Université Paul Sabatier
Licence L3 E (Mathématiques pour l'enseignement)
2018-2019
Algèbre 1

Chap. 4 : Applications et cardinaux

Table des matières

1. Applications 1
1.1. Définitions 1
1.2. Image directe et image réciproque 1
1.3. Composition 2
1.4. Injections, surjections, bijections 2
1.5. Bijection réciproque 3
1.6. Passage au quotient 4
2. Compléments sur les cardinaux 6
2.1. Équipotence 6
2.2. Arithmétique 6
2.3. Comparaison des cardinaux 7
3. Exercices 9

1. Applications

1.1. **Définitions.** Rappelons qu'une *application* de A (son ensemble de départ ou domaine) *dans* B (son ensemble d'arrivée ou codomaine), ou de A *vers* B, *est une relation* $f = (A, B, \Gamma_f)$ *telle que*

$$\forall\, a \in A,\ \exists\,!\, b \in B,\ (a, b) \in \Gamma_f$$

On emploie alors la notation $f : A \to B$ *ou*

$$\begin{array}{cccc} f & : & A & \longrightarrow & B \\ & & a & \longmapsto & f(a) \end{array}$$

où $f(a)$ *est l'unique élément de* B *tel que* $(a, f(a)) \in \Gamma_f$*. L'élément* $f(a)$ *de* B *est appelé image de* a *et ce dernier est appelé antécédent de* $f(a)$*.*

Exemples 1.1. *Pour tout ensemble* A*,*
— *l'application* $\mathrm{id}_A : a \mapsto a$ *est appelée* l'application identité *de* A *;*
— *si* $b_0 \in B$*, l'application* $A \to B : a \mapsto b_0$ *est appelée* application constante *de* A *dans* B *de valeur* b_0*.*

<u>Notation :</u> *L'ensemble des applications de* A *dans* B *est noté* B^A*.*

1.2. **Image directe et image réciproque.** *Soient* A *et* B *deux ensembles et* $f : A \to B$*.*

Pour tout $X \subset A$*, l'image directe de* X *par* f *est le sous-ensemble de* B *dont les éléments sont les images par* f *des éléments de* X *:*

$$f(X) := \{f(x) \mid x \in X\}.$$

L'image de f *correspond au cas particulier* $X = A$ *:*

$$\mathrm{Im}(f) := f(A).$$

Pour tout $Y \subset B$*, l'image réciproque de* Y *par* f *est le sous-ensemble de* A *constitué des éléments dont l'image est dans* Y *:*

$$f^{-1}(Y) := \{x \in A \mid f(x) \in Y\}.$$

Remarques 1.2. — *Une reformulation plus opérationnelle de ces deux définitions est :*

$$y \in f(X) \Leftrightarrow \exists x \in X \quad y = f(x)\ ;$$
$$x \in f^{-1}(Y) \Leftrightarrow f(x) \in Y.$$

On voit que la seconde est plus simple. Elle s'étend d'ailleurs aux sous-ensembles, c.-à-d. $X \subset f^{-1}(Y) \Leftrightarrow f(X) \subset Y$ *(exercice 1).*

— *La notation* $f^{-1}(Y)$ *désigne un ensemble qui existe toujours dès que* f *est une application à valeurs dans un ensemble qui contient* Y, *même lorsque* f^{-1} *n'existe pas* *c'est-à-dire lorsque* f *n'est pas bijective.*

Proposition 1.3. *Soient* A *et* B *deux ensembles et* f *une application de* A *dans* B. *Soient également* $X, X' \subset A$ *et* $Y, Y' \subset B$.

i) $f(\varnothing) = \varnothing = f^{-1}(\varnothing)$; $f^{-1}(B) = A$.

ii) $f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$ *et* $f(X \cup X') = f(X) \cup f(X')$.

iii) $Y \subset Y' \Rightarrow f^{-1}(Y) \subset f^{-1}(Y')$ *et* $X \subset X' \Rightarrow f(X) \subset f(X')$.

iv) $f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$ *mais en général, on a seulement* $f(X \cap X') \subset f(X) \cap f(X')$.

v) $X \subset f^{-1}(f(X))$ *et* $f(f^{-1}(Y)) = Y \cap \operatorname{Im} f$.

vi) $f^{-1}(\complement_B Y) = \complement_A f^{-1}(Y)$ *mais* $f(\complement_A X)$ *et* $\complement_B f(X)$ *ne sont en général pas comparables.*

vii) $X \subset f^{-1}(Y) \Leftrightarrow f(X) \subset Y$.

Exercice : 1.

1.3. **Composition.** *Soient* A, B *et* C *trois ensembles. Si* $f : A \to B$ *et* $g : B \to C$ *sont deux applications, la relation composée (cf. chapitre 2), de* A *dans* C, *est encore une application. L'application composée de* f *par* g *est :*

$$\begin{array}{ccccc} g \circ f & : & A & \longrightarrow & C \\ & & a & \longmapsto & g\big(f(a)\big) \end{array}$$

On a donc une application

$$\begin{array}{ccccccc} \circ & : & C^B & \times & B^A & \longrightarrow & C^A \\ & & (\ g & , & f\ ) & \longmapsto & g \circ f. \end{array}$$

On peut représenter la composition par le diagramme commutatif suivant :

$$\begin{tikzcd} A \arrow[rr, "g \circ f"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

Un diagramme commutatif se lit ainsi : deux chemins orientés de même départ et de même arrivée décrivent la même application.

Remarques 1.4.

— *La composition des applications est associative.*

— *Pour toute application* $f : A \to B$, *on a* $f \circ \mathrm{id}_A = f$ *et* $\mathrm{id}_B \circ f = f$.

— *Les itérées d'une application* $f : A \to A$ *sont définies par :* $f^0 = \mathrm{id}_A$ *et* $f^{n+1} = f \circ f^n$ *pour tout* $n \in \mathbb{N}$.

— *Les images directes et réciproques par une fonction composée s'expriment naturellement :* $(g \circ f)(X) = g(f(X))$ *et* $(g \circ f)^{-1}(Z) = f^{-1}(g^{-1}(Z))$ *(attention à l'ordre).*

1.4. **Injections, surjections, bijections.** *Soient* A *et* B *deux ensembles. Une application* $f : A \to B$ *est dite :*

— *injective si tout élément de* B *admet au plus un antécédent, autrement dit si*

$$\forall a, a' \in A \quad f(a) = f(a') \Longrightarrow a = a$$

ou encore :

$$\forall a, a' \in A \quad a \neq a' \Longrightarrow f(a) \neq f(a').$$

— *Parmi les propriétés qui suivent, indiquer lesquelles impliquent l'injectivité de* f *:*

1. $f(x) = f(y) \Rightarrow x = y$ *2.* $x = y \Rightarrow f(x) = f(y)$

3. $f(x) \neq f(y) \Rightarrow x \neq y$ *4.* $x \neq y \Rightarrow f(x) \neq f(y)$.

— *surjective si tout élément de* B *admet au moins un antécédent, autrement dit si*

$$\forall\, b \in B \quad \exists a \in A \quad f(a) = b$$

ou encore, si

$$\operatorname{Im} f = B$$

(ce qui équivaut à $B \subset \operatorname{Im} f$, *puisque l'inclusion réciproque est toujours vraie) ;*

— *bijective si elle est à la fois injective et surjective, autrement dit si*

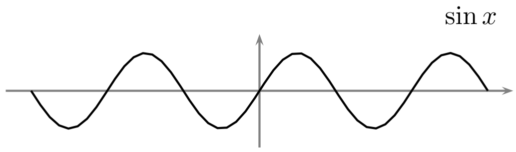
$$\forall b \in B \quad \exists\,!\, a \in A \quad f(a) = b.$$

Remarques 1.5. — *Dans les deux définitions (équivalentes) de l'injectivité, attention à ne pas inverser le sens des implications !*
— *Si $f : A \to B$ et $g : B \to C$ sont injectives (resp. surjectives, resp. bijectives) alors $g \circ f : A \to C$ est injective (resp. surjective, resp. bijective).*

Exemples 1.6.
— *Pour tout ensemble A, l'application id_A (identité de A) est une bijection de A dans A.*
— *Si A est un sous-ensemble de B, l'inclusion $A \subset B$ définit une injection $i_{A,B} : A \to B$, $a \mapsto a$.*
— *Toute application $f : A \to B$ induit une surjection $s : A \to \operatorname{Im} f$, $a \mapsto f(a)$; de plus, s est bijective si et seulement si f est injective.*
— *Si $\mathcal{R}$ est une relation d'équivalence sur l'ensemble E, la projection “canonique” $p_{\mathcal{R}} : E \to E/\mathcal{R}$, $x \mapsto \overline{x}$ est une surjection.*

Remarque 1.7. *En général, pour “rendre” une application surjective, on la remplace par une corestriction, c.-à-d. qu'on “rapetisse” son ensemble d'arrivée ; et pour la “rendre” injective, on la remplace par une restriction, c.-à-d. qu'on “rapetisse” son ensemble de départ.*

Exemples 1.8.



graphe de $\sin \,:\, [-3\pi, 3\pi] \to [-1, 1]$

- $\sin : [0, \pi] \to [-1, 1]$ *n'est ni injective, ni surjective.*
- $\sin : [0, \pi/2] \to [-1, 1]$ *est injective mais n'est pas surjective.*
- $\sin : [0, \pi] \to [0, 1]$ *n'est pas injective mais est surjective.*
- $\sin : [0, \pi/2] \to [0, 1]$ *est bijective.*

1.5. **Bijection réciproque.**

Théorème 1.9. *Soit $f : A \to B$ une application, de graphe Γ. Pour toute application $g : B \to A$, les propositions suivantes sont équivalentes :*

1) le graphe de g est Γ^{-1} (cf. chap. 2, relation réciproque) ;

2) $g(b) = a \Leftrightarrow b = f(a)$ (pour tout $a \in A$ et tout $b \in B$) ;

3) $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$.

Une telle application g (nécessairement unique) existe si et seulement si f est bijective. On la note alors f^{-1} ; elle est bijective – on l'appelle donc la bijection réciproque de f – et sa bijection réciproque est f.

Preuve. *L'existence d'une application g de graphe Γ^{-1} (donc unique) équivaut à $\forall b \in B \quad \exists\,!\, a \in A \quad (b, a) \in \Gamma^{-1}$. Par définition de Γ^{-1}, cela équivaut à la bijectivité de f.*

À nouveau par définition de Γ^{-1}, les conditions 1 et 2 sont équivalentes .

Les conditions 2 et 3 sont équivalentes car $g \circ f = \mathrm{id}_A$ équivaut à $b = f(a) \Rightarrow g(b) = a$, et $f \circ g = \mathrm{id}_B$ équivaut à $a = g(b) \Rightarrow f(a) = b$.

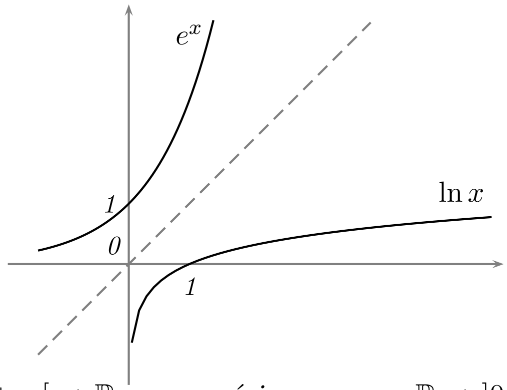
Enfin, puisque la condition 3 est symétrique en f et g, si f est bijective alors f^{-1} l'est aussi et $(f^{-1})^{-1} = f$. □

Remarques 1.10.
— *Les deux égalités $f^{-1} \circ f = \mathrm{id}_A$ et $f \circ f^{-1} = \mathrm{id}_B$ se traduisent par deux diagrammes commutatifs :*

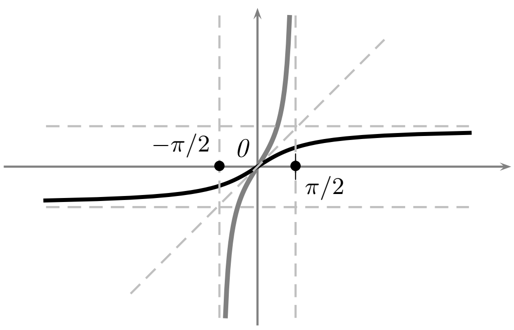
$$\begin{tikzcd}
A \arrow[rr, "\mathrm{id}_A"] \arrow[dr, "f"'] & & A \\
& B \arrow[ur, "f^{-1}"'] &
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
B \arrow[rr, "\mathrm{id}_B"] \arrow[dr, "f^{-1}"'] & & B \\
& A \arrow[ur, "f"'] &
\end{tikzcd}$$

— *Si $f : A \to B$ est bijective et $Y \subset B$, la notation $f^{-1}(B)$ désigne aussi bien l'image réciproque de Y par f (qui existe toujours) que l'image directe de Y par f^{-1} (qui n'existe que parce que f est bijective). Heureusement, ces deux ensembles sont égaux.*

— *Soient $f : A \to B$ et $g : B \to C$ deux bijections. Alors, $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*
— *Si f est une bijection de A dans A, on peut définir f^n non seulement pour $n \in \mathbb{N}$ mais pour $n \in \mathbb{Z}$, en posant, pour tout $k > 0$, $f^{-k} = (f^{-1})^k$.*
— *Soient $A, B \subset \mathbb{R}$. Si $f : A \to B$ est bijective, il y a (comme dans le cas général d'une relation réciproque) une interprétation géométrique naturelle du lien entre f et f^{-1} : dans un repère orthonormé, le graphe de l'une se déduit du graphe de l'autre par la symétrie orthogonale par rapport à la bissectrice $y = x$:*



ln: $]0, +\infty[\to \mathbb{R}$ *a pour réciproque* exp: $\mathbb{R} \to]0, +\infty[$.



tan : $]-\pi/2, \pi/2[\to \mathbb{R}$ *a pour réciproque* arctan: $\mathbb{R} \to]-\pi/2, \pi/2[$.

Exercices : 2, 3, 4, 5, 6, 14 questions 1 à 4.

1.6. **Passage au quotient.**

1.6.1. *Application définie sur le quotient.*

Théorème 1.11. "de factorisation". *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.*

Une application $f : E \to F$ (à valeurs dans un ensemble quelconque F) se factorise par la surjection canonique $p_{\mathcal{R}} : E \to E/\mathcal{R}$, $x \mapsto \overline{x}$ (c'est-à-dire s'écrit sous la forme $f = \overline{f} \circ p_{\mathcal{R}}$ pour une certaine application $\overline{f}$) si et seulement si :

$$\forall x, y \in E \quad (x\mathcal{R}y \Rightarrow f(x) = f(y)).$$

L'application $\overline{f} : E/\mathcal{R} \to F$ est alors unique, puisque la condition $\overline{f} \circ p_{\mathcal{R}} = f$ équivaut à :

$$\forall x \in E \quad \overline{f}(\overline{x}) = f(x).$$

On dit alors que f "passe au quotient" par $\mathcal{R}$.

Preuve. La condition $\overline{f}(\overline{x}) = f(x)$ (pour tout $x \in E$) définit une application $\overline{f} : E/\mathcal{R} \to F$ si et seulement si $\overline{x} = \overline{y} \Rightarrow f(x) = f(y)$ (pour tous $x, y \in E$), ce qui équivaut bien à $x\mathcal{R}y \Rightarrow f(x) = f(y)$. ☐

Remarques 1.12. — *Le théorème 1.11 nous dit à quelle condition on peut « compléter » le diagramme suivant :*

$$\begin{tikzcd} E \arrow[rr, "f"] \arrow[dr, "p_{\mathcal{R}}"'] & & F \\ & E/\mathcal{R} \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd} \qquad (\bigstar)$$

Ce diagramme (★) traduit le fait d'avoir des ensembles E, F, une relation d'équivalence sur E et une application f de E vers F. La flèche en pointillé signifie qu'on se demande si l'on peut trouver une application $g : E/\mathcal{R} \to F$ qui « `complète le diagramme` », c.-à-d. telle que $f = g \circ p_{\mathcal{R}}$. Le théorème 1.11 nous dit que c'est possible si, et seulement si, quels que soient x, y dans E, $x\mathcal{R}y$ implique $f(x) = f(y)$; de plus, lorsque c'est le cas, la seule manière de compléter le diagramme est alors de prendre $g = \overline{f}$, c.-à-d. g définie par $g(\overline{x}) = f(x)$.

— $\operatorname{Im} \overline{f} = \operatorname{Im} f$ *(en particulier, $\overline{f}$ est surjective si et seulement si f l'est).*
— *$\overline{f}$ est injective si et seulement si on a non seulement $x\mathcal{R}y \Rightarrow f(x) = f(y)$ mais $x\mathcal{R}y \Leftrightarrow f(x) = f(y)$.*
— *Toute application $f : A \to B$ peut se décomposer sous la forme*

$$f = i \circ s$$

où $s : A \to C$ est une surjection et $i : C \to B$ une injection. Par exemple, on a déjà vu

$$A \xrightarrow{s} \operatorname{Im} f \xrightarrow{i} B$$

où s est la corestriction de f et i l'injection canonique, mais

$$A \xrightarrow{p_{\mathcal{R}}} A/\mathcal{R} \xrightarrow{\overline{f}} B$$

convient aussi (l'application $\overline{f}$ fournie par le théorème 1.11 est bien injective, par définition de $\mathcal{R}$). Ces "deux exemples" sont en réalité équivalents, et équivalents à tout autre, d'après le résultat suivant (admis faute de temps) : une décomposition $f = i \circ s$ avec i injective et s surjective est "unique à une unique bijection près", ce qui signifie que si $A \xrightarrow{s_1} C_1 \xrightarrow{i_1} B$ et $A \xrightarrow{s_2} C_2 \xrightarrow{i_2} B$ sont deux telles décompositions, alors il existe une unique bijection $b : C_1 \to C_2$ telle que le diagramme suivant commute :

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "s_1"] \arrow[ddr, "s_2"'] & & B \\
& C_1 \arrow[ur, "i_1"] \arrow[d, dashed, "b"] & \\
& C_2 \arrow[uur, "i_2"'] &
\end{tikzcd}$$

(en fait, il suffit qu'une application $b : C_1 \to C_2$ vérifie l'une des trois égalités $s_2 = b \circ s_1$, $f = i_2 \circ b \circ s_1$ et $i_2 \circ b = i_1$ pour qu'elle vérifie les deux autres et qu'elle soit bijective).

1.6.2. *Opération définie sur un quotient.* Soit A un ensemble muni d'une loi interne $\star : A \times A \to A$ (addition, multiplication, soustraction, ...) et d'une relation d'équivalence $\mathcal{R}$. Pour pouvoir définir une loi sur $A/\mathcal{R}$ (qui sera alors unique, et qu'on continuera en général à noter $\star$) en posant

$$\overline{x} \star \overline{y} = \overline{x \star y},$$

il faut et il suffit que

$$\forall x, x', y, y' \in A \quad \left(\left(\overline{x} = \overline{x'} \text{ et } \overline{y} = \overline{y'}\right) \Rightarrow \overline{x \star y} = \overline{x' \star y'}\right).$$

C'est un corollaire immédiat du théorème 1.11, appliqué à l'ensemble $E := A \times A$ muni de la relation d'équivalence $\mathcal{S} := \mathcal{R} \times \mathcal{R}$ (c.-à-d. $(a, b)\mathcal{S}(a', b') \Leftrightarrow (a\mathcal{R}a' \text{ et } b\mathcal{R}b')$) et à l'ensemble $F := A/\mathcal{R}$. Plus généralement, on obtient de même :

Corollaire 1.13. *Soient A, B, C trois ensembles, munis respectivement des relations d'équivalence $\mathcal{R}$, $\mathcal{S}$ et $\mathcal{T}$, et soit $f : A \times B \to C$ une application. Pour qu'il existe une application $\overline{f} : A/\mathcal{R} \times B/\mathcal{S} \to C/\mathcal{T}$ vérifiant*

$$\forall a \in A \quad \forall b \in B \quad \overline{f}(\overline{a}, \overline{b}) = \overline{f(a, b)}$$

(où $\overline{a}$, $\overline{b}$ et $\overline{f(a, b)}$ désignent des classes d'équivalence pour, respectivement, $\mathcal{R}$, $\mathcal{S}$ et $\mathcal{T}$), il faut et il suffit que

$$\forall a, a' \in A \quad \forall b, b' \in B \quad ((a\mathcal{R}a' \text{ et } b\mathcal{S}b') \Rightarrow f(a, b)\mathcal{T}f(a', b')).$$

De plus, l'application $\overline{f}$ est alors unique.

Exercices : *7, 8, 9.*

2. Compléments sur les cardinaux

2.1. **Équipotence.** *On suppose connu l'ensemble $\mathbb{N}$ des entiers naturels, muni de ses opérations et son ordre usuel (pour information : on le construit à l'aide d'axiomes de la théorie des ensembles, dont celui appelé l'axiome de l'infini), avec – par construction –*

$$0 = \varnothing \quad \text{et} \quad n+1 = n \cup \{n\} = \{0, 1, \dots, n\}).$$

Définition 2.1.

- *On dit que deux ensembles A et B sont* **équipotents***, et l'on note $A \sim B$, s'il existe une bijection de l'un des deux ensembles vers l'autre.*
- *On dit qu'un ensemble est* **fini** *s'il est équipotent à un certain entier naturel $n = \{k \in \mathbb{N} \mid k < n\}$, et* **infini** *sinon.*
- *On dit qu'un ensemble est* **dénombrable** *s'il est équipotent à l'ensemble $\mathbb{N}$ des entiers naturels, et* **au plus dénombrable** *s'il est fini ou dénombrable.*
- *On dit qu'un ensemble a la* **puissance du continu** *s'il est équipotent à l'ensemble $\mathbb{R}$ des nombres réels.*

Exemples 2.2.

- *Le seul ensemble équipotent à $0 = \varnothing$ est $\varnothing$; les ensembles équipotents à $1 = \{0\}$ sont les singletons ; ceux équipotents à $2 = \{0, 1\}$ sont les paires de deux éléments distincts, etc.*
- *Pour tout singleton $\{x\}$ et tout ensemble E, le produit cartésien $\{x\} \times E$ est équipotent à E.*
- *La bijection $\mathbb{N} \to \mathbb{N}^*$, $n \mapsto n+1$ montre que $\mathbb{N}^*$ est dénombrable*
- *La bijection $\mathbb{N} \to 2\mathbb{N}$, $n \mapsto 2n$ montre que l'ensemble $2\mathbb{N}$ des entiers naturels pairs est dénombrable.*
- *La bijection $\exp : \mathbb{R} \to \mathbb{R}_+^*$ montre que l'ensemble $\mathbb{R}_+^*$ des réels strictement positifs a la puissance du continu.*
- *$\mathbb{N}$ et $\mathbb{R}$ sont infinis, et même "infinis au sens de Dedekind", un ensemble étant dit infini au sens de Dedekind s'il est équipotent à l'une de ses parties propres ($\mathbb{N}^* \subsetneq \mathbb{N}$, $\mathbb{R}_+ \subsetneq \mathbb{R}$) ou, ce qui est équivalent, s'il contient une partie dénombrable ($\mathbb{N} \subset \mathbb{N}$, $\mathbb{N} \subset \mathbb{R}$). (Avec une version faible de l'axiome du choix, cette notion d'infinitude, a priori plus forte que la définition usuelle ci-dessus, est en fait équivalente.)*

Remarque 2.3. *L'équipotence a les trois propriétés d'une relation d'équivalence mais n'est pas une relation (binaire) au sens du chapitre 2, parce qu'elle n'a pas d'ensembles de départ et d'arrivée : la classe $\mathcal{U}$ de tous les ensembles ne forme pas un ensemble (sinon on tomberait sur le paradoxe de Russell, cf. chapitre 2) et même, aucune des "classes d'équivalence" de cette fausse relation d'équivalence n'est un ensemble (sauf la classe d'équipotence de $\varnothing$, égale au singleton $\{\varnothing\}$) car cela contredirait l'axiome de la réunion (toute réunion d'un ensemble d'ensembles est un ensemble), puisque pour tout ensemble $A \neq \varnothing$, la réunion de tous les ensembles équipotents à A est la classe $\mathcal{U}$.*

Définition 2.4. *À tout ensemble A, on associe un nouvel ensemble appelé cardinal de A et noté $\operatorname{card} A$ ou $|A|$ ou $\#A$, de telle façon que*

$$A \sim B \Leftrightarrow \operatorname{card} A = \operatorname{card} B.$$

Nous admettrons que cette construction est possible (au sein de la théorie des ensembles, de la même façon qu'on a "codé" les couples de telle façon que les égalités entre couples soient celles attendues, et qu'on a "codé" chaque entier naturel par un ensemble), avec de plus, pour tout $n \in \mathbb{N}$, $\operatorname{card} n = n$. On peut alors démontrer :

Proposition 2.5. *Soient E un ensemble fini de cardinal n et F un ensemble.*

- *S'il existe une injection $i : F \to E$ alors F est fini de cardinal $p \leq n$; si de plus $p = n$, alors i est bijective.*
- *S'il existe une surjection $s : E \to F$ alors F est fini de cardinal $p \leq n$; si de plus $p = n$, alors s est bijective.*

Définition 2.6.

- *Les entiers naturels sont appelés les cardinaux finis.*
- *Le cardinal d'un ensemble dénombrable est noté $\aleph_0$* [1].

2.2. **Arithmétique.** *Lorsque A est fini, $|A|$ est le nombre d'éléments de A. La définition suivante étend donc de façon naturelle les opérations arithmétiques usuelles sur les cardinaux finis (les entiers naturels) aux cardinaux quelconques, ce qui justifie l'appellation de "nombres cardinaux" pour ces derniers.*

Définition 2.7. *Soient α et β deux nombres cardinaux et A et B deux ensembles tels que $\alpha = \operatorname{card} A$ et $\beta = \operatorname{card} B$. On définit la somme, le produit et l'exponentiation des cardinaux α et β par :*

$$\alpha + \beta := \operatorname{card}\left[(\{0\} \times A) \cup (\{1\} \times B)\right], \quad \alpha\beta := \operatorname{card}(A \times B) \quad \text{et} \quad \alpha^\beta := \operatorname{card}\left(A^B\right).$$

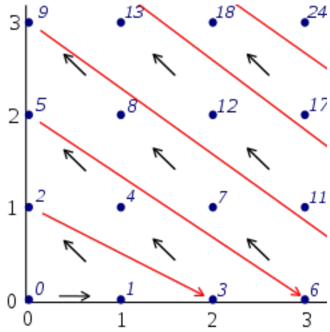
Exemples 2.8.

- *$\aleph_0 + \aleph_0 = \aleph_0$, c.-à-d. qu'il existe une bijection de $\{0, 1\} \times \mathbb{N}$ dans $\mathbb{N}$ (par exemple : $(a, n) \mapsto 2n + a$).*

---

1. Cette notation a été choisie par Georg Cantor.

— $\aleph_0\aleph_0 = \aleph_0$, *c.-à-d. qu'il existe une bijection de* $\mathbb{N}$ *dans* $\mathbb{N}\times\mathbb{N}$. *La plus célèbre est la fonction de couplage de Cantor, obtenue en traçant dans le premier quadrant du plan les parallèles successives* $y=-x, y=1-x, y=2-x,\ldots$ *et en numérotant à partir du bas, sur chacune de ces droites, les points à coordonnées entières positives :* $0\mapsto(0,0)$, $1\mapsto(1,0)$, $2\mapsto(0,1)$, *etc. On démontre facilement que le point de*



coordonnées (p,q) *portera le numéro* $\frac{(p+q+1)(p+q)}{2}+q$.

— $n\aleph_0=\aleph_0$ *et* $\aleph_0^n=\aleph_0$ *pour tout* $n\in\mathbb{N}^*$ *(par récurrence).*

Remarques 2.9.

— *L'ensemble* $(\{0\}\times A)\cup(\{1\}\times B)$ *est appelé l'union disjointe de* A *et* B *et noté* $A\sqcup B$. *Lorsque* A *et* B *sont disjoints,* $A\sqcup B$ *est équipotent à* $A\cup B$ *(exercice facile, corrigé sur Wikiversité).*

— *Pour que la définition 2.7 ait un sens, il faut bien sûr vérifier que les "opérations" union disjointe, produit cartésien et exponentiation ensembliste passent bien au "quotient" par la "relation" d'équivalence* $\sim$ *(l'équipotence). Les guillemets sont là pour rappeler qu'il ne s'agit pas d'ensembles (remarque 2.3), mais le principe est le même que dans le corollaire 1.13 : on vérifie (exercice facile, corrigé sur Wikiversité) que si* $A\sim A'$ *et* $B\sim B'$ *alors* $A\sqcup B\sim A'\sqcup B'$, $A\times B\sim A'\times B'$ *et* $A^B\sim A'^{B'}$.

— 2^X *désigne l'ensemble des applications de* X *dans* $2=\{0,1\}$ *et cet ensemble est en bijection avec* $\mathcal{P}(X)$ *(cf. chapitre 1, fin du § 3). On a donc, pour tout ensemble* X *:*

$$|\mathcal{P}(X)| = \left|2^X\right| = 2^{|X|}.$$

— *Attention, une union dénombrable d'ensembles dénombrables est dénombrable (cf. exercice 10) mais* **un produit dénombrable d'ensembles dénombrables n'est pas dénombrable** *(cf. § suivant).*

Théorème 2.10. *Soient* α, β *et* γ *des cardinaux. On a alors :*

— *commutativité :* $\begin{cases}\alpha+\beta=\beta+\alpha\\ \alpha\beta=\beta\alpha\end{cases}$;

— *associativité :* $\begin{cases}(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)\\ (\alpha\beta)\gamma=\alpha(\beta\gamma)\end{cases}$;

— *distributivité :* $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$;

— *propriétés de* 0 *et* 1 *:* $0+\alpha=1\alpha=\alpha^1=\alpha$, $\alpha^0=1$, $0\alpha=0$;

— *propriété de l'exponentielle :* $\alpha^{\beta+\gamma}=\alpha^\beta\alpha^\gamma$, $\quad(\alpha\beta)^\gamma=\alpha^\gamma\beta^\gamma \quad$ *et* $\quad(\alpha^\beta)^\gamma=\alpha^{\beta\gamma}$.

Preuve. *Ces propriétés se déduisent, respectivement, des propriétés similaires pour les ensembles (exercice 13).* □

2.3. **Comparaison des cardinaux.**

Définition 2.11. *Soient* A *et* B *deux ensembles avec* $\alpha=\operatorname{card}A$ *et* $\beta=\operatorname{card}B$. *On dit que* α *est inférieur ou égal à* β, *et l'on écrit* $\alpha\le\beta$, *s'il existe une injection de* A *dans* B.

On dit que α *est strictement inférieur à* β, *et l'on écrit* $\alpha<\beta$, *si* $\alpha\le\beta$ *et* $\alpha\ne\beta$.

Remarques 2.12.

— *De même que l'addition, la multiplication et l'exponentiation, on vérifie facilement (exercice) que la "relation"* $\le$ *sur les cardinaux (encore avec des guillemets, cf. remarque 2.3) est bien définie, c'est-à-dire que si* $A\sim A'$ *et* $B\sim B'$ *et s'il existe une injection de* A *dans* B, *alors il existe une injection de* A' *dans* B'.

— *On a* $0\le\alpha$ *pour tout cardinal* α *(exercice très facile).*

— *S'il existe une injection* $i:A\to B$ *et si* A *est non vide, alors il existe une surjection* $s:B\to A$ *(exercice 5). La réciproque (pour tous ensembles* A *et* B, *s'il existe une surjection* $s:B\to A$ *alors il existe une injection* $i:A\to B$*) est équivalente à l'axiome du choix*[2], *dont il ne sera pas question dans ce cours. Cela justifie de définir* $\le$ *à l'aide d'injections dans un sens plutôt que de surjections dans l'autre.*

2. Si B est au plus dénombrable, cet axiome n'est pas nécessaire car si $B\subset\mathbb{N}$, on peut simplement poser $i(a)=$ le plus petit antécédent de a par s.

— *La "relation" $\leq$ entre cardinaux est évidemment réflexive et transitive. Le théorème suivant montre qu'elle est également antisymétrique. C'est donc une "relation" d'ordre. La comparabilité cardinale, c.-à-d. l'affirmation que cet ordre est total, est, elle aussi, équivalente à l'axiome du choix.*
— $\aleph_0$ *est alors le plus petit cardinal infini.*

Théorème 2.13. Théorème de Cantor-Bernstein *(admis) Soient A et B deux ensembles.*

$$\operatorname{card} A \leq \operatorname{card} B \qquad \text{et} \qquad \operatorname{card} B \leq \operatorname{card} A \implies \operatorname{card} A = \operatorname{card} B$$

Autrement dit : à partir d'une injection $f : A \to B$ et d'une injection $g : B \to A$, on sait construire une bijection entre A et B (ce qui n'a rien d'évident, contrairement à ce que les notations pourraient faire croire).

Le théorème de Cantor-Bernstein permet, comme dans la preuve du théorème suivant, d'établir l'existence de bijections sans prendre la peine d'en expliciter une.

Théorème 2.14.

$$|\mathbb{R}| = 2^{|\mathbb{N}|}.$$

Preuve. *D'après le théorème de Cantor-Bernstein, il suffit de trouver une injection de $\mathbb{R}$ dans $\mathcal{P}(\mathbb{N})$ (ou dans $\mathcal{P}(\mathbb{Q})$: cela revient au même puisque $\mathbb{Q}$ est dénombrable – exercice 12) et une injection de $\{0,1\}^{\mathbb{N}}$ dans $\mathbb{R}$.*

L'application

$$\begin{array}{rccc} f & : & \mathbb{R} & \longrightarrow & \mathcal{P}(\mathbb{Q}) \\ & & x & \longmapsto & \{q \in \mathbb{Q} \mid q < x\} \end{array}$$

est injective car $\forall x \in \mathbb{R} \quad x = \sup(f(x))$.

L'application

$$\begin{array}{rccc} g & : & \{0,1\}^{\mathbb{N}} & \longrightarrow & \mathbb{R} \\ & & (a_n)_n & \longmapsto & 0, a_0 a_1 a_2 a_3 \dots \end{array}$$

(qui fait correspondre, à une suite de zéros et de uns, le nombre réel compris entre 0 et 1 dont les décimales sont données par cette suite) est injective. □

Corollaire 2.15. *Tout produit dénombrable d'ensembles dénombrables a la puissance du continu. Autrement dit :*

$$\left|\mathbb{N}^{\mathbb{N}}\right| = |\mathbb{R}|.$$

Preuve. *Cf. exercice 13.*

Théorème 2.16. Théorème de Cantor *Pour tout ensemble A,*

$$|A| < 2^{|A|}.$$

Preuve. *Soit A un ensemble. L'injection*

$$\begin{array}{ccc} A & \longrightarrow & \mathcal{P}(A) \\ a & \longmapsto & \{a\} \end{array}$$

montre que $|A| \leq 2^{|A|}$. Il reste à prouver qu'il n'existe pas de bijection entre A et $\mathcal{P}(A)$. On va même montrer qu'aucune application de A dans $\mathcal{P}(A)$ n'est surjective.

Considérons pour cela, étant donnée une application $f : A \to \mathcal{P}(A)$, l'ensemble

$$Z := \{a \in A \mid a \notin f(a)\}.$$

Cet élément Z de $\mathcal{P}(A)$ n'a aucun antécédent a par f. En effet, par définition de Z, si l'on avait $f(a) = Z$, on aurait $a \in Z \Leftrightarrow a \notin Z$. □

Remarque 2.17. *On aura reconnu dans cette preuve le raisonnement déjà vu pour montrer que la classe de tous les ensembles ne forme pas un ensemble (paradoxe de Russell).*

Corollaire 2.18. *Pour tout nombre cardinal α, on a $\alpha < 2^{\alpha}$.*

En particulier, $\mathbb{R}$ n'est pas dénombrable.

Commentaire : *La célèbre hypothèse du continu affirme qu'il n'y a aucun cardinal entre celui de $\mathbb{N}$ et celui de $\mathbb{R}$. Cette hypothèse a donné lieu à des travaux difficiles avec deux résultats majeurs : Gödel (1938) montrera que l'hypothèse du continu est consistante avec la théorie des ensembles (en supposant celle-ci consistante) ; autrement dit, on ne risque pas plus de contradiction en l'ajoutant aux axiomes de base. Cohen (1963) montrera que la négation de l'hypothèse du continu est, elle aussi, consistante avec la théorie des ensembles ! Elle est donc indécidable.*

Exercices : 10, 11, 12, 13, 14 question 5.

3. Exercices

Pour tous les liens ci-dessous vers des solutions, le préfixe est https ://fr.wikiversity.org/wiki/

Exercice 1. *Soient une application $f : A \to B$ et soient $X, X' \subset A$ et $Y, Y' \subset B$. Prouver que :*

i) $f(\varnothing) = \varnothing = f^{-1}(\varnothing)$; $f^{-1}(B) = A$;
ii) $f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y')$ *et* $f(X \cup X') = f(X) \cup f(X')$;
iii) $Y \subset Y' \Rightarrow f^{-1}(Y) \subset f^{-1}(Y')$ *et* $X \subset X' \Rightarrow f(X) \subset f(X')$;
iv) $f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y')$ *et* $f(X \cap X') \subset f(X) \cap f(X')$;
v) $X \subset f^{-1}(f(X))$ *et* $f(f^{-1}(Y)) = Y \cap \operatorname{Im} f$;
vi) $f^{-1}(\complement_B Y) = \complement_A f^{-1}(Y)$;
vii) $X \subset f^{-1}(Y) \Leftrightarrow f(X) \subset Y$;
viii) $f(f^{-1}(Y)) = Y \cap \operatorname{Im} f$.

Solutions :Application_(mathématiques)/Exercices/Images_directes_et_réciproques.

Exercice 2. *Pour toute application $f : A \to B$:*

1) *montrer que les propositions suivantes sont équivalentes :*
- *i)* f *est injective,*
- *ii)* $\forall X \in \mathcal{P}(A) \quad f^{-1}(f(X)) = X$,
- *iii)* $\forall X, X' \in \mathcal{P}(A) \quad f(X \cap X') = f(X) \cap f(X')$,
- *iv)* $\forall X \in \mathcal{P}(A) \quad f(\complement_A X) \subset \complement_B f(X)$;

2) *montrer que les propositions suivantes sont équivalentes :*
- *i)* f *est surjective,*
- *ii)* $\forall Y \in \mathcal{P}(B) \quad f(f^{-1}(Y)) = Y$,
- *iii)* $\forall X \in \mathcal{P}(A) \quad f(\complement_A X) \supset \complement_B f(X)$.

Solutions : Application_(mathématiques)/Exercices/Injection,_surjection,_bijection#Exercice_1 et 2.

Exercice 3. *Soient $f : A \to B$ et $g : B \to C$. Montrer que :*

1. *Si $g \circ f : A \to C$ est injective alors f est injective.*
2. *Si $g \circ f : A \to C$ est surjective alors g est surjective.*

Solution : .../Injection,_surjection,_bijection#Exercice_3.

Exercice 4. *Soient X et Y deux parties d'un ensemble E et*

$$f : \mathcal{P}(E) \to \mathcal{P}(X) \times \mathcal{P}(Y), \quad A \mapsto (A \cap X, A \cap Y).$$

Donner une CNS sur X et Y pour que f soit :
1. injective ; 2. surjective ; 3. bijective.

Solution : .../Injection,_surjection,_bijection#Exercice_8.

Exercice 5. *Soit $i : A \to B$ une injection. On suppose $A \neq \varnothing$.*

1) *Montrer qu'il existe une application $s : B \to A$ telle que $s \circ i = \mathrm{id}_A$.*
2) *En déduire que :*
- *(a)* *pour toute application $f : A \to C$, il existe une application $g : B \to C$ telle $f = g \circ i$;*
- *(b)* *i est simplifiable à gauche, c.-à-d.*

$$\forall C \quad \forall h, h' : C \to A \quad (i \circ h = i \circ h' \Rightarrow h = h') \ ;$$

- *(c)* *si $A \neq \varnothing$ et s'il existe une injection de A dans B, alors il existe une surjection de B dans A.*

3) *Qu'en est-il si $A = \varnothing$?*

Solution : .../Injection,_surjection,_bijection#Exercice_4.

Exercice 6. *Montrer qu'une application $s : B \to A$ est surjective si et seulement si elle est simplifiable à droite, c.-à-d.*

$$\forall C \quad \forall f, f' : A \to C \quad (f \circ s = f' \circ s \Rightarrow f = f').$$

Solution : .../Injection,_surjection,_bijection#Exercice_5.

Exercice 7. *1. Sur $X = \mathbb{N} \times \mathbb{N}$: $(m,n)\mathcal{R}(m',n') \iff m + n' = n + m'$ est une relation d'équivalence.*

a) Montrer que l'opération $\overline{(m,n)} + \overline{(s,t)} = \overline{(m+s, n+t)}$ est bien définie.

b) Montrer que l'opération $\overline{(m,n)} * \overline{(s,t)} = \overline{(ms+nt, ns+mt)}$ est bien définie.

c) Quel est l'intérêt de ces relations ?

Exercice 8. *Soit $n \in \mathbb{N}$. On note $\mathbb{Z}_n$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n.*

1. a) Montrer que la loi d'addition $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ induit une loi d'addition dans $\mathbb{Z}_n$.

b) Écrire les tables d'addition de $\mathbb{Z}_5$ et $\mathbb{Z}_6$.

2. a) Montrer que la loi de multiplication $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ induit une loi de multiplication dans $\mathbb{Z}_n$.

b) Écrire les tables de multiplication de $\mathbb{Z}_5$ et $\mathbb{Z}_6$.

Exercice 9. *(Extrait de l'examen de janvier 2018)*

On note $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, -\overline{1}\}$ l'ensemble des classes de congruence modulo 3, muni des opérations $+$ et $\times$ (déduites, par passage au quotient, des opérations usuelles sur $\mathbb{Z}$, donc héritant des bonnes propriétés de ces opérations usuelles – associativité, commutativité, neutres, distributivité – qui font de $\mathbb{F}_3$ ce qu'on appelle un anneau commutatif unitaire).

1) *Dresser les tables de ces deux opérations sur $\mathbb{F}_3$.*
2) *Soit $A = \mathbb{F}_3[X]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_3$ et $B \subset A$ le sous-ensemble des polynômes de degré strictement inférieur à 2 (y compris le polynôme $\overline{0}$, qui par convention est de degré $-\infty$).*
   Dresser la liste des éléments de B.
3) *En notant $q(P)$ et $r(P)$ (pour tout $P \in A$) le quotient et le reste de la division euclidienne de P par $X^2 + \overline{1}$ dans A, caractérisés par*
   $$q(P) \in A, \quad r(P) \in B \quad \text{et} \quad P = \left(X^2 + \overline{1}\right) q(P) + r(P),$$
   on définit sur A une relation d'équivalence $\mathcal{R}$ par :
   $$P\mathcal{R}Q \Leftrightarrow r(P) = r(Q).$$
   On note $\mathrm{cl}(P)$ la $\mathcal{R}$-classe d'un élément $P \in A$.
   Montrer que l'application
   $$\overline{r} : A/\mathcal{R} \to B, \quad \mathrm{cl}(P) \mapsto r(P)$$
   est bien définie et bijective.
4) *Montrer que $P\mathcal{R}Q$ si et seulement si $X^2 + \overline{1} \mid P - Q$ (c'est-à-dire si $P - Q$ est le produit de $X^2 + \overline{1}$ par un polynôme de A).*
5) *Montrer qu'il existe une unique application $\oplus : A/\mathcal{R} \times A/\mathcal{R} \to A/\mathcal{R}$ et une unique application $\otimes : A/\mathcal{R} \times A/\mathcal{R} \to A/\mathcal{R}$ telles que*
   $$\forall P, Q \in A \quad \mathrm{cl}(P) \oplus \mathrm{cl}(Q) = \mathrm{cl}(P+Q) \text{ et } \mathrm{cl}(P) \otimes \mathrm{cl}(Q) = \mathrm{cl}(P \times Q).$$
6) *Calculer $r(-X^2)$ et $r((X + \overline{1})(X - \overline{1}))$, puis montrer que*
   $$\forall P \in B \setminus \{\overline{0}\} \quad \exists Q \in B \quad r(P \times Q) = \overline{1}.$$
   Comment cette propriété se traduit-elle sur les éléments de l'anneau $A/\mathcal{R}$?

Exercice 10. *On rappelle que $\mathbb{N} \times \mathbb{N}$ est dénombrable.*

1. Soit $(E_p, f_p)_{p \in \mathbb{N}}$ une suite d'ensembles dénombrables E_p, munis chacun d'une bijection $f_p : \mathbb{N} \to E_p$. Déduire du rappel que l'ensemble $\cup_{p \in \mathbb{N}} E_p$ est dénombrable.

2. En déduire que l'ensemble des nombres complexes algébriques (c.-à-d. racines d'un polynôme non nul à coefficients rationnels) est dénombrable.

Exercice 11. *Montrer que tout intervalle réel non trivial (c.-à-d. contenant au moins deux réels) a la puissance du continu.*

Solution : Introduction_aux_mathématiques/Exercices/Ensembles_infinis#Exercice_1-6.

Exercice 12. *Vrai ou faux ? (justifier !)*

1. $\mathbb{Q}$ *est dénombrable ?*
2. $[0,1] \cap \mathbb{Q}$ *est équipotent à* $[0,1]$ *?*
3. *Soient* $a, b \in \mathbb{R}$, $a < b$. *Si* $f : [a,b] \to \mathbb{R}$ *est continue, alors* $\mathrm{Im}(f)$ *est équipotent à* $[a,b]$ *?*
4. *L'ensemble* $\mathcal{P}_f(\mathbb{N})$ *des parties finies de* $\mathbb{N}$ *est dénombrable ?*
5. *S'il existe une injection non surjective de* E *dans* F *alors* $\operatorname{card} E < \operatorname{card} F$ *?*
6. *S'il existe une surjection non injective de* E *dans* F *alors* $\operatorname{card} E > \operatorname{card} F$ *?*

Exercice 13. 1. *Démontrer que pour tous cardinaux* α, β *et* γ,

$$\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma, \quad (\alpha\beta)^\gamma = \alpha^\gamma \beta^\gamma \quad \text{et} \quad (\alpha^\beta)^\gamma = \alpha^{\beta\gamma}.$$

2. *En déduire que* $\mathbb{R}^\mathbb{N}$ *et* $\mathbb{N}^\mathbb{N}$ *ont la puissance du continu.*
   Solutions :
   Application (mathématiques)/Exercices/Bijections_ canoniques (question 1) ;
   Introduction_aux_mathématiques/Exercices/Ensembles_infinis#Exercice_1-1 (question 2).

Exercice 14. *(Extrait de l'examen de janvier 2018)*

On rappelle que l'ensemble $\mathbb{N}^\mathbb{N}$ *des applications de* $\mathbb{N}$ *dans* $\mathbb{N}$ *est équipotent à* $\mathbb{R}$, *et que* $S_\mathbb{N}$ *désigne le sous-ensemble des bijections de* $\mathbb{N}$ *dans* $\mathbb{N}$. *On note* $I\overline{S}$, $S\overline{I}$ *et* $\overline{IS}$ *les parties de* $\mathbb{N}^\mathbb{N}$ *constituées respectivement des injections non surjectives, des surjections non injectives et des applications ni injectives, ni surjectives.*

1) *Montrer que* $I\overline{S}$ *et* $S\overline{I}$ *sont non vides.*
2) *Soient* $g \in I\overline{S}$ *et* $h \in S\overline{I}$. *Expliquer rapidement pourquoi* $f \mapsto g \circ f$, $f \mapsto f \circ h$ *et* $f \mapsto g \circ f \circ h$ *sont des injections de* $S_\mathbb{N}$ *dans (respectivement)* $I\overline{S}$, $S\overline{I}$ *et* $\overline{IS}$. *(On rappellera, sans les démontrer, les propriétés utilisées reliant injectivité, surjectivité et composition.)*
3) *Pour toute partie* A *de* $\mathbb{N}$, *on définit* $f_A : \mathbb{N} \to \mathbb{N}$ *par : pour tout* $n \in A$, f_A *échange* $2n$ *et* $2n+1$ *et pour tout* $n \in \mathbb{N} \setminus A$, f_A *fixe* $2n$ *et* $2n+1$. *Montrer que* f_A *est bijective, en précisant sa bijection réciproque.*
4) *On considère l'application* $F : \mathcal{P}(\mathbb{N}) \to S_\mathbb{N}$, $A \mapsto F(A) = f_A$. *Montrer qu'il existe une application* $G : S_\mathbb{N} \to \mathcal{P}(\mathbb{N})$ *telle que* $G \circ F = \mathrm{Id}_{\mathcal{P}(\mathbb{N})}$.
5) *Déduire des questions 4 et 2 que* $S_\mathbb{N}$, $I\overline{S}$, $S\overline{I}$ *et* $\overline{IS}$ *sont équipotents à* $\mathbb{R}$.

Solution : ../Ensembles_infinis#Exercice_1-5.