$ et $h(2n+1) = g(n)$. Il est clair qu'elle est surjective. Donc $E \cup F$ est au plus dénombrable d'après 2.2.b.3). De plus $E \cup F$ est infini d'après 1.5.a.2) $\square$

b) Proposition. *La réunion d'une famille dénombrable d'ensembles au plus dénombrables est au plus dénombrable.*

Preuve. Soient I dénombrable, et, pour tout $i \in I$, un ensemble E_i au plus dénombrable.
Pour tout $i \in I$, il existe une injection $g_i : E_i \to \mathbb{N}$ d'après 2.2.b.4), donc une injection $f_i : E_i \to I$ (en composant par une bijection de $\mathbb{N}$ sur I). Posons $F_i = f_i(E_i) \times \{i\} \subseteq I \times I$, et $F = \bigcup_{i \in I} F_i \subseteq I \times I$. Comme I est dénombrable, $I \times I$ l'est d'après 2.3.b, donc F est au plus dénombrable d'après 2.2.b.2).
Posons $E = \bigcup_{i \in I} E_i$. Construisons $h : F \to E$ de la façon suivante: tout élément x de F appartient à au moins un F_i, donc est de la forme $x = (f_i(t), i)$ pour un $i \in I$ et un $t \in E_i$, et l'on pose $h(x) = t$. Alors h est surjective par construction (car pour tout $t \in E$, il existe au moins un $i \in I$ tel que $t \in E_i$, de sorte que l'élément $x = (f_i(t), i)$ de F vérifie $h(x) = t$). Ainsi $h : F \to E$ est surjective avec F au plus dénombrable, d'où E au plus dénombrable [d'après 2.2.b.3)]. $\square$

2.5 Exemples.

a) $\mathbb{N}$ *est dénombrable* (par définition), et donc aussi $\mathbb{N}^*$ [d'après 2.2.b.1)].

b) $\mathbb{Z}$ *est dénombrable.*
En effet: $\mathbb{Z}^-$ est dénombrable via la bijection $x \mapsto -x$ de $\mathbb{N}$ sur $\mathbb{Z}^-$, et $\mathbb{Z} = \mathbb{N} \cup \mathbb{Z}^-$

c) $\mathbb{Q}$ *est dénombrable.*
En effet: Comme $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^-$, et comme $\mathbb{Q}^+$ est équipotent à $\mathbb{Q}^-$ via la bijection $x \mapsto -x$, il suffit d'après 2.4.a de vérifer que $\mathbb{Q}^+$ est dénombrable. Or l'application $\mathbb{N} \times \mathbb{N}^* \to \mathbb{Q}^+$ définie par $(p, q) \mapsto \frac{p}{q}$ est surjective, et $\mathbb{N} \times \mathbb{N}^*$ est dénombrable d'après 2.3.b, ce qui assure que $\mathbb{Q}^+$ est au plus dénombrable grâce à 2.2.b.3), et donc dénombrable puisque $\mathbb{Q}^+$ est infini [d'après 1.5.b.2)].

On aborde maintenant des questions plus délicates, touchant au cœur de la description des ensembles infinis, qui est la première étape non triviale de la théorie des cardinaux.

2.6 Ensembles infinis non dénombrables.

a) Théorème. (G. Cantor, 1845-1918)
Pour tout ensemble E, il existe (au moins) une injection de E dans $\mathcal{P}(E)$, mais il n'existe aucune injection de $\mathcal{P}(E)$ dans E.

On traduit cet énoncé en disant que $\mathcal{P}(E)$ est toujours *strictement plus puissant* que E. Il en résulte en particulier que:

- *$\mathcal{P}(E)$ est infini dès lors que E est infini* [d'après 1.5.b.2)],
- *$\mathcal{P}(E)$ n'est jamais équipotent à E.*

Preuve. Le premier point est évident via l'injection $x \mapsto \{x\}$ de E dans $\mathcal{P}(E)$.

- Pour le second montrons d'abord qu'il n'existe aucune surjection de E sur $\mathcal{P}(E)$. En effet, soit $f : E \to \mathcal{P}(E)$ une application. On considère $A = \{x \in E\,;\, x \notin f(x)\} \subset E$. Soit $a \in E$ quelconque. Ou bien $a \in A$, ce qui signifie que $a \notin f(a)$, d'où $f(a) \neq A$. Ou bien $a \notin A$, ce qui signifie que $a \in f(a)$, d'où $f(a) \neq A$. Ainsi, il n'existe pas de $a \in E$ tel que $A = f(a)$, de sorte que f ne peut pas être surjective.
- Déduisons-en qu'il n'existe aucune injection de $\mathcal{P}(E)$ sur E. (C'est un argument absolument général). Posons $F = \mathcal{P}(E)$. Il est non-vide (même si $E = \emptyset$, $\mathcal{P}(E) = \{\emptyset\}$ est un singleton). Supposons par l'absurde qu'il existe $g : F \to E$ injective. Soit $a \in F$ quelconque fixé. Construisons une application $f : E \to F$ de la façon suivante. Pour tout $x \in E$, ou bien il existe $y \in F$ unique (car g injective) tel que $x = g(y)$ auquel cas on pose $f(x) = y$, ou bien $y \notin g(F)$, auquel cas on pose $f(x) = a$. Par construction, on a $f \circ g = \mathrm{id}_F$, d'où l'on déduit que f est surjective, ce qui contredit la première étape. □

On en déduit immédiatement le:

b) Théorème. *Il existe des ensembles infinis non-dénombrables.*
En particulier, l'ensemble $\mathcal{P}(\mathbb{N})$ est infini non-dénombrable.

Preuve. Résulte immédiatement du a) ci-dessus, pour $E = \mathbb{N}$. □

c) Proposition. *S'il existe une injection $E \to F$ et si E est infini non dénombrable, alors F est infini non dénombrable. En particulier, tout ensemble contenant un sous-ensemble infini non-dénombrable est infini non dénombrable.*

Preuve. Résulte immédiatement de 1.5.b.2) et 2.2.b.3). □

d) Théorème.

- $\mathbb{R}$ *est infini non-dénombrable.*
- *Tout intervalle non-vide de* $\mathbb{R}$ *qui n'est pas un singleton est infini non-dénombrable.*

Preuve. Faisons d'abord quelques commentaires sur ce résultat et sa preuve.

On peut montrer que $\mathbb{R}$ et tout intervalle non trivial de $\mathbb{R}$ sont en fait équipotents à $\mathcal{P}(\mathbb{N})$, ce qui est un résultat plus fort (voir plus loin en 3.1.d, et preuve dans les exercices). Pour l'instant on se contente de montrer la non-dénombrabilité. Comme $\mathbb{R}$ et tout intervalle non trivial de $\mathbb{R}$ contiennent un intervalle du type $[a, b[$ avec $a < b$, et comme tout intervalle $[a, b[$ est équipotent à $[0, 1[$ (via par exemple $x \mapsto \frac{x-a}{b-a}$), il suffit finalement de montrer que $[0, 1[$ est non dénombrable. Pour cela on va utiliser le développement décimal des réels. On y reviendra plus en détail dans un autre chapitre, mais ce qu'on en utilise ici est élémentaire et supposé connu.

Par l'absurde, supposons $E = [0, 1[$ dénombrable. D'après 2.2.c, il existe une suite (x_n) d'éléments de E deux à deux distincts telle que $E = \{x_n\ ;\ n \in \mathbb{N}\}$. Construisons alors un réel $\xi \in E$ en le définissant par le développement décimal suivant (dont on exclut les chiffres 0 et 9 pour éviter les ambiguïtés de double écriture: voir chapitre suivant). Avant la virgule, on met 0. Après la virgule, on prend pour j-ième décimale n'importe quel entier entre 1 et 8 à condition qu'il soit distinct de la j-ième décimale de x_j. De la sorte, on a $\xi \neq x_n$ pour tout $n \in \mathbb{N}$ (puisque leur n-ième décimale diffère). Et pourtant $0 \leq \xi < 1$, d'où la contradiction. □

2.7 Exemple. (Nombres transcendants)

Un réel x est dit ALGÉBRIQUE lorsqu'il existe un polynôme non constant $P \in \mathbb{Z}[X]$ tel que $P(x) = 0$. Un réel est dit TRANSCENDANT lorsqu'il n'est pas algébrique.

Il est clair que x est algébrique si et seulement s'il existe un polynôme non constant $Q \in \mathbb{Q}[X]$ tel que $Q(x) = 0$. Il est clair aussi que tout nombre rationnel est algébrique et que la réciproque est fausse (prendre par exemple $\sqrt{2}$). Il n'est pas évident a priori d'expliciter des nombres transcendants (voir ci-dessous), bien que la proposition suivante montre qu'il en existe "beaucoup" (et en un certain sens "beaucoup plus" que des algébriques).

Proposition.

- *L'ensemble* A *des réels algébriques est dénombrable.*
- *L'ensemble* T *des réels transcendants est infini non dénombrable.*

Preuve. $\mathbb{Z}^{n+1}$ est dénombrable comme produit fini d'ensembles dénombrables (cf.2.3.b), pour tout $n \in \mathbb{N}$. Or l'ensemble $\mathbb{Z}_n[X]$ des polynômes de degré $\leq n$ est équipotent à $\mathbb{Z}^{n+1}$, via la bijection canonique $a_0 + a_1 X + \cdots + a_n X^n \mapsto (a_0, a_1, \ldots, a_n)$.

Soit I l'ensemble des polynômes non constants de $\mathbb{Z}[X]$. Donc $I = \bigcup_{n \in \mathbb{N}^*} \mathbb{Z}_n[X]$ est d'après 2.4.b dénombrable comme réunion dénombrable d'ensemble dénombrables.

Pour tout $P \in I$, l'ensemble $Z(P)$ des zéros réels de P est fini (de cardinal $\leq \deg P$).

Par définition, $A = \cup_{P \in I} Z(P)$ est donc une réunion dénombrable d'ensembles finis.

D'après 2.4.b, A est donc au plus dénombrable. De plus, A est infini ($\mathbb{Q} \subset A$), donc A est dénombrable.

Comme $\mathbb{R} = A \cup T$ avec $\mathbb{R}$ infini non dénombrable et A dénombrable, il résulte de 2.4.a que T est infini non dénombrable. □

Remarque. Cet exercice montre en particulier que $T \neq \emptyset$, mais ne construit pas d'élément de T. Montrer qu'un réel est transcendant est un problème souvent très délicat. Il est connu que par exemple $e, \pi, \ln 2$ sont transcendants. (On se contentera de montrer dans un autre chapitre qu'ils sont irrationnels). Il existe des réels dont la question de savoir s'ils sont ou non transcendants (ou même s'ils sont ou non rationnels...) reste encore ouverte (cf. note historique).

III. Quelques compléments d'ordre "culturel"

Le but est de comparer entre eux des ensembles infinis.

3.1 Notion de cardinal.

a) Pour un ensemble donné A, on appelle CARDINAL de A la classe de tous les ensembles qui lui sont équipotents (pour des raisons liées à l'axiomatique de la théorie des ensembles, que nous n'aborderons pas ici, ce n'est pas un ensemble). On le note $\operatorname{card} A$. Tout ensemble B équipotent à A est un REPRÉSENTANT de la classe $\operatorname{card} A$. (Comme pour les ensembles, la classe de tous les cardinaux n'est pas un ensemble).

b) Dans le cas des ensembles finis, cette notion correspond bien à la notion de cardinal défini en 1.2.c :

En effet: Si A est fini non-vide, tout ensemble de la classe $\operatorname{card} A$ au sens ci-dessus est équipotent d'après 1.2.c au sous-ensemble $[\![1, p]\!]$ de $\mathbb{N}$ pour un unique $p \in \mathbb{N}^*$. Cette classe $\operatorname{card} A$ est entièrement déterminée par l'entier p, ce qui autorise à écrire sans ambiguïté $\operatorname{card} A = p$, comme on l'a fait en 1.2. Comme de plus $\emptyset$ est le seul ensemble équipotent à $\emptyset$, on a finalement:

0 a pour seul représentant $\emptyset$,
1 a pour représentants tous les singletons,
2 a pour représentants toutes les paires, etc...

c) Le cardinal de $\mathbb{N}$ est noté $\aleph_0$; c'est donc bien sûr le cardinal de tous les ensembles dénombrables.

d) Le cardinal de $\mathcal{P}(\mathbb{N})$ est noté $2^{\aleph_0}$ par analogie avec 1.4.d. D'après 2.6.b, $2^{\aleph_0}$ est distinct de $\aleph_0$. Un résultat fondamental, qui précise le théorème 2.6.d, est le suivant:

<u>Théorème.</u>

- $\mathbb{R}$ *est équipotent à* $\mathcal{P}(\mathbb{N})$.
- *Tout intervalle I non-vide et non singleton de* $\mathbb{R}$ *est équipotent à* $\mathcal{P}(\mathbb{N})$, *donc à* $\mathbb{R}$.
- $\mathbb{R}^p$ *et* I^p *pour tout* $p \in \mathbb{N}^*$ *sont équipotents à* $\mathcal{P}(\mathbb{N})$, *donc à* $\mathbb{R}$.

En d'autres termes: $\operatorname{card} \mathbb{R} = 2^{\aleph_0}$.
Ce cardinal est appelé la PUISSANCE DU CONTINU.
On dit donc qu'un ensemble a la puissance du continu s'il est équipotent à $\mathbb{R}$ (c'est-à-dire s'il est un représentant du cardinal $2^{\aleph_0}$).
D'après le théorème de Cantor, tout ensemble qui a la puissance du continu est strictement plus puissant (au sens de 2.6.a) que tout ensemble fini ou dénombrable.
La preuve du théorème sera faite sous forme d'une série d'exercices (voir plus loin). En revanche, le calcul sur les cardinaux (arithmétique et ordre) ne sera pas développé ici.

3.2 Le théorème de Cantor-Schröder-Bernstein.

a) <u>Théorème.</u> *Soient deux ensembles E et F.*

(i) *Il existe forcément une injection de E dans F, ou une injection de F dans E.*
(ii) *S'il existe à la fois une injection de E dans F et une injection de F dans E, alors E et F sont équipotents.*

Preuve. Les deux points sont de natures différentes.

Le point (i) a été montré en 1904 par Zermelo; sa preuve utilise le lemme de Zorn; on l'admet ici. On dit que Cantor a énoncé le premier le théorème; Schröder en a donné une première démonstration inexacte et Serge Bernstein (russe, 1880-1968), qui était l'élève de Schröder, en a donné une preuve à l'âge de 19 ans.

A titre d'exercice, rédigeons une preuve de (ii). (C'est un résultat qui peut être utile dans certaines situations pratiques; voir plus loin exercice 3.4). Remarquons aussi que (ii) est trivial pour les ensembles finis d'après 1.3.

Soit donc $f : E \to F$ et $g : F \to E$ injectives. Pour tout $A \in \mathcal{P}(E)$, l'application $f_0 : A \to f(A)$ définie par $f_0(x) = f(x)$ est une bijection de A sur $f(A)$. L'idée est de trouver un $A \in \mathcal{P}(E)$ telle que l'on ait la propriété suivante:

(*) l'application $g_0 : F \setminus f(A) \to E \setminus A$ définie par $g_0(y) = y$ est bijective.

Ceci permet alors de définir une bijection h de E sur F en posant:

$$h(x) = \begin{cases} f_0(x) & \text{si } x \in A \\ {g_0}^{-1}(x) & \text{si } x \in E \setminus A, \end{cases} \qquad \text{donc} \qquad h^{-1}(y) = \begin{cases} {f_0}^{-1}(y) & \text{si } y \in f(A) \\ g_0(y) & \text{si } x \in F \setminus f(A), \end{cases}$$

ce qui achève la preuve. Le problème est donc de montrer (*). En fait, comme g est injective, il suffit de trouver A tel que $g_0 : F \setminus f(A) \to E \setminus A$ soit surjective, c'est-à-dire tel que $g\big(F \setminus f(A)\big) = E \setminus A$, ce qui équivaut à $E \setminus \big(F \setminus f(A)\big) = A$.

Pour cela introduisons l'application:

$$\phi : \mathcal{P}(E) \to \mathcal{P}(E) \text{ définie par } \phi(M) = E \setminus \big(F \setminus f(M)\big) \quad \text{pour tout } M \in \mathcal{P}(E).$$

Il est clair que ϕ est croissante pour l'inclusion (vérification immédiate). Il en résulte (lemme général) qu'il existe $A \in \mathcal{P}(E)$ tel que $\phi(A) = A$.

En effet: posons $\mathcal{X} = \{M \in \mathcal{P}(E)\,;\, M \subseteq \phi(M)\}$. Il est clair que $\mathcal{X} \neq \emptyset$ car $\emptyset \in \mathcal{X}$ puisque nécessairement $\emptyset \subseteq \phi(\emptyset)$. Introduisons $A = \bigcup_{M \in \mathcal{X}} M$.

Soit $M \in \mathcal{X}$; d'une part $M \subseteq A$ par définition de A donc $\phi(M) \subseteq \phi(A)$ puisque ϕ est croissante; d'autre part $M \subseteq \phi(M)$ par définition de $\mathcal{X}$; et donc $M \subseteq \phi(A)$. Ainsi $M \subseteq \phi(A)$ pour tout $M \in \mathcal{X}$, donc $A \subset \phi(A)$ par définition de A. Mais $A \subseteq \phi(A)$ implique $\phi(A) \subseteq \phi(\phi(A))$ puisque ϕ est croissante, et donc $\phi(A) \in \mathcal{X}$ par définition de $\mathcal{X}$. Mais par définition de A, $\phi(A) \in \mathcal{X}$ implique $\phi(A) \subseteq A$. En résumé $A \subset \phi(A)$ et $\phi(A) \subseteq A$. D'où l'égalité voulue.

On a montré qu'il existe $A \in \mathcal{P}(E)$ tel que $A = \phi(A) = E \setminus \big(F \setminus f(A)\big)$, ce qui prouve donc (*) et achève la preuve. □

b) Corollaire et définitions.

Soient deux ensembles E et F. Trois cas seulement peuvent se présenter

(i) *Il existe une injection de E dans F et il n'existe pas d'injection de F dans E; on dit dans ce cas que F est strictement plus puissant que E, ou que E est strictement moins puissant que F, et on note* $\operatorname{card} E < \operatorname{card} F$.

(ii) *Il existe une injection de F dans E et il n'existe pas d'injection de E dans F; on dit dans ce cas que E est strictement plus puissant que F, ou que F est strictement moins puissant que E, et on note* $\operatorname{card} F < \operatorname{card} E$.

(iii) *Il existe une bijection de E dans F, c'est-à-dire que E et F sont équipotents, (on dit aussi également puissants), et l'on a* $\operatorname{card} E = \operatorname{card} F$..

Preuve. Evident d'après le a). □

c) Remarque. Le théorème de Cantor (2.6.a) s'écrit donc:

pour tout ensemble E, on a: $\operatorname{card} E < \operatorname{card} \mathcal{P}(E)$.

d) Remarque historique et culturelle.

(Pourquoi on ne peut pas considérer l'ensemble de tous les ensembles)
Par l'absurde, supposons qu'il existe un ensemble E qui soit l'ensemble de tous les ensembles. Tout élément de $\mathcal{P}(E)$ étant un ensemble (car un sous-ensemble de E), tout élément de $\mathcal{P}(E)$ serait un élément de E, de sorte que l'on aurait $\mathcal{P}(E) \subseteq E$. Il existerait donc une injection de $\mathcal{P}(E)$ dans E. (On serait forcément dans le cas (i) ou (iii) du corollaire b, pour $F = \mathcal{P}(E)$). Ce qui contredirait le théorème de Cantor [2.6.a ou 3.2.c]. (cf. aussi note historique sur les paradoxes classiques relatifs à cette question).

3.3 L'hypothèse du continu.

• D'après 1.1.b et 1.2.c, la notion de puissance entre ensembles finis correspond simplement à l'ordre des entiers naturels, via le nombre d'éléments:
$0 = \operatorname{card} \emptyset < 1 = \operatorname{card}\{a\} < 2 = \operatorname{card}\{a, b\} < 3 = \operatorname{card}\{a, b, c\} < \cdots < n < n + 1 < \cdots$

• D'après 1.5.d, $\aleph_0$ est le premier des cardinaux d'ensembles infinis:
tout ensemble fini E vérifie $\operatorname{card} E < \aleph_0$,
tout ensemble (infini) dénombrable E vérifie $\operatorname{card} E = \aleph_0$,
tout ensemble infini non-dénombrable E vérifie $\aleph_0 < \operatorname{card} E$,

• D'après 3.2.c ou 2.6.c, on a: $\aleph_0 < 2^{\aleph_0}$.

L'hypothèse du continu est une conjecture de Cantor (et premier problème de Hilbert: cf. note historique) affirmant que: *il n'existe pas d'ensemble strictement plus puissant que $\mathbb{N}$ et strictement moins puissant que $\mathbb{R}$.*

A la suite des travaux de Gödel, Paul Cohen (1963) a montré que cette assertion est indécidable: si la théorie des ensembles est non contradictoire, on peut lui ajouter comme axiome l'hypothèse du continu ou sa négation. Plus précisement, Gödel avait montré en 1938 que si la théorie de Zermelo-Fraenkel était consistante, elle restait encore consistante si on lui ajoutait l'hypothèse du continu. Cohen a montré que l'hypothèse du continu ne peut être une conséquence des axiomes de Zermelo-Fraenkel, même lorsqu'on y ajoute l'axiome du choix.

On peut montrer qu'il existe un plus petit cardinal strictement plus grand que $\aleph_0$, noté $\aleph_1$, et l'hypothèse du continue s'énonce alors sous la forme:

$$\aleph_1 = 2^{\aleph_0}, \text{ ou encore: } \operatorname{card} \mathbb{R} = \aleph_1.$$

L'hypothèse du continu généralisé affirme de même que: *pour tout ensemble infini E, il n'existe pas d'ensemble strictement plus puissant que E et strictement moins puissant que $\mathcal{P}(E)$.*

NB. Outre les exercices immédiats incorporés dans les paragraphes précédents, ce chapitre est complété par une feuille d'exercices plus élaborés, et une série de notes historiques.

EXERCICES (une preuve du théorème 3.1.d)

Un des buts de cette série d'exercice est d'aboutir finalement à la preuve du fait que $\mathbb{R}$ et tous ses intervalles non triviaux sont équipotents à $\mathcal{P}(\mathbb{N})$. Plusieurs des résultats intermédiaires pour y parvenir ont néanmoins un intérêt en eux-mêmes ou pour leurs applications à d'autres contextes.

Exercice 1.

1) Montrer que, si F est infini, alors F est équipotent à $E = F \setminus A$ pour tout sous-ensemble fini A de F. (Remarquer que la propriété est fausse si F est fini)
2) Montrer que, si F est infini non-dénombrable, alors F est équipotent à $E = F \setminus I$ pour tout sous-ensemble dénombrable I de F. (Remarquer que la propriété est fausse si F est dénombrable)

Exercice 2.

1) Montrer que, pour tout ensemble E, l'ensemble $\mathcal{P}(E)$ est équipotent à l'ensemble $\mathcal{F}(E, \{0,1\})$.
2) Montrer que, pour E, F, G ensembles quelconques, $\mathcal{F}(G, E \times F)$ est équipotent à $\mathcal{F}(G,E) \times \mathcal{F}(G,F)$.
3) Soient E, F, G trois ensembles. Montrer que, s'il existe une injection de F dans G, alors il existe une injection de $\mathcal{F}(E,F)$ dans $\mathcal{F}(E,G)$. Montrer que, si F est équipotent à G, alors $\mathcal{F}(E,F)$ est équipotent à $\mathcal{F}(E,G)$.

Exercice 3.

1) Soit $\mathcal{E} = \mathcal{F}(\mathbb{N}, \{0,1\})$. Montrer que $\mathcal{E}$ est équipotent à $\mathcal{E} \times \mathcal{E}$.
   N.B. : d'après l'ex.2, $\mathcal{E}$ est équipotent à $\mathcal{P}(\mathbb{N})$ donc on ne peut pas appliquer 2.3.b; on peut en fait montrer d'une façon générale que E est équipotent à $E \times E$ pour tout ensemble E infini; mais on donnera ici une preuve élémentaire pour $\mathcal{E}$.
2) En déduire avec l'exercice précédent que, pour tout $p \in \mathbb{N}^*$, $\mathcal{F}(\mathbb{N}, [\![1, 2^p]\!])$ est équipotent à $\mathcal{P}(\mathbb{N})$.

Exercice 4.

1) Soit E l'intervalle $[0,1[$ de $\mathbb{R}$. Montrer qu'il existe une injection de E dans $\mathcal{F}(\mathbb{N}, [\![0,9]\!])$.
2) Soit E' le sous-ensemble de E formé des réels de $[0,1[$ dont le développement décimal ne contient (après la virgule) que les chiffres $1, 2, \dots, 8$. Montrer que E' est équipotent à $\mathcal{F}(\mathbb{N}, [\![1,8]\!])$.
3) Déduire des questions précédentes et des exercices 2 et 3 que $[0,1[$ est équipotent à $\mathcal{P}(\mathbb{N})$.

Exercice 5.

1) Déduire des exercices 1 et 4 que les intervalles $[0,1[$, $]0,1]$, $]0,1[$ et $[0,1]$ sont équipotents à $\mathcal{P}(\mathbb{N})$.
2) Montrer que $x \mapsto \ln \frac{x}{1-x}$ définit une bijection de $]0,1[$ sur $\mathbb{R}$. En déduire que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$.
3) Montrer que tout intervalle non-vide et non-singleton de $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$.
4) Montrer (avec la question 2 de l'exercice 1) que l'ensemble des réels irrationnels et l'ensemble des réels transcendants sont équipotents à $\mathcal{P}(\mathbb{N})$.
5) Montrer (avec la question 1 de l'exercice 3) que pour tout ensemble E équipotent à $\mathcal{P}(\mathbb{N})$, le produit $E \times E$ est équipotent à $\mathcal{P}(\mathbb{N})$. En déduire que, pour tout $p \in \mathbb{N}^*$, les ensembles $\mathbb{R}^p$ et I^p (où I est un intervalle quelconque non-vide et non singleton de $\mathbb{R}$) sont équipotents à $\mathcal{P}(\mathbb{N})$.

Cet exercice démontre tous les résultats annoncés en cours au théorème 3.1.d.

SOLUTIONS DES EXERCICES

Exercice 1.

1) La propriété est fausse si F est fini et $A \neq \emptyset$, car $\operatorname{card}(F \setminus A) = \operatorname{card} F - \operatorname{card} A \neq \operatorname{card} F$.

Supposons donc F infini. Par une récurrence évidente sur le nombre FINI d'éléments de A, il suffit de faire la preuve dans le cas où $A = \{a\}$ est un singleton. De plus, le choix de $a \in F$ est indifférent car $F \setminus \{a\}$ et équipotent à $F \setminus \{b\}$ pour tout $b \in F$, via les bijections:

$$g : F \setminus \{a\} \to F \setminus \{b\}, \quad x \mapsto \begin{cases} x & \text{si } x \neq b \\ a & \text{si } x = b \end{cases}$$

$$g^{-1} : F \setminus \{b\} \to F \setminus \{a\}, \quad y \mapsto \begin{cases} y & \text{si } y \neq a \\ b & \text{si } y = a \end{cases}$$

Choisissons $a = f(0)$ où f est une injection $\mathbb{N} \to F$ (il en existe d'après 1.5.d puisque F est infini). Comme on l'a vu dans la preuve de 1.5.e, F et $F \setminus \{f(0)\}$ sont équipotents via la bijection:

$$f' : F \to F \setminus \{f(0)\}, \qquad x \mapsto \begin{cases} x & \text{si } x \notin f(\mathbb{N}) \\ f(n+1) & \text{si } x = f(n) \in f(\mathbb{N}) \end{cases}$$

ce qui, d'après ce qui précède, achève la preuve.

2) La propriété est fausse si F est dénombrable (prendre par exemple $F = I = \mathbb{N}$, d'où $F \setminus I = \emptyset$).

Supposons donc F infini non dénombrable. Comme $I \subset F$ est dénombrable, il existe d'après 2.2.c une suite infinie (a_n) d'éléments de F deux à deux distincts telle que $I = \{a_n \,;\, n \in \mathbb{N}\}$.

Comme $F = (F \setminus I) \cup I$ avec I dénombrable et F infini non dénombrable, il résulte de 2.4.a que $F \setminus I$ est infini (et même non dénombrable). D'après 1.5.d et 2.2.c, il existe une suite infinie (b_n) d'éléments de $F \setminus I$ deux à deux distincts telle que $J = \{b_n \,;\, n \in \mathbb{N}\} \subset F \setminus I$. Il est clair, $I \cap J = \emptyset$. Il en résulte que l'application $f : F \to F \setminus I$ définie par:

$$f(x) = x \text{ si } x \notin (I \cup J), \quad f(x) = b_{2n} \text{ si } x = a_n \in I, \quad f(x) = b_{2n+1} \text{ si } x = b_n \in J$$

est injective. Comme on a réciproquement l'injection canonique $F \setminus I \to F$, on déduit du point (ii) du théorème de Bernstein (3.2.a) que F et $F \setminus I$ sont équipotents.

Exercice 2.

1) Il est clair que l'application qui à tout $A \in \mathcal{P}(E)$ associe sa fonction indicatrice définit une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E, \{0,1\})$.

2) Si $f_1 : G \to E$ et $f_2 : G \to F$, on définit $f : G \to E \times F$ en posant $f(x) = (f_1(x), f_2(x))$ pour tout $x \in E$. Il est clair que toute application $G \to E \times F$ est de ce type, de sorte que $f \mapsto (f_1, f_2)$ définit une bijection de $\mathcal{F}(G, E \times F)$ sur $\mathcal{F}(G,E) \times \mathcal{F}(G,F)$.

3) Soit $f : F \to G$ injective. Pour tout $g : E \to F$, on pose $\phi(g) = f \circ g : E \to G$. Si $\phi(g) = \phi(g')$ dans $\mathcal{F}(E,G)$, alors $f \circ g = f \circ g'$ implique $g = g'$ par injectivité de f. Donc ϕ est une injection de $\mathcal{F}(E,F)$ dans $\mathcal{F}(E,G)$. Si de plus f est bijective, ϕ est une bijection de $\mathcal{F}(E,F)$ sur $\mathcal{F}(E,G)$ puisque ϕ^{-1} est simplement définie par $\phi^{-1}(h) = f^{-1} \circ h$ pour tout $h \in \mathcal{F}(E,G)$.

Exercice 3.

1) Soit $\mathcal{E} = \mathcal{F}(\mathbb{N}, \{0,1\})$. Si $f \in \mathcal{E}$ définissons $f_0, f_1 \in \mathcal{E}$ par $f_0(n) = f(2n)$ et $f_1(n) = f(2n+1)$ pour tout $n \in \mathbb{N}$, et posons $\phi(f) = (f_1, f_2)$. On définit ainsi une application

$\phi : \mathcal{E} \to \mathcal{E} \times \mathcal{E}$. Réciproquement, quelles que soient $g_0, g_1 \in \mathcal{E}$, définissons $g = \psi(g_0, g_1) \in \mathcal{E}$ par $g(m) = g_0(n)$ si $m = 2n$ est pair et $g(m) = g_1(n)$ si $m = 2n+1$ est impair. Il est immédiat que ϕ et ψ sont des bijections réciproques entre $\mathcal{E}$ et $\mathcal{E} \times \mathcal{E}$.
2) Soit $p \in \mathbb{N}^*$. Il résulte de la question précédente que $\mathcal{E}$ est équipotent à $\mathcal{E}^p$. Mais $\mathcal{F}(\mathbb{N}, \{0,1\})^p$ est d'après la question 2) de l'ex.2 équipotent à $\mathcal{F}(\mathbb{N}, \{0,1\}^p)$. Comme $\mathrm{card}\{0,1\}^p = 2^p = \mathrm{card}[\![1, 2^p]\!]$, il résulte de la question 3) de l'ex.2 que $\mathcal{F}(\mathbb{N}, \{0,1\}^p)$ est équipotent à $\mathcal{F}(\mathbb{N}, [\![1, 2^p]\!])$. En résumé, $\mathcal{F}(\mathbb{N}, [\![1, 2^p]\!])$ est équipotent à $\mathcal{E} = \mathcal{F}(\mathbb{N}, \{0,1\})$. Or ce dernier est d'après la question 1) de l'ex.2 équipotent à $\mathcal{P}(\mathbb{N})$.

Exercice 4.
1-2) Rappelons d'abord brièvement quelques notions élémentaires sur l'approximation décimale des nombres réels. Pour tout réel x de $E = [0, 1[$, il existe une suite infinie (a_n) d'entiers de $[\![0, 9]\!]$ telle que $x = 0, a_1a_2a_3 \ldots$ Si deux telles suites (a_n) et (b_n) sont égales, alors elles déterminent le même réel: $0, a_1a_2a_3 \ldots = 0, b_1b_2b_3 \ldots$. Mais réciproquement, l'écriture décimale d'un réel peut ne pas être unique: par exemple $0, 1230000 \ldots = 0.1229999 \ldots$ Il en résulte que l'on a seulement une injection de E dans $\mathcal{F}(\mathbb{N}, [\![0, 9]\!])$.
En revanche, si l'on se limite aux réels de E dont l'écriture décimale ne fait intervenir ni 0 ni 9, on obtient une bijection entre leur ensemble E' et $\mathcal{F}(\mathbb{N}, [\![1, 8]\!])$. (On verra en fait au chapitre suivant qu'il suffit de se limiter aux suites propres, c'est-à-dire ne se terminant pas par une infinité de 9...)
3) Comme E' est un sous-ensemble de E, on déduit de la question précédente qu'il existe deux injections:

$$\mathcal{F}(\mathbb{N}, [\![1, 8]\!]) \longrightarrow E \longrightarrow \mathcal{F}(\mathbb{N}, [\![0, 9]\!]).$$

$\mathrm{card}[\![0, 9]\!] = 10$ donc il s'injecte dans $[\![1.16]\!]$ donc, d'après la question 3) de l'ex.2, on a deux injections:

$$\mathcal{F}(\mathbb{N}, [\![1, 2^3]\!]) \longrightarrow E \longrightarrow \mathcal{F}(\mathbb{N}, [\![1, 2^4]\!]).$$

D'après l'ex.3, les deux ensembles extrêmes sont tous les deux équipotents avec $\mathcal{P}(\mathbb{N})$. Il en résulte que $\mathcal{P}(\mathbb{N})$ s'injecte dans E et E s'injecte dans $\mathcal{P}(\mathbb{N})$. D'après le point (ii) du théorème de Bernstein (3.2.a), on conclut que E est équipotent à $\mathcal{P}(\mathbb{N})$.

Exercice 5.
1) Clair d'après la question 3 de l'ex.4 et la question 1 de l'ex.1
2) Pour tout $x \in]0, 1[$, soit $f(x) = \ln \frac{x}{1-x}$, donc $f'(x) = \frac{1}{1-x} > 0$. De plus $\lim_{x \to 0^+} f(x) = -\infty$ et $\lim_{x \to 1^-} f(x) = +\infty$. Ainsi f est continue et strictement croissante, donc réalise une bijection de $]0, 1[$ sur $\mathbb{R}$. On applique la question 1) pour conclure que $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$.
3) Tout intervalle $]a, b[$ non trivial ($a < b$) est équipotent à $]0, 1[$ (via $x \mapsto \frac{x-a}{b-a}$). Donc on applique la question 1. De même pour $[a, b[$, $]a, b]$ et $[a, b]$.
Pour tout $a \in \mathbb{R}$, l'intervalle $[a, +\infty[$ est équipotent à $\mathbb{R}$ (via par exemple $x \mapsto e^x + a$). On applique la question 2). De même $]a, +\infty[$ d'après la question 1) de l'ex.1. Le résultat pour les intervalles $] - \infty, b[$ ou $] - \infty, b]$ s'en déduit via la bijection $x \mapsto -x$.
4) On sait que $\mathbb{Q}$ est dénombrable, et $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$, donc d'après la question 2) de l'ex.1, l'ensemble $\mathbb{R} \setminus \mathbb{Q}$ des nombres irrationnels est est équipotent à $\mathcal{P}(\mathbb{N})$.
On a vu en cours (2.7) que l'ensemble A des nombres algébriques est dénombrable. Comme $\mathbb{R}$ est équipotent à $\mathcal{P}(\mathbb{N})$, on déduit de la question 2) de l'ex.1 que l'ensemble $\mathbb{R} \setminus A$ des nombres transcendant est est équipotent à $\mathcal{P}(\mathbb{N})$.

5) Soit E un ensemble E équipotent à $\mathcal{P}(\mathbb{N})$. L'ensemble $\mathcal{E} = \mathcal{F}(\mathbb{N}, \{0,1\})$ de l'ex.3 est aussi équipotent à $\mathcal{P}(\mathbb{N})$, d'après la question 1 de l'ex.2. Donc E est équipotent à $\mathcal{E}$. Il en résulte que $E \times E$ est équipotent à $\mathcal{E} \times \mathcal{E}$, et donc à $\mathcal{E}$ d'après la question 1) de l'ex.3, et donc à $\mathcal{P}(\mathbb{N})$ d'après la question 1) de l'ex.2.
Une récurrence évidente montre qu'alors E^p est équipotent à $\mathcal{P}(\mathbb{N})$ pour tout $p \in \mathbb{N}^*$. C'est en particulier vrai pour $E = \mathbb{R}$ ou $E =$ tout intervalle non-vide et non-singleton de $\mathbb{R}$.