

1 Introduction

Nous n'avons pas l'intention de présenter ici une théorie mathématique rigoureuse et complète. Il faudrait pour cela des prérequis de logique, un appareillage complexe, choisir entre différentes axiomatiques... Nous nous bornerons à une partie de la «théorie naïve des ensembles», selon l'expression de Paul Halmös.

1 Ensembles, applications

1.1 Ensembles

Acceptons la notion intuitive d'ensemble et d'appartenance.

Définition 1 (?). Un ensemble E est un objet mathématique tel si x est un objet mathématique, la relation d'appartenance $x \in E$ est soit vraie, soit fausse.

Les objets x pour lesquels la relation $x \in E$ est vraie sont appelés les **éléments** de E . Deux ensembles sont égaux s'ils ont exactement les mêmes éléments.

- Un ensemble est défini en **extension** si on en donne la liste des éléments, liste mise entre des accolades.

$$E = \{1, 2, 4, 8\}, F = \{1, 2, 4, 8, \dots, 2^n, \dots\}$$

La seconde version est intuitivement compréhensible, mais « incorrecte ». Un cas particulier : $\emptyset = \{\}$ est l'ensemble qui n'a aucun élément, on l'appelle **ensemble vide** ; $\{\emptyset\}$ est un ensemble qui a un élément : $\emptyset \in \{\emptyset\}$.

- Un ensemble est défini en **compréhension** lorsqu'on définit ses éléments par une propriété, exprimée sous forme d'une proposition mathématique.

Dans ce second cas, il pourra être utile de se poser la question : mon ensemble peut-il être vide ? Admettons qu'on connaisse l'ensemble des nombre entiers naturels $\mathbb{N}$. On peut alors définir les ensembles :

- $F = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, n = 2^k\}$
- $\mathcal{A} = \{n \in \mathbb{N} \mid n \mid 60\}$
- $\mathcal{Q} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$
- $\mathcal{P} = \{p \in \mathbb{N} \mid (\forall n \in \mathbb{N}, n \mid p \Rightarrow n = 1 \text{ ou } n = p) \text{ et } (p \neq 1)\}$
- $\mathcal{I} = \{a \in \mathbb{N} \mid \exists b \in \mathbb{N}, a^2 - 1973b^2 = -1\}$

Il est facile de voir que l'ensemble F est formé des puissances de 2, l'ensemble $\mathcal{P}$ est formé des nombres premiers, les deux ensembles $\mathcal{A}$ et $\mathcal{Q}$ sont égaux, et quant à l'ensemble $\mathcal{I}$, il n'est pas du tout immédiat de décider s'il est ou non vide¹. Mais étant donné un nombre a , on peut décider rapidement s'il est, ou non, dans l'ensemble $\mathcal{I}$.

1. Il est non vide : essayer avec $a = 88526$ et $b = 1993$.

On appelle **sous-ensemble** d'un ensemble E , un ensemble F tel que : $\forall x \in F, x \in E$, et on écrit $F \subset E$. L'ensemble vide et E lui-même sont des sous-ensembles de E .

Remarque 1. – Un ensemble est défini en compréhension de la façon suivante

$$\mathcal{A} = \{x \in E \mid p(x)\}$$

et ses éléments sont a priori choisis dans un ensemble E , p étant une propriété qui a un sens pour les éléments de E . Si on ne fait pas cette restriction, on pourrait écrire :

$$\mathcal{A} = \{x \mid x \notin x\}$$

et la proposition $\mathcal{A} \in \mathcal{A}$ risque de donner des maux de têtes : est-elle vraie, mais alors elle est fausse ?...

- Autre remarque : un «vrai» logicien ne fait pas la différence entre des êtres mathématiques qui seraient des ensembles, d'autres qui n'auraient vocation qu'à être des éléments. Dans la «vraie» théorie des ensembles, tout est ensemble. Un mathématicien « ordinaire » fait plutôt une hiérarchie :

$$0, [0, 1], \text{ l'ensemble des intervalles fermés.}$$

Rappelons également que $\mathcal{P}(E)$ est l'ensemble de tous les sous-ensembles de E . Il contient en particulier l'ensemble vide et E lui-même.

1.2 Union et intersection de deux ensembles, produit cartésien.

Si A et B sont deux ensembles, on définit leur union $A \cup B$ et leur intersection $A \cap B$ par :

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\} \quad A \cap B = \{x \mid x \in A \text{ et } x \in B\}$$

Ce sont deux ensembles (et cela nécessite un axiome pour l'union, en vertu de la remarque précédente, alors que l'intersection peut être définie comme $\{x \in A \mid x \in B\}$). Les opérations ainsi définies ont des propriétés bien connues que nous ne détaillerons pas. Signalons également la définition de la différence ensembliste

$$A \setminus B = \{x \in A \mid x \notin B\}$$

et rappelons que la proposition $A \subset B$ est une abréviation de $A \cap B = A$. Si $A \subset B$, l'ensemble $B \setminus A$ s'appelle le complémentaire de A dans B .

On va maintenant définir le couple (a, b) : c'est l'ensemble

$$(a, b) = \{a, \{a, b\}\}$$

Cela permet d'obtenir l'équivalence :

$$(a, b) = (a', b') \quad \Longleftrightarrow \quad (a = a' \text{ et } b = b')$$

Ne pas confondre le couple (a, b) avec l'ensemble (la paire) $\{a, b\}$; avec notre définition, le couple (a, a) désigne l'ensemble $\{a, \{a\}\}$. Cette définition des couples peut paraître inutilement abstraite, et elle masque la «symétrie» qu'il y a entre (a, b) et (b, a) .

Définition 2. Le **produit cartésien**² de deux ensembles est l'ensemble des couples :

$$A \times B = \{(a, b) \mid a \in A \text{ et } b \in B\}$$

1.3 Relations, Applications

Des définitions :

- Une relation binaire $\mathcal{R}$ est un sous-ensemble de $A \times B$; on écrit $a \mathcal{R} b$ plutôt que $(a, b) \in \mathcal{R}$.
- Une application de A dans B est une relation f qui vérifie :

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

et

$$\forall a \in A, \forall (b, b') \in B \times B, \quad (a f b \text{ et } a f b') \Rightarrow (b = b')$$

Cela signifie qu'il y a toujours un b tel que tel que $a f b$ et qu'il alors unicité de b . On écrit :

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

Une relation un peu spéciale est l'égalité : L'ensemble $\mathcal{R}$ est alors

$$\mathcal{R} = \{(a, a) \mid a \in E\}$$

abréviation de

$$\mathcal{R} = \{x \in E \times E \mid \exists a \in E, x = (a, a)\}$$

On peut composer des relations, mais considérons seulement le cas des applications. Si $\mathcal{R}$ et $\mathcal{S}$ sont des applications, de A dans B , resp. de B dans C , $\mathcal{S} \circ \mathcal{R}$ est une application définie par :

$$z = \mathcal{S} \circ \mathcal{R}(x) \iff \exists y \in B \quad y = \mathcal{R}(x) \text{ et } z = \mathcal{S}(y)$$

C'est ce qu'on appelle «la loi rond».

L'ensemble des applications d'un ensemble A dans un ensemble B est noté B^A (chercher une justification de cette notation...). On peut alors définir les applications **injectives**, **surjectives** et **bijectives**.

1.4 Familles, produits

On appelle **famille** indexée par un ensemble I , une application de I dans un ensemble $\mathcal{A}$. On note a_i l'image de $i \in I$ et $(a_i)_{i \in I}$ la famille. Il est possible bien sûr que les a_i soient eux-mêmes des ensembles. Si $(A_i)_{i \in I}$ est une famille d'ensembles, il existe un ensemble qui est la **réunion** des ensembles A_i ; on le note

$$A = \bigcup_{i \in I} A_i$$

et il est caractérisé par :

$$a \in A \iff \exists i \in I, a \in A_i$$

2. En l'honneur de René Descartes, qui a utilisé les couples de coordonnées pour repérer des points.

Si I est de la forme $I = \{i_1, i_2\}$, on retrouve la réunion traditionnelle de deux ensembles. Si I est vide, la réunion est vide. Et si I est non vide, on peut définir l'intersection de la famille :

$$B = \bigcap_{i \in I} A_i$$

caractérisée par :

$$a \in B \iff \forall i \in I, a \in A_i$$

Il y a un peu de subtilité dans ces définitions : l'intersection d'une famille vide $I = \emptyset$ ne peut être définie sans contradiction, (c'est lié à l'impossibilité d'accepter l'existence de l'ensemble de tous les ensembles) ; bien sûr, l'intersection peut être vide, par exemple quand l'un des A_i est vide, mais pas seulement dans ce cas...

De même qu'on a défini le produit cartésien de deux ensembles, définissons le produit d'une famille par :

$$\prod_{i \in I} A_i = \{f : I \longrightarrow \bigcup_{i \in I} A_i \mid f(i) \in A_i\}$$

Se donner un élément de ce produit, c'est finalement se donner une famille, indexée par I , de la forme $(a_i)_{i \in I}$ où $a_i \in A_i$ pour tout $i \in I$, et si I a deux éléments, on retrouve (moyennant une identification), le produit cartésien habituel.

1.5 Relations d'équivalence

Une relation d'équivalence dans E est associée à un regroupement en « classes », ou à une « partition » de E . Rappelons : une famille $(E_i)_{i \in I}$ de sous-ensembles de E est une **partition** de E si :

- $\bigcup_{i \in I} E_i = E$.
- $\forall i, j \in I, (i \neq j) \Rightarrow (E_i \cap E_j = \emptyset)$

Définition 3. Une relation binaire dans E est une relation d'équivalence si elle a les trois propriétés :

- | | | |
|--|---|-------------------------|
| (1) $\forall x \in E,$ | $x \mathcal{R} x$ | (réflexivité) |
| (2) $\forall (x, y) \in E \times E,$ | $(x \mathcal{R} y) \Rightarrow (y \mathcal{R} x)$ | (symétrie) |
| (3) $\forall (x, y, z) \in E \times E \times E,$ | $(x \mathcal{R} y \text{ et } y \mathcal{R} z) \Rightarrow (x \mathcal{R} z)$ | (transitivité) |

On obtient alors la partition associée à une relation d'équivalence par :

Définition 4. À tout $a \in E$, on associe sa **classe d'équivalence** :

$$\bar{a} = \{b \in E \mid b \mathcal{R} a\}$$

et les classes d'équivalence forment une partition de E .

La démonstration est immédiate, et le lecteur vérifiera sans peine qu'à toute partition de E , on peut associer une relation d'équivalence.

2 Cardinal d'un ensemble

On ne peut se contenter d'une définition circulaire comme «le cardinal d'un ensemble est son nombre d'éléments». Depuis Cantor, on procède en gros de la façon suivante : on dit que deux ensembles sont **équipotents** s'il existe une bijection de l'un vers l'autre, et on conviendra que le cardinal d'un ensemble est la «classe» de tous les ensembles qui sont en bijection avec lui.

Attention, on ne peut parler d'«ensemble de tous les ensembles» sans contradiction. C'est pour cela qu'on a employé le terme un peu vague de classe.

2.1 Ensembles finis, infinis, dénombrables

Commençons par admettre qu'on a défini l'ensemble des nombres entiers $\mathbb{N}$: cet ensemble contient un élément noté 0 et tout élément n a un successeur, noté $n + 1$; deux éléments qui ont même successeur sont égaux, et 0 n'est pas un successeur. De plus, $\mathbb{N}$ a la propriété de récurrence, que l'on peut énoncer ainsi : pour tout $F \subset \mathbb{N}$, on a

$$\begin{cases} 0 \in F \\ \forall n \in \mathbb{N}, (n \in F \Rightarrow n + 1 \in F) \end{cases} \Rightarrow F = \mathbb{N}$$

On peut alors définir dans $\mathbb{N}$ l'addition, la multiplication et la relation d'ordre habituelle, que l'on appelle **ordre naturel** et que l'on note $\leq$. Nous ne détaillerons pas ces constructions. En suivant la démarche proposée dans le cas général, on va définir les ensembles finis, infinis, dénombrables :

- On dit qu'un ensemble A est **fini** s'il existe un entier n tel que A soit en bijection avec $\{1, \dots, n\}$ ³.
- Un ensemble est **infini** s'il n'est pas fini, et **dénombrable** s'il est en bijection avec $\mathbb{N}$.

Dans le cas d'un ensemble fini E , l'entier n est appelé **cardinal** de E et est noté $\text{card}(E)$.

Remarque 2. Cette définition a un sens, car on peut démontrer (par récurrence) que si $n \neq p$, l'ensemble $\{1, \dots, n\}$ et l'ensemble $\{1, \dots, p\}$ ne sont pas en bijection. On dit également que le cardinal de l'ensemble vide est 0.

On peut vérifier (voir par exemple la section suivante) que $\mathbb{Q}$ est dénombrable, mais un théorème célèbre attribué à Cantor affirme que $\mathbb{R}$ n'est pas dénombrable.

Il est alors possible d'énoncer le théorème suivant :

Théorème 1. *Si E et F sont deux ensembles finis de même cardinal, toute injection (resp. surjection) de l'un dans l'autre, est bijective.*

Avant de faire la démonstration, remarquons l'analogie avec le théorème qui concerne les applications linéaires entre espaces vectoriels de même dimension finie.

Démonstration. Il convient d'abord de montrer que si F' est un sous-ensemble de F , alors F' est fini, de cardinal inférieur à celui de F . De plus, l'inclusion est stricte si et seulement si $\text{card}(F') < \text{card}(F)$. Ce lemme se démontre par récurrence sur le cardinal de F : si $\text{card}(F) = 1$, il est facile de déterminer tous les sous-ensembles de F et de vérifier le lemme. Supposons la proposition vraie pour tous les ensembles de cardinal n , et prenons F de cardinal $n + 1$, une bijection permet de supposer que $F = \{1, \dots, n + 1\}$. Soit F' un sous-ensemble strict de F . On

3. Notation qui représente bien sûr l'ensemble $\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$

peut supposer, quitte à composer par une bijection, que F' ne contient pas $n+1$, ainsi F' est un sous-ensemble de $\{1, \dots, n\}$. Si cette inclusion est stricte, l'hypothèse de récurrence s'applique, F' est fini de cardinal strictement inférieur à n donc à $n+1$. Sinon, F' coïncide avec $\{1, \dots, n\}$, il est de cardinal n , strictement inférieur à $n+1$.

Passons à la démonstration du théorème, et soit f injective de E dans F . Alors $f(E)$ est un sous-ensemble de F , qui est en bijection avec E , donc de même cardinal que E donc que F . On en déduit que $f(E) = F$ et que f est surjective. Le lecteur terminera la démonstration. ■

2.2 Théorème de Cantor-Bernstein

Il n'est pas toujours facile de définir une bijection entre deux ensembles. Le théorème suivant, qui n'est pas complètement banal, permet de prouver que deux ensembles ont même cardinal.

Théorème 2. Théorème de Cantor-Bernstein. *Soit A et B deux ensembles. On suppose qu'il existe une application f **injective** de A vers B , et une application g **injective** de B vers A . Alors A et B ont même cardinal.*

Démonstration. Commençons par observer que tout élément de A a au maximum un antécédent par g . Et tout élément de B a au maximum un antécédent par f . Partant d'un élément a de A , on peut construire une suite, éventuellement finie des antécédents successifs, par g puis par f , etc....

- Si cette suite est infinie, on dit que a est dans A_∞ .
- Si elle est finie, mais s'arrête en un élément de B , on dit que a est dans A_1 .
- Sinon, elle est finie et s'arrête en A , ou elle est vide, (cas où a n'a pas d'antécédent par g), on dit que a est dans A_0 .

On a ainsi défini une partition de A et on va en déduire une bijection ϕ de A dans B . Si $a \in A_0$ ou $a \in A_\infty$, on pose $\phi(a) = f(a)$. Si $a \in A_1$, il a un antécédent par g , et on pose $\phi(a) = g^{-1}(a)$, notation un peu abusive pour désigner cet antécédent unique. On peut définir de même dans B trois ensembles B_∞ , B_1 et B_0 .

- L'image de A_∞ par ϕ est alors incluse dans B_∞ , puisque si a a une infinité d'antécédents successifs, $f(a)$ aussi, et tout élément de B_∞ est l'image par ϕ d'un élément qui a une infinité d'antécédents successifs : ϕ restreint à A_∞ est donc bijective sur B_∞ .
- L'image de A_0 est formée de $f(a)$, où a a un nombre pair d'antécédents successifs; les $f(a)$ ont donc un nombre impair d'antécédents successifs, donc $f(a)$ est dans B_1 , et tout élément de B_1 est l'image par ϕ d'un élément de A_0 , pour les mêmes raisons; ϕ est bijective de A_0 sur B_1 .
- De même, ϕ réalise une bijection de A_1 sur B_0 .

En conclusion, ϕ est bien bijective de A sur B . ■

2.3 Le théorème de Cantor

Il s'agit de montrer que E et $\mathcal{P}(E)$ n'ont pas le même cardinal.

Théorème 3. Théorème de Cantor. *Il n'existe pas de surjection d'un ensemble E dans l'ensemble de ses sous-ensembles $\mathcal{P}(E)$*

Démonstration. Supposons que $f : E \rightarrow \mathcal{P}(E)$ soit surjective. L'image d'un élément de E est un sous-ensemble de E , et on peut donc considérer

$$F = \{x \in E \mid x \notin f(x)\}$$

Mais comme f est surjective, il existe $y \in E$ tel que $F = f(y)$. Si $y \in F$, c'est donc que $y \notin f(y)$ soit $y \notin F$, contradiction. L'alternative $y \notin F$ conduit à la même impasse, car y doit vérifier $y \in f(y) = F$, encore une contradiction⁴. ■

Il existe bien sûr une application injective de E dans $\mathcal{P}(E)$, et on peut donc dire que le cardinal de $\mathcal{P}(E)$ est strictement plus grand que le cardinal de E .

On peut montrer que $\mathcal{P}(E)$ est en bijection avec $\{0, 1\}^E$. Dans le cas où E est fini, on en déduit que

$$\text{card}(\mathcal{P}(E)) = 2^{\text{card } E}$$

3 Ensembles ordonnés, bon ordre

3.1 Définition

En plus des relations d'équivalence que nous verrons plus loin, il est utile de s'intéresser à des relations qui « ordonnent » les éléments d'un ensemble.

Définition 5. Une relation binaire, notée $\preceq$ dans E est une relation d'ordre si elle a les trois propriétés :

- | | | |
|--|---|----------------|
| (1) $\forall x \in E,$ | $x \preceq x$ | (réflexivité) |
| (2) $\forall (x, y) \in E \times E,$ | $(x \preceq y \text{ et } y \preceq x) \Rightarrow (x = y)$ | (antisymétrie) |
| (3) $\forall (x, y, z) \in E \times E \times E,$ | $(x \preceq y \text{ et } y \preceq z) \Rightarrow (x \preceq z)$ | (transitivité) |

L'exemple le plus immédiat est celui de la relation ordinaire $\leq$ dans les ensembles de nombres $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$. Un autre exemple est la relation d'inclusion entre des sous-ensembles d'un même ensemble E (par exemple entre les sous-espaces vectoriels d'un même espace vectoriel). Enfin un exemple intéressant est la relation « divise » parmi l'ensemble des entiers naturels (éventuellement privé de 0).

3.2 Définitions associées

Quelques définitions supplémentaires.

- Une relation d'ordre dans E permet parfois d'ordonner les éléments comme les points d'une droite. On dit qu'un ordre est **total** si

$$\forall (x, y) \in E \times E, \quad (x \preceq y \quad \text{ou} \quad y \preceq x)$$

c'est-à-dire si deux éléments quelconques sont toujours comparables. Une relation d'ordre qui n'est pas totale est dite **partielle**.

4. On pourra réfléchir à la phrase : le barbier de cette ville rase tous les hommes qui ne se rasent pas eux-mêmes, et ceux-là seulement.

- Un élément M de E est un **majorant** de $A \subset E$ si

$$\forall a \in A, \quad a \preceq M$$

- α est le **plus grand élément** (ou maximum) de A lorsque

$$\alpha \in A \quad \text{et} \quad \forall a \in A, \quad a \preceq \alpha$$

Et bien sûr, on définit de même minorant et plus petit élément (ou minimum). Deux notions un peu plus difficiles :

- s est **borne supérieure** de A si c'est le plus petit élément de l'ensemble des majorants de A .
- un élément μ de A est **maximal** si

$$\forall a \in A, \quad (\mu \preceq a) \Rightarrow (a = \mu)$$

Rappelons également que l'on abrège

$$x \preceq y \text{ et } x \neq y$$

par

$$x \prec y$$

On parle alors d'ordre strict : attention, ce n'est pas une relation d'ordre.

Quelques propriétés de démonstration facile :

Proposition 4. 1. *S'ils existent, les p.p.e, p.g.e, sup et inf sont uniques.*

2. *Par contre, majorant, minorant, élément maximal, élément minimal, s'ils existent, ne sont pas forcément uniques.*

3. *Si $A \subset E$ admet un p.g.e, alors ce p.g.e. est aussi la borne supérieure. Dans ce cas, on dit parfois que le sup est atteint. Idem de l'autre côté.*

et des exemples :

Dans $\mathbb{N} \setminus \{1, 0\}$, pour la relation divise : préciser si pour $A = \{a, b\}$ il y a des minorants, majorants, pge, ppe, sup et inf. Y-a-t-il des éléments minimaux ?

Dans $F = \mathcal{P}$, muni de la relation d'inclusion, même question, de même lorsque G est l'ensemble des sous-espaces vectoriels d'un espace vectoriel E , toujours muni de l'inclusion.

Rappelons enfin que, dans le cas des réels, la borne supérieure d'un ensemble A peut être caractérisée ainsi :

$$s = \text{Sup}(A) \iff \begin{cases} \forall a \in A, a \leq s \\ \forall \epsilon > 0, \exists a \in A, s - \epsilon < a \leq s \end{cases}$$

3.3 Bon ordre

Autre vocabulaire, une relation d'ordre dans E est un **bon ordre** si on a la propriété :

Toute partie non vide de E admet un plus petit élément. C'est le cas de $\mathbb{N}$, qui sert un peu de modèle, et de ses sous-ensembles. Une première remarque

Proposition 5. *Un bon ordre est un ordre total.*

Démonstration. Il suffit de dire que toute partie de la forme $\{a, b\}$ admet un plus petit élément.

■ Un théorème utile et important :

Théorème 6. *L'ensemble $\mathbb{N}$ est bien ordonné.*

Démonstration. On suppose bien sûr qu'on a défini la relation d'ordre sur $\mathbb{N}$, par exemple en posant

$$n \leq p \iff \exists k \in \mathbb{N}, p = n + k$$

On considère ensuite A , une partie non vide de $\mathbb{N}$, il s'agit de montrer qu'elle a un plus petit élément. Raisonnons par l'absurde, en supposant qu'il n'y a pas de plus petit élément. Soit alors B le complémentaire de A dans $\mathbb{N}$. Alors $0 \in B$, sinon 0 serait le plus petit élément de A . Si tout $k \leq n$ était dans B , alors $n + 1$ aussi, sinon $n + 1$ serait dans A et serait donc le plus petit élément de A . Donc B serait $\mathbb{N}$, et A serait vide. remarquons que nous avons utilisé ici la récurrence totale. ■

Par contre, l'exemple de $\mathbb{Z}$ avec l'ordre naturel montre qu'un ordre total n'est pas forcément un bon ordre. C'est également le cas de $\mathbb{R}^+$, avec l'ordre naturel : les intervalles ouverts à gauche, par exemple, n'ont pas de plus petit élément.

Passons maintenant à des considérations un peu plus délicates. Un théorème affirme :

Théorème 7. Théorème de Zermelo.

Tout ensemble peut être muni d'une relation de bon ordre.

Ce théorème est un peu surprenant, si on pense à des ensembles «grands» comme $\mathbb{R}$, pour lequel l'ordre naturel n'est certes pas un bon ordre. En fait, ce théorème résulte d'un axiome que nous n'avons pas encore énoncé, et qui est nommé l'**axiome du choix**.

Axiome 1. Axiome du choix

Tout produit $\prod_{i \in I} A_i$ d'ensembles non vides est non vide

Cet axiome est ainsi nommé car il signifie qu'il existe f dans ce produit, c'est-à-dire une application de I dans la réunion de A_i , telle que $f(i) \in A_i$ pour tout i ; on dit que c'est une **fonction de choix**. Lorsque la famille est infinie, l'existence d'une telle fonction n'est pas évidente : il s'agit de «choisir» d'un seul coup une infinité d'éléments, sans forcément avoir un algorithme. Terminons avec un troisième théorème, encore équivalent aux deux énoncés précédents :

Théorème 8. Théorème de Zorn

*Soit E un ensemble tel que toute partie $\mathcal{P}$ de $\mathcal{P}(E)$ qui est totalement ordonnée admet un majorant : on dit parfois que E est **inductif**. Alors E admet (au moins un) élément maximal.*

On peut déduire les théorèmes de l'axiome du choix, mais l'axiome est aussi impliqué par chacun des théorèmes. On va l'admettre, mais donnons néanmoins un exemple de démonstration : le théorème de Zorn implique le théorème de Zermelo.

Démonstration. Soit X un ensemble. On considère l'ensemble des parties de X qui peuvent être munies d'un bon ordre ; si A est une telle partie, on notera $(A, \preceq)$ le couple formé de cette partie et d'un bon ordre. Soit $\mathcal{X}$ l'ensemble de tous les couples possibles. Cet ensemble est non vide (il contient l'ensemble vide et l'ordre vide, et, si X est non vide, il contient les singletons), et il est muni d'un ordre partiel, le prolongement : on dira que A et B deux parties bien ordonnées de X vérifient $A \prec B$ si $A \subset B$ et si l'ordre de B prolonge celui de A , les éléments de $B \setminus A$

étant tous plus grands que ceux de A . Soit alors $\mathcal{P}$ une partie totalement ordonnée de $\mathcal{X}$. La réunion des éléments de $\mathcal{P}$ est bien ordonnée et c'est donc un majorant des éléments de $\mathcal{P}$. On en déduit que $\mathcal{X}$ contient un élément maximal M . Mais cet élément maximal est X lui-même, muni d'un bon ordre. En effet, si $x \in X \setminus M$, l'ensemble $\{x\} \cup M$ peut être muni d'un bon ordre (en prenant x supérieur à tous les autres éléments de M), contredisant ainsi la maximalité de M . ■

Reconnaissons qu'on n'utilise pas très souvent ces énoncés. Donnons un des exemples pour lesquels le théorème de Zorn est incontournable.

Théorème 9. *Tout espace vectoriel sur un corps K admet une base.*

Démonstration. E est un espace vectoriel et $\mathcal{V}$ l'ensemble des systèmes libres. On peut ordonner $\mathcal{V}$ par l'inclusion, et si $\mathcal{C}$ est un sous-ensemble totalement ordonné de $\mathcal{V}$, il admet un majorant, qui est la réunion des ensembles de $\mathcal{C}$: cette réunion U est un système libre (car si un sous-ensemble fini de U donnait une relation de liaison, ce sous-ensemble serait inclus dans un des éléments de $\mathcal{C}$, contradiction) et c'est un majorant de $\mathcal{C}$. On en déduit que l'ensemble des systèmes libres admet un élément maximal : un tel élément $\mathcal{B}$ est une base ; si en effet un vecteur x n'était pas dans $\text{vect}(\mathcal{B})$, l'ensemble $\mathcal{B} \cup \{x\}$ serait libre, contradiction avec la maximalité de $\mathcal{B}$. ■