

# L'axiome du choix

Xavier Caruso

Mars 2002

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Présentation de la théorie des ensembles</b>	<b>3</b>
2.1	Les axiomes de ZF	3
2.2	Constructions mathématiques usuelles	6
2.2.1	Ensembles “finis”	6
2.2.2	Couples, triplets, $n$ -uplets	6
2.2.3	Produits “finis”	6
2.2.4	Relations	7
2.2.5	Fonctions	7
2.2.6	Produits quelconques	8
2.2.7	Les nombres	8
2.3	Et les démonstrations dans tout ça	9
<b>3</b>	<b>Axiome du choix</b>	<b>10</b>
3.1	Énoncé	10
3.2	Commentaires	11
3.3	Axiome du choix dénombrable, axiome du choix dépendant	11
3.4	Énoncés équivalents classiques	13
3.5	Quelques exemples	14
3.5.1	Existence de bases dans les espaces vectoriels	15
3.5.2	Théorème de Tychonov	15
3.5.3	Théorème de Cantor-Bernstein	15
3.5.4	Dénombrabilité de $\mathbb{Q}$	16
3.5.5	Produits d’ouverts dans $\mathbb{R}$	17
3.5.6	Constructions par récurrence	17
3.5.7	Théorème de Baire	18
3.5.8	Complétude de $\mathbb{R}^n$	18
<b>4</b>	<b>Étude des bons ordres</b>	<b>19</b>
4.1	Présentation intrinsèque	19
4.2	Les ordinaux	20
4.3	Construction de $\mathbb{N}$	21
4.4	Principe d’induction	22
4.5	Retour sur les équivalents de l’axiome du choix	22
4.5.1	Théorème de Zermelo	22
4.5.2	Lemme de Zorn	23
4.6	D’autres applications	23
4.6.1	$E$ est-il en bijection avec $2E$ ?	23
4.6.2	$E$ est-il en bijection avec $E^2$ ?	24
4.6.3	Clôture algébrique	24
4.7	Quelque désillusion	25
<b>5</b>	<b>Conclusion</b>	<b>26</b>

# 1 Introduction

Nous allons parler de l'axiome du choix, spécifiquement dans un contexte mathématique et spécifiquement en logique classique dans l'axiomatisation des ensembles usuelle appelée ZF. Nous allons donc dans un premier temps présenter cette axiomatisation et faire tous les (r)appels nécessaires à un énoncé précis de l'axiome du choix.

Il est important d'avoir constamment en tête que la logique ne cherche pas à construire le “monde” à partir de rien, mais plutôt à supposer qu'il est là et à l'étudier. Bien entendu, pour cela, on se donne des a priori sur ce monde, ce que l'on appelle les axiomes, et on voit comment il réagit. Dans la suite, quand on parlera de modèle de ZF, il faut sans doute avoir à l'esprit qu'il s'agit simplement d'une boîte qui se comporte comme on lui demande et qui est censée se comporter comme le monde qui nous entoure. Ce sont ces boîtes, extérieures à nous osons le dire, que nous allons étudier.

Bon arrêtons de mal philosopher et parlons un peu de maths pour changer :-).

## 2 Présentation de la théorie des ensembles

Avant de parler de l'axiome du choix, il s'agit de formaliser les ensembles. La formalisation classique, que l'on appelle ZF (pour théorie de Zermelo-Fraenkel), est celle que nous allons présenter. Pour se mettre dans l'esprit de ZF, il faut oublier la description des ensembles tels des patates qui contiennent des points. Dans ZF, il n'y a pas de typage, il n'y a pas non plus de distinction entre ensemble et élément. Plus précisément dans ZF, tout est ensemble. En particulier, les éléments d'un ensemble sont encore des ensembles qui ont à leur tour des éléments qui sont encore des ensembles, etc. Ce point de vue a priori un peu barbare permet en fait d'écrire les choses de façon simple. Paradoxalement, la bonne façon de se représenter ces ensembles ne passe pas par des patates incluses les unes dans les autres, mais plutôt par une grosse patate que l'on appelle l'univers et dont les éléments sont précisément les ensembles, ces ensembles étant reliés par des flèches orientées qui indiquent l'appartenance. Informellement, l'univers représente l'ensemble de tous les ensembles mais celui-ci n'en est pas un au sens où il ne correspondra à aucun point dans la grosse patate.

Mais commençons tout de suite à dire les choses de façon plus précise.

### 2.1 Les axiomes de ZF

Un *modèle de ZF* ou encore un *univers* est un “ensemble” non vide (dans un sens intuitif) que l'on va appeler  $U$  muni d'une relation binaire vérifiant certains axiomes que l'on va lister. Rappelons dans un premier temps, qu'une relation binaire sur  $U$  est simplement une partie de  $U \times U$ , autrement dit pour tout couple  $(x, y)$  d'éléments de  $U$ , on est capable de dire si  $x$  est en relation avec  $y$ , ou si ce n'est pas le cas. Attention, l'ordre ici est important, la relation n'est pas du tout supposée symétrique. Une façon de représenter une relation binaire est de placer une flèche orientée entre  $x$  et  $y$  lorsqu'ils sont en relation dans cet ordre.

Les éléments de  $U$  vont être ce que l'on appelle les *ensembles* et le fait que  $x$  soit en relation avec  $y$  se notera “ $x \in y$ ” (lire  $x$  appartient à  $y$ ). Il faut faire attention au fait que le mot “ensemble” est à ce stade très ambigu. Par la suite, lorsque nous l'emploierons, il désignera toujours (sauf mention expresse du contraire) un élément de l'univers  $U$ .

Disons finalement que si  $A$  est un ensemble (donc un élément de  $U$ ), un élément de  $A$  sera simplement un ensemble  $x$  tel que  $x \in A$ . Il est temps maintenant de donner les axiomes que doit vérifier la relation d'appartenance donnée sur  $U$ .

On utilisera l'abréviation “ $A \subset B$ ” pour “ $\forall x(x \in A) \Rightarrow (x \in B)$ ”. On dira dans ce cas que  $A$  est un sous-ensemble (ou une partie) de  $B$ .

Remarquons aussi que par convention, tous les quantificateurs portent sur tous les ensembles. On utilisera aussi ce que l'on appelle des quantificateurs bornés, cela veut dire que l'on se permettra encore les abréviations suivantes :

$$\begin{aligned}\forall x \in A, [...] &\longrightarrow \forall x(x \in A) \Rightarrow [...] \\ \exists x \in A, [...] &\longrightarrow \exists x(x \in A) \text{ et } [...]\end{aligned}$$

1. *Axiome d'extensionnalité*

$$\forall A \forall B [(\forall x(x \in A) \Leftrightarrow (x \in B)) \Rightarrow A = B]$$

Il dit que si  $A$  et  $B$  sont deux ensembles ayant exactement les mêmes éléments, alors ils sont égaux. Ainsi pour définir un ensemble  $A$  il suffira de définir ses éléments.

2. *Axiome de la paire*

$$\forall x \forall y \exists A (\forall z(z \in A) \Leftrightarrow (z = x \text{ ou } z = y))$$

Il dit qu'étant donné deux ensembles  $x$  et  $y$ , il existe un ensemble  $A$  qui n'a pour éléments que  $x$  et  $y$ . Cet ensemble est unique par l'axiome d'extensionnalité et on le notera  $\{x, y\}$ .

3. *Axiome de l'union*

$$\forall I \exists A (\forall z(z \in A) \Leftrightarrow (\exists y \in I, z \in y))$$

Cela veut dire que les éléments de  $A$  sont exactement les éléments des éléments de  $I$ . Encore une fois un tel ensemble est unique, on le notera  $\cup I$  (lire *union* de  $I$ ). Cela correspond informellement à une union indexée par l'ensemble d'indices  $I$ , les ensembles que l'on réunit étant précisément les éléments de  $I$ .

4. *Axiome des parties*

$$\forall A \exists B (\forall X(X \in B) \Leftrightarrow (X \subset A))$$

L'ensemble  $B$  est unique, il s'agit de l'ensemble des parties de  $A$ , que l'on note  $\mathcal{P}(A)$ .

5. *Schéma d'axiomes de compréhension*

Un schéma d'axiomes regroupe en général une infinité d'axiomes indexée par les formules logiques. Plus précisément il dit que pour toute formule  $F$  on a un certain axiome. Le schéma de compréhension permet de parler de sous-ensembles, il est décrit par :

$$\forall u_1 \dots \forall u_n \forall X \exists Y (\forall x(x \in Y) \Rightarrow ((x \in X) \text{ et } (F(x, u_1, \dots, u_n))))$$

où  $F$  est une formule quelconque à  $(n+1)$  variables libres, c'est-à-dire dans laquelle on peut substituer  $(n+1)$  variables, ici en l'occurrence  $x, u_1, \dots, u_n$ . Le schéma de compréhension dit quels sous-ensembles de  $X$  doivent exister, il s'agit de ceux qui sont définissables par une formule. Les autres ont le droit d'exister mais on ne leur impose pas. C'est le maximum que l'on peut imposer étant donné que l'on aimerait au moins que les axiomes soient décrits par des formules logiques.

Ce schéma implique en particulier l'existence d'un ensemble n'ayant aucun élément. En effet, prenons  $X$  un ensemble quelconque de l'univers (qui existe puisque  $U$  est non vide) alors l'ensemble  $Y$  défini par :

$$\forall x(x \in Y) \Leftrightarrow ((x \in X) \text{ et } x \neq x)$$

existe justement par l'axiome de compréhension et est vide. Un tel ensemble est unique par extensionnalité, on le notera  $\emptyset$  par la suite.

Ce schéma permet aussi de définir l'intersection de deux ensembles, disons  $A$  et  $B$ . Il s'agit simplement de l'ensemble  $X$  défini par :

$$\forall z(z \in X) \Leftrightarrow ((z \in A) \text{ et } (z \in B))$$

(en le voyant ici comme un sous-ensemble de  $A$ ). Encore l'extensionnalité prouve l'unicité d'un tel ensemble, on le notera  $(A \cap B)$ .

#### 6. Schéma d'axiomes de remplacement

Les axiomes précédents ne permettent en fait pas de parler de tous les ensembles dont on aurait envie. Il faut encore ajouter la chose suivante. On dit que  $F(x, y, u_1, \dots, u_n)$  une formule à  $(n + 2)$  variables libres est une fonctionnelle en  $x$  et  $y$  si elle vérifie la condition suivante :

$$\forall x \forall y \forall y' \forall u_1 \dots \forall u_n (F(x, y, u_1, \dots, u_n) \text{ et } F(x, y', u_1, \dots, u_n)) \Rightarrow (y = y')$$

Cela veut exactement dire qu'étant donné  $x, u_1, \dots, u_n$ , il y a au plus un  $y$  qui vérifie  $F(x, y, u_1, \dots, u_n)$ . C'est moralement l'image de  $x$  par la fonctionnelle  $F$ .

Le schéma de remplacement dit que pour toute fonctionnelle  $F$ , si  $A$  est un ensemble, il en est de même de  $F(A)$  (avec des notations évidentes, je l'espère mais de toute façon l'axiome précis sera écrit plus bas), on aimerait donc indexer les axiomes par des fonctionnelles. Seulement cela n'est pas possible, car la propriété d'être une fonctionnelle dépend fortement de l'univers considéré et on aimerait que les axiomes n'en dépendent pas quand même. Pour pallier cela, on indexe en fait les axiomes par toutes les formules et on procède ainsi :

$$(F(x, y, u_1, \dots, u_n) \text{ fonctionnelle}) \Rightarrow [\forall u_1 \dots \forall u_n \forall A \exists B (\forall y (y \in B) \Rightarrow (\exists x \in A F(x, y, u_1, \dots, u_n)))]$$

L'ensemble  $B$  sera noté  $F(A)$ .

#### 7. Axiome de l'infini

Il est censé dire qu'il existe au moins un ensemble infini... on remarquera que toutes les constructions précédentes n'en ont pas encore fourni. Il y a plein de façons de le formuler, par exemple :

$$\exists X ((\exists x \in X) \text{ et } (\forall x \in X, x \cup \{x\} \in X))$$

où  $\{x\}$  est l'ensemble contenant uniquement  $x$ , il existe en vertu de l'axiome de la paire.

#### 8. Axiome de fondation

Il dit intuitivement que l'on ne peut pas trouver une suite infinie d'ensemble  $x_i$  "décroissante" pour l'appartenance... je veux dire par là qui vérifie  $x_{i+1} \in x_i$  pour tout entier  $i$ . Je vous laisse vous convaincre que cela revient exactement à dire que tout ensemble peut se construire seulement à partir de l'ensemble vide à l'aide des opérations précédentes. La façon la plus simple d'écrire cela sous forme d'un axiome est sans doute la suivante :

$$\forall x (x \neq \emptyset) \Rightarrow (\exists y \in x, (x \cap y) = \emptyset)$$

Il n'est pas si évident de montrer que cette condition simple équivaut aux énoncés plus intuitifs que l'on a donnés juste ci-dessus, nous ne le prouverons pas ici.

Voilà pour la liste. À ce niveau, il est peut-être légitime de se demander si un tel univers existe. On ne sait pas répondre à cette question, et même mieux, on peut montrer que l'on ne peut pas répondre à une formalisation dans cet univers de cette question... enfin bon, ce n'est pas le sujet. Pour plus d'informations, aller voir <http://www.eleves.ens.fr:8080/home/ollivier/goedel/goedel.html>

Il est sans doute amusant de remarquer que moyennant l'existence des entiers naturels, on peut construire un modèle de ZF auquel on a retiré l'axiome de l'infini. On laisse au lecteur le soin de vérifier que si l'on met sur  $\mathbb{N}$  la relation suivante ( $x$  et  $y$  donc sont deux entiers) :

$$x \in y \text{ ssi l'écriture binaire de } y \text{ contient un } 1 \text{ en } x\text{-ième position}$$

on obtient ce que l'on souhaite.

## 2.2 Constructions mathématiques usuelles

### 2.2.1 Ensembles "finis"

Si  $x$  et  $y$  sont deux ensembles, l'axiome de la paire assure l'existence d'un ensemble dont les seuls éléments sont  $x$  et  $y$ , que l'on a pris soin de noter  $\{x, y\}$ . En fait, étant donné des ensembles  $x_1, \dots, x_n$ , on peut montrer l'existence d'un ensemble ne contenant que  $x_1, \dots, x_n$  que l'on va bien entendu noter  $\{x_1, \dots, x_n\}$ .

On montre bien entendu cela par récurrence. Pour  $n = 1$  et  $n = 2$ , c'est déjà fait. Supposons donc que  $n \geq 2$ . On note alors  $X = \{x_1, \dots, x_{n-1}\}$  et  $Y = \{x_n\}$  dont l'hypothèse de récurrence assure l'existence. On appelle maintenant  $I = \{X, Y\}$ . La réunion de  $I$ ,  $\cup I$ , est alors précisément l'ensemble  $\{x_1, \dots, x_n\}$  que l'on cherchait à construire.

### 2.2.2 Couples, triplets, $n$ -uplets

On définit le *couple*  $(x, y)$ , noté donc " $(x, y)$ ", comme l'ensemble  $\{\{x\}, \{x, y\}\}$ . C'est un petit jeu laissé au lecteur de démontrer que  $(x, y) = (x', y')$  si et seulement si  $x = x'$  et  $y = y'$ .

On définit ensuite les  *$n$ -uplets* par récurrence sur  $n$ , il y a plein de définitions possibles, par exemple  $(x_1, \dots, x_n) = ((x_1, \dots, x_{n-1}), x_n)$

Il n'est pas possible de prendre  $(x, y, z) = \{\{x\}, \{x, y\}, \{x, y, z\}\}$  par exemple. En effet, dans ce cas les triplets  $(a, b, b)$  et  $(a, b, a)$  seraient égaux, ce qui est indésirable.

Si  $A$  et  $B$  sont deux ensembles, on notera pas la suite  $A \cup B$  la réunion de la paire  $I = \{A, B\}$ .

### 2.2.3 Produits "finis"

Commençons par le produit de deux ensembles, disons  $X$  et  $Y$ . On aimerait définir le produit  $X \times Y$  comme l'ensemble dont les éléments sont précisément les couples  $(x, y)$  où  $x$  est un élément de  $X$ , et  $y$  un élément de  $Y$ . Il reste juste à voir que cet ensemble existe effectivement. Une méthode générale pour ça est de voir l'ensemble en question comme un sous-ensemble *définissable* (ie dont les éléments sont caractérisés par une formule) d'un certain ensemble dont on connaît par ailleurs l'existence. Ici par exemple, il suffit de remarquer qu'un couple  $(x, y)$  est, tel qu'on vient de le définir, un élément de l'ensemble  $\mathcal{P}(\mathcal{P}(X \cup Y))$  et donc que le produit  $X \times Y$  est naturellement inclus dans  $\mathcal{P}(\mathcal{P}(X \cup Y))$ . Maintenant il ne reste plus qu'à écrire une formule qui identifie ces couples à l'intérieur de cet ensemble. C'est un peu laborieux mais pas difficile et nous laissons le lecteur sceptique le faire par lui-même.

Maintenant si  $X_1, \dots, X_n$  sont des ensembles, on définit le produit  $X_1 \times \dots \times X_n$  encore par récurrence via la formule

$$X_1 \times \dots \times X_n = (X_1 \times \dots \times X_{n-1}) \times X_n$$

On vérifie alors que ses éléments sont exactement les  $n$ -uplets  $(x_1, \dots, x_n)$  où  $x_i$  est un élément de  $X_i$  pour tout  $i$  compris entre 1 et  $n$ .

## 2.2.4 Relations

Soit  $E$  un ensemble. Une relation sur  $E$  est par définition un ensemble  $R$  inclus dans le produit  $E \times E$ . Bien entendu, on dira que  $x$  est en relation avec  $y$  si et seulement si le couple  $(x, y)$  appartient à  $R$ . Il est bien sûr possible de définir l'ensemble des relations sur  $E$ , il s'agit tout simplement de l'ensemble  $\mathcal{P}(E \times E)$ .

Bien entendu, on peut définir les relations réflexives, symétriques, anti-symétriques, transitives par les axiomes habituels. En particulier, on peut sans problème parler de relation d'ordre, de relation d'ordre total, de relation de bon ordre, de relation d'équivalence, etc. On peut même, étant donné un ensemble  $E$ , parler de l'ensemble des relations d'ordre sur  $E$ , des relations d'ordre total sur  $E$ , des relations de bon ordre sur  $E$ , des relations d'équivalence sur  $E$ ... cela se définissant par des formules, certes longues à écrire mais qui existent bien.

Si  $E$  est un ensemble et  $R$  une relation d'équivalence sur  $E$ , on peut définir l'ensemble quotient  $E/R$ . Pour cela, il faut d'abord donner une formule explicite qui dit qu'une partie  $A$  de  $E$  est une classe d'équivalence pour  $R$ . On peut par exemple prendre :

$$\exists x \in A, \forall y \in E, (y \in A) \Leftrightarrow ((x, y) \in R)$$

L'ensemble  $E/R$  est alors le sous-ensemble de  $\mathcal{P}(E)$  formé des éléments qui sont des classes d'équivalence pour la relation  $R$ . L'axiome de compréhension assure son existence.

## 2.2.5 Fonctions

Une fonction  $f$  est par définition un ensemble dont les éléments sont des couples, c'est-à-dire des ensembles de la forme  $\{\{x\}, \{x, y\}\}$ , qui vérifie de surcroît :

$$(\forall x \forall y \forall y' ((x, y) \in f \text{ et } (x, y') \in f) \Rightarrow (y = y'))$$

Étant donnée une fonction  $f$ , on peut définir son domaine et son image. Un ensemble  $x$  est dans le domaine de  $f$  s'il existe un ensemble  $y$  tel que  $(x, y) \in f$ . Le fait que le domaine de  $f$  soit un ensemble peut se voir avec l'axiome de remplacement (mais ce n'est pas nécessaire). Voyons comment cela fonctionne. On définit la fonctionnelle  $P_1(X, x)$  suivante :

$$\exists y, X = (x, y)$$

Cette fonctionnelle n'est définie que sur les couples et pour ceux-ci est simplement la première projection. L'image par  $P_1$  de l'ensemble  $f$  est alors précisément le domaine de  $f$ .

L'image de  $f$  est bien ce que l'on pense. Il s'agit de l'ensemble des  $y$  tels qu'il existe  $x$  vérifiant  $(x, y) \in f$ . On utilise l'axiome de remplacement avec ce coup-ci la deuxième projection pour voir qu'il s'agit bien d'un ensemble.

Les notations traditionnelles sont  $\text{Dom}(f)$  pour le domaine de la fonction  $f$  et  $\text{Im}(f)$  pour l'image de  $f$ .

Il faut préciser qu'il n'existe pas d'ensemble dont les éléments soient précisément les fonctions. Par contre si  $E$  et  $F$  sont deux ensembles, on définit une fonction de  $E$  dans  $F$  comme étant une fonction  $f$  de domaine  $E$  et d'image incluse dans  $F$  ( $f$  est donc en particulier inclus dans  $E \times F$ ). L'axiome de compréhension prouve que les fonctions de  $E$  dans  $F$  forment bien un ensemble (puisque'il est inclus dans  $\mathcal{P}(E \times F)$ ) que l'on note souvent  $F^E$  ou encore  $\text{Fonc}(E, F)$ . Remarquons qu'une fois précisés les ensembles

de départ et d'arrivée, il est possible de définir une injection, une surjection et une bijection par les axiomes habituels. Une *injection*  $f : E \rightarrow F$  est une fonction de  $E$  dans  $F$  vérifiant :

$$\forall x \in E, \forall x' \in E, (\exists y \in F, (x, y) \in f \text{ et } (x', y) \in f) \Rightarrow (x = x')$$

Une *surjection*  $f : E \rightarrow F$  est une fonction de  $E$  dans  $F$  vérifiant :

$$\forall y \in F, \exists x \in E, (x, y) \in f$$

Une *bijection*  $f : E \rightarrow F$  est une fonction de  $E$  dans  $F$  qui est à la fois une injection et une surjection.

Remarquons qu'une fonction  $f$  est toujours une fonction de  $\text{Dom}(f)$  dans  $\text{Im}(f)$ . Remarquons également que l'ensemble  $\text{Fonc}(\emptyset, F)$  est toujours réduit à un unique élément, qui est précisément l'ensemble vide, l'ensemble  $\text{Fonc}(E, \emptyset)$  quant à lui est vide dès que  $E$  est non vide.

Il s'agit de dire finalement que par la suite les termes "fonction", "injection", "surjection" et "bijection" désigneront toujours les objets précis que l'on vient de définir. Cela est très important pour la bonne compréhension de l'axiome du choix.

### 2.2.6 Produits quelconques

On aimerait définir le produit d'une famille quelconque d'ensembles. Mais avant de faire cela, il s'agit d'abord de dire ce que c'est une famille quelconque d'ensembles. Pour cela, on considère un certain ensemble  $I$  que l'on appelle ensemble d'indices et on définit une famille d'ensembles indexée par  $I$ . C'est simplement une fonction (au sens précédent donc) de domaine  $I$ . Une famille quelconque d'ensembles sera alors une famille d'ensembles indexée par un certain ensemble.

Remarquez qu'il n'est pas clair qu'il existe un ensemble ayant exactement pour éléments les familles indexées par l'ensemble  $I$ . En effet, ici on ne peut pas a priori borner ces éléments (c'est-à-dire tous les mettre dans un gros ensemble) et donc le fait que l'on dispose d'une jolie formule ne permet pas de conclure. De fait, il est faux de façon générale qu'un tel ensemble existe. Un exercice éducatif est sans doute de démontrer que cet ensemble existe si et seulement si  $I$  est vide.

Soit donc  $F = (X_i)$  une famille d'ensembles indexée par l'ensemble  $I$ . Il existe un ensemble dont les éléments sont exactement les  $X_i$ , il s'agit par définition de l'image de  $F$ . La réunion de cet ensemble fournit ce que l'on appelle habituellement la réunion des  $X_i$  pour  $i$  parcourant  $I$ . Notons-la par exemple  $X$ . Un élément du produit des  $X_i$  est alors une fonction  $x$  de  $I$  dans  $X$  telle que l'image de l'élément  $i$  de  $I$  appartienne à l'ensemble  $X_i$ . Formellement  $x$  est un élément du produit des  $X_i$  si :

$$x \in \text{Fonc}(I, X) \quad \text{et} \quad \forall i \forall y \forall Y ((i, y) \in x \text{ et } (i, Y) \in F) \Rightarrow (y \in Y)$$

On voit alors directement que l'axiome de compréhension permet de définir le produit des  $X_i$ .

### 2.2.7 Les nombres

Toutes les constructions données précédemment permettent de construire dans un univers  $U$  la plupart des objets que l'on utilise couramment en mathématiques. Enfin, presque... la construction de l'ensemble des entiers naturels  $\mathbb{N}$  muni des opérations classiques ne se déduit pas directement de tout cela. Admettons pour l'instant son existence, nous en donnerons une construction plus tard.

Une fois que l'on a  $\mathbb{N}$ , il n'est pas bien difficile par exemple de construire  $\mathbb{Z}$ . On met sur l'ensemble  $\mathbb{N} \times \mathbb{N}$  la relation d'équivalence suivante :



$$(x, y) R (x', y') \quad \text{ssi} \quad x + y' = x' + y$$

(où bien sûr,  $x + y$  désigne l'image par la fonction  $+$  qui va de  $\mathbb{N} \times \mathbb{N}$  dans  $\mathbb{N}$  du couple  $(x, y)$ )

Le quotient de  $\mathbb{N} \times \mathbb{N}$  par cette relation d'équivalence fournit précisément  $\mathbb{Z}$ . Il s'agit alors de prolonger les opérations. On définit pour cela le sous-ensemble  $+$  de  $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  en disant qu'un triplet  $(A, B, C)$  est dans  $+$  si et seulement si :

$$\exists(a_1, a_2) \in A, \exists(b_1, b_2) \in B, \exists(c_1, c_2) \in C, a_1 + b_1 + c_2 = a_2 + b_2 + c_1$$

(là encore, il y a beaucoup d'abus d'écriture, nous laissons au lecteur le soin d'écrire cette formule aussi rigoureusement que possible...)

Pour la multiplication on procède de même.  $\times$  est le sous-ensemble de  $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  formé des triplets  $(X, Y, Z)$  vérifiant :

$$\exists(a_1, a_2) \in A, \exists(b_1, b_2) \in B, \exists(c_1, c_2) \in C, a_1 \times b_1 + a_2 \times b_2 + c_2 = a_1 \times b_2 + a_2 \times b_1 + c_1$$

Il faut ensuite vérifier que  $+$  et  $\times$  ainsi définies sont bien des fonctions de  $\mathbb{Z} \times \mathbb{Z}$  dans  $\mathbb{Z}$ , ce qui se fait sans difficulté particulière.

Maintenant on peut construire  $\mathbb{Q}$  en mettant à nouveau la bonne relation d'équivalence sur  $\mathbb{Z} \times \mathbb{Z}$ . On peut également construire  $\mathbb{R}$ , en prenant l'ensemble des suites à valeurs rationnelles (ie des fonctions de  $\mathbb{N}$  dans  $\mathbb{Q}$ ) qui sont de Cauchy, et en quotientant cet ensemble par la relation d'équivalence qui dit deux suites sont équivalentes si et seulement si leur différence tend vers 0. Là encore, il faut prolonger les opérations, mais ces constructions ne requièrent pas plus d'astuce du côté théorie des ensembles que celle détaillée précédemment.

## 2.3 Et les démonstrations dans tout ça

Avant d'entrer dans le vif du sujet, il nous faut faire une dernière précision. En effet, dans la suite, nous allons parler d'axiome du choix, d'axiome du choix dénombrable, d'axiome du choix dépendant, etc. et nous allons nous demander lorsqu'un tel énoncé l'"utilise", mais nous n'avons pas encore défini ce que cela pouvait bien vouloir dire formellement.

Prenons donc un certain énoncé, qui s'exprime sous la forme d'une formule  $F$ . Dire que  $F$  est démontrable (ou encore prouvable) dans ZF signifie que la formule  $F$  est vérifiée dans tous les modèles de ZF. Comme on l'a dit, on ne sait pas construire un modèle de ZF, on ne sait même pas s'il en existe un. Il se pourrait donc que tous les énoncés soient démontrables dans ZF. Et effectivement... personne n'a encore trouvé de contradiction interne dans les axiomes que l'on a listés précédemment mais personne non plus ne peut prouver qu'il n'y en a pas. Il faut donc faire avec et par la suite, on supposera toujours implicitement qu'il existe au moins un modèle de ZF.

Voyons brièvement comment on peut voir qu'un énoncé est ou n'est pas démontrable. Pour prouver qu'il est démontrable comme on vient de le dire, il "suffit" de montrer qu'il est vrai dans tous les modèles de ZF, en gros il "suffit" de triturer les axiomes que l'on a pour en sortir le théorème que l'on veut. Il existe une définition précise de ce "triturer" pour laquelle la phrase qui précède est vraie, mais nous n'allons pas entrer plus en avant dans les détails, cela n'étant pas notre sujet. Signalons toutefois que le théorème cité précédemment est ce que l'on appelle classiquement le théorème de complétude de Gödel.

Mais comment faire pour voir qu'un énoncé n'est pas démontrable? Ben, il s'agit de construire un modèle de ZF dans lequel cet énoncé est faux. Ouille, construire un modèle de ZF, c'est difficile, on a

déjà dit que l'on ne savait pas faire. Oui, mais on a dit aussi que l'on allait sans vergogne supposer qu'il en existe un. Ainsi les méthodes classiques pour ce faire consistent à construire plus ou moins explicitement à partir d'un modèle donné, un nouveau modèle dans lequel l'énoncé en question est faux. Ce n'est pas quelque chose de facile. Une méthode générale pour construire ces modèles est ce que l'on appelle le "forcing". Nous n'allons là encore pas détailler davantage. Pour plus d'informations, aller voir <http://www-math.mit.edu/~tchow/mathstuff/forcingdum> (en anglais).

Bien sûr, il y a des cas où prouver qu'une formule  $F$  n'est pas démontrable dans ZF est plus simple. Par exemple, mais c'est un peu de la triche, si la formule (non  $F$ ) est démontrable,  $F$  ne va pas l'être. En effet, si on prend un modèle quelconque de ZF (dont on rappelle que l'on suppose l'existence), la formule  $F$  va y être vérifiée et donc (non  $F$ ) ne le sera pas. Une autre façon qui porte ses fruits est de prouver dans ZF que  $F$  implique une formule  $G$  que l'on sait par ailleurs ne pas être démontrable.

Un peu de terminologie peut-être. Si la formule (non  $F$ ) est démontrable, on dit que  $F$  est réfutable. Si  $F$  n'est ni démontrable, ni réfutable, on dit que  $F$  est indécidable.

Bien entendu, on a expliqué ici les choses avec les axiomes de ZF, mais tout ce que l'on vient de dire s'étend sans problème à tout système d'axiomes cohérent (c'est-à-dire pour lequel il existe un modèle...). Par la suite, on va énoncer l'axiome du choix et dire qu'il est indécidable (au sens précédent donc) dans ZF. Ainsi la théorie formée des axiomes de ZF auxquels on ajoute l'axiome du choix, que l'on note ZFC, est encore cohérente. Dire qu'un énoncé  $F$  "utilise" l'axiome du choix, c'est précisément dire que celui-ci est prouvable dans ZFC mais ne l'est pas dans ZF. Ainsi, en général, prouver effectivement qu'un énoncé "utilise" l'axiome du choix n'est pas quelque chose de facile, alors que prouver qu'il ne l'"utilise" pas est quand même relativement plus simple.

## 3 Axiome du choix

### 3.1 Énoncé

Ne perdons plus de temps et énonçons enfin cet axiome. Il dit que pour tout ensemble  $E$ , il existe une fonction  $f$  de  $\mathcal{P}(E) \setminus \{\emptyset\}$  dans  $E$  qui soit telle que pour toute partie  $A$  non vide de  $E$ ,  $f(A)$  appartient à  $A$ . De façon plus formelle, cela s'écrit :

$$\forall E \exists f (f \text{ fonction de } \mathcal{P}(E) \setminus \{\emptyset\} \text{ dans } E) \text{ et } (\forall A \in \mathcal{P}(E) \setminus \{\emptyset\}, (A, a) \in f \Rightarrow a \in A)$$

Une fonction  $f$  qui vérifie cette propriété s'appelle une *fonction de choix* sur  $E$ . L'axiome du choix dit exactement que tout ensemble admet une fonction de choix.

De façon équivalente et plus compacte, il dit qu'un produit non vide (ie indexé par un ensemble non vide) d'ensembles non vides est non vide. Cette formulation est un peu plus dangereuse dans le sens où il faut bien garder à l'esprit que le mot "produit" a le sens précis que l'on a introduit dans la première partie. De nombreuses confusions proviennent surtout de cela. (Pour les algébristes convaincus, cela peut se reformuler en disant que toute surjection ensembliste est scindée, c'est-à-dire que si  $p : A \rightarrow B$  est une application surjective, alors il existe une application  $s : B \rightarrow A$ , que l'on appelle une section, vérifiant  $p \circ s = \text{id}_B$ ).

Il n'est peut-être pas clair a priori que ces deux énoncés sont bien équivalents. Démontrons cela. Supposons dans un premier temps le premier énoncé. Il s'agit de montrer que si  $I$  est un ensemble non vide et  $F = (X_i)$  une famille d'ensembles non vides indexée par  $I$ , alors on peut exhiber une fonction de  $I$  dans l'union des  $X_i$ , telle que  $f(i)$  soit dans  $X_i$  pour tout  $i$ . Pour faire cela, on considère une fonction de choix,

disons  $g$ , sur l'union des  $X_i$ . Il ne reste plus alors qu'à définir  $f(i)$  comme étant  $g(X_i)$ . Réciproquement, prenons  $E$  un ensemble quelconque et montrons que le deuxième énoncé assure l'existence d'une fonction de choix sur  $E$ . On considère pour cela comme ensemble d'indices l'ensemble  $\mathcal{P}(E) \setminus \{\emptyset\}$ . La famille indexée par cet ensemble sera également  $\mathcal{P}(E) \setminus \{\emptyset\}$ . On laisse au lecteur le soin de se persuader qu'un élément du produit de cette famille correspond précisément à une fonction de choix sur  $E$ .

Il est bon de dire tout de suite que l'axiome du choix n'est pas une conséquence formelle des autres axiomes de ZF. La négation de l'axiome du choix, non plus. Autrement dit, l'axiome du choix est indécidable dans ZF. La théorie constituée des axiomes de ZF et de l'axiome du choix est donc cohérente, c'est elle que l'on appelle ZFC (C pour "Choice").

### 3.2 Commentaires

L'axiome du choix est souvent sur-interprété ou mal interprété. Essayons de mettre les choses au clair en détaillant quelques exemples. Donnons-nous pour commencer un singleton  $I$  et une famille  $(X_i)$  indexée par  $I$ , c'est-à-dire en fait simplement un ensemble  $X$ . On suppose  $X$  non vide. Le produit des  $X_i$  s'identifie alors à  $X$  et est non vide puisque nous venons de le supposer. Tout ça pour dire que l'on n'a pas besoin de l'axiome du choix pour choisir un élément dans un ensemble.

Par récurrence, on peut montrer que même que si  $I$  est fini, exhiber un élément du produit est possible. Dit en termes plus concrets, on n'utilise pas l'axiome du choix pour choisir simultanément un élément dans un nombre fini d'ensembles.

Attention par contre, si ce sont les  $X_i$  (ie les ensembles dans lesquels on va choisir les éléments) qui sont des ensembles finis mais que  $I$  ne l'est pas, la construction par récurrence a priori ne marche plus. Et en fait cet énoncé plus faible où l'on suppose les ensembles  $X_i$  finis n'est pas non plus démontrable dans ZF même si  $I$  est l'ensemble des entiers naturels.

Mais à côté de cela, il est des cas où l'axiome du choix n'est pas nécessaire pour construire une telle fonction. Supposons par exemple que l'on veuille construire une fonction de choix sur l'ensemble des entiers naturels  $\mathbb{N}$ . Il est vrai que l'on n'a toujours pas construit cet ensemble (mais il est vrai aussi que cela viendra plus tard :-)) mais supposons pour l'instant qu'il existe et qu'il est muni des opérations usuelles et de la relation d'ordre usuelle. C'est cette dernière qui va nous être utile. En effet, elle a la particularité remarquable que toute partie non vide de  $\mathbb{N}$  admet pour cette relation d'ordre un plus petit élément. Ainsi l'idée vient de considérer la fonction  $f$  qui à une partie non vide de  $\mathbb{N}$  associe son plus petit élément qui sera bien une fonction de choix. Voyons pour une fois que cela est bien possible, c'est-à-dire qu'il existe bien un ensemble  $f$  qui correspond à une telle fonction. Il est défini par la formule :

$$f \subset (\mathcal{P}(\mathbb{N}) - \{\emptyset\}) \times \mathbb{N} \quad \text{et} \quad (X, x) \in f \Rightarrow (x \in X \text{ et } \forall y \in X, x \leq y)$$

Le schéma de compréhension, finalement, assure bien l'existence d'un tel ensemble  $f$ .

De façon très informelle et imagée, on peut dire que choisir une chaussette par paire parmi une infinité de paires en vrac dans une bassine requiert l'axiome du choix, alors que ce n'est pas le cas pour les chaussures car il suffit par exemple de prendre toutes les chaussures gauches.

### 3.3 Axiome du choix dénombrable, axiome du choix dépendant

Avant de dire ce que sont ces axiomes, il est peut-être nécessaire de faire le point sur la notion de dénombrabilité. Soit  $X$  un ensemble. On dit que  $X$  est dénombrable s'il peut être mis en bijection avec  $\mathbb{N}$ . Mais là, encore "bijection" est à prendre dans le sens défini dans la première partie et  $\mathbb{N}$  désigne encore

l'ensemble des entiers naturels qu'effectivement nous n'avons toujours pas construit mais ça viendra... Attention, cela ne veut pas du tout dire que la sous-patate de l'univers regroupant tous les ensembles éléments de  $X$  est "dénombrable". Aussi étonnant que cela puisse paraître, il existe des univers qui comptent un nombre "dénombrable" d'ensembles (bien entendu toujours sous l'hypothèse qu'il existe au moins un modèle de ZF) et pourtant on peut montrer que l'ensemble des réels n'est jamais dénombrable.

Maintenant cette mise au point faite, on peut énoncer l'axiome du choix dénombrable. On le note souvent CC pour "Countable Choice". Il dit qu'un produit dénombrable d'ensembles non vides est non vide. Cela signifie que si  $I$  est un ensemble dénombrable, si  $(X_i)$  est une famille d'ensembles non vides indexée par  $I$ , alors le produit des  $X_i$  est non vide. Il est important de bien remarquer que la condition de dénombrabilité porte sur l'ensemble d'indices  $I$  et non sur les ensembles indexés. Comme être dénombrable signifie être en bijection avec  $\mathbb{N}$ , ce dernier énoncé peut se reformuler en disant que toute famille  $(X_n)$  d'ensembles non vides indexée par  $\mathbb{N}$  est telle que le produit des  $X_n$  est non vide.

L'axiome du choix dépendant, que l'on note souvent DC pour "Dependent Choice", lui, dit quelque chose de plus fort. On part d'un ensemble  $E$  que l'on suppose simplement non vide. On se donne en outre une fonction  $f : E \rightarrow \mathcal{P}(E) \setminus \{\emptyset\}$  quelconque. L'axiome du choix dépendant dit alors que pour tout  $x$  de  $E$ , il existe une suite  $(x_n)$  d'éléments de  $E$  telle que

1.  $x_0 = x$
2.  $x_{n+1} \in f(x_n)$

Il est peut-être nécessaire de préciser ce que l'on entend par "suite" : là encore, il y a une définition formelle. Une suite à valeurs dans  $E$  est simplement une fonction de  $\mathbb{N}$  (oui, oui, on ne l'a toujours pas construit, je sais :-)) dans  $E$ , fonction bien entendu au sens formel, celui dont on parle depuis le début. Ce que l'on note communément  $x_n$  est bien entendu l'image de  $n$ , élément de  $\mathbb{N}$ , par cette fonction.

Il s'agit sans doute de la forme de l'axiome du choix la plus couramment utilisée, du moins en analyse. C'est celle que l'on emploie par exemple typiquement pour construire une suite par récurrence.

Voyons les rapports qu'entretiennent tous ces axiomes. Déjà, il est clair que l'axiome du choix, dans sa deuxième formulation, implique l'axiome du choix dénombrable. Il est peut-être un peu moins clair que l'axiome du choix implique l'axiome du choix dépendant, et comme l'on n'a toujours pas défini ce qu'était  $\mathbb{N}$ , on aura du mal à démontrer quoi que ce soit en fait. Disons quand même plus ou moins informellement comment on fait les choses. On considère donc  $E$  un ensemble non vide et  $f$  une fonction de  $E$  dans  $\mathcal{P}(E) \setminus \{\emptyset\}$ . D'après l'axiome du choix justement il existe sur  $E$  une fonction de choix, disons  $g : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$ . Il suffit alors, étant donné un élément  $x$  de  $E$ , de construire la suite  $(x_n)$  de la façon suivante :

1.  $x_0 = x$
2.  $x_{n+1} = g(f(x_n))$

On verra en que cela définit bien une fonction de  $\mathbb{N}$  dans  $E$ .

Il est finalement vrai que l'axiome du choix dépendant implique l'axiome du choix dénombrable. Prenons donc une famille  $(X_n)$  d'ensembles non vides indexée par  $\mathbb{N}$ . Il s'agit de montrer que le produit des  $X_n$  est non vide. Pour cela, on commence par construire ce que l'on appelle l'union disjointe des  $X_n$ , que l'on va noter  $X$ . Il s'agit de l'ensemble des couples  $(n, x)$  où  $n$  est un entier naturel (ie un élément de  $\mathbb{N}$ ) et  $x$  un élément de  $X_n$ . Montrons tout d'abord que cet ensemble existe. Notons  $X'$  l'union des  $X_n$  que l'on a déjà considérée plusieurs fois. Bien entendu, on va voir  $X$  comme une partie de  $\mathbb{N} \times X'$ , elle est définie par la formule  $(n, x) \in X \Rightarrow x \in X_n$ . L'axiome de compréhension prouve donc que l'union disjointe existe.

Il nous faut maintenant définir une fonction  $f : X \rightarrow \mathcal{P}(X) \setminus \{\emptyset\}$ . On prend celle qui au couple  $(n, x)$  associe  $\{n + 1\} \times X_{n+1}$  qui est bien une partie non vide de  $X$ . (Le lecteur encore sceptique pourra s'amuser à écrire lui-même une formule et se convaincre qu'une telle fonction existe encore grâce à l'axiome de compréhension). Il ne reste alors plus qu'à prendre un élément  $x$  dans  $X_0$  et à appliquer l'axiome du choix dépendant au couple  $(0, x_0)$  élément de  $X$ . Il faut encore construire un élément du produit des  $X_n$  à partir de la suite obtenue mais cela se fait sans difficulté.

Finalement on a :

$$\text{Axiome du choix} \Rightarrow \text{Axiome du choix dépendant} \Rightarrow \text{Axiome du choix dénombrable}$$

Il est à noter que toutes les réciproques sont fausses, dans le sens où, comme nous l'avons déjà expliqué, il existe un modèle de ZF vérifiant l'axiome du choix dépendant mais pas l'axiome du choix, et un modèle de ZF vérifiant l'axiome du choix dénombrable mais pas l'axiome du choix dépendant. Construire de tels modèles n'est pas quelque chose de facile, et nous n'allons pas le faire.

### 3.4 Énoncés équivalents classiques

Il est peut-être nécessaire au préalable de faire quelques rappels sur les notions d'ordre. Prenons donc  $E$  un ensemble muni d'une relation binaire que l'on va noter  $\leq$ . On dit que cette relation est un *ordre* si elle vérifie les trois propriétés suivantes :

1. (*réflexivité*)  $\forall x \in E, x \leq x$
2. (*transitivité*)  $\forall x \in E, \forall y \in E, \forall z \in E, (x \leq y \text{ et } y \leq z) \Rightarrow (x \leq z)$
3. (*antisymétrie*)  $\forall x \in E, \forall y \in E, (x \leq y \text{ et } y \leq x) \Rightarrow (x = y)$

Une relation sur  $E$  qui vérifie juste les deux premières conditions est ce que l'on appelle un *pré-ordre*.

On dit que l'ordre est *total*, ou encore que  $E$  est *totalement ordonné*, si la relation  $\leq$  vérifie en outre la condition :

4.  $\forall x \in E, \forall y \in E, (x \leq y \text{ ou } y \leq x)$

On dira souvent de  $E$  qu'il est un ensemble *partiellement ordonné* s'il est juste muni d'une relation d'ordre. Le mot "partiellement" ne sous-entend aucunement que la relation d'ordre n'est pas totale, il est juste là pour préciser qu'elle ne l'est pas forcément.

Prenons donc  $E$  un ensemble partiellement ordonné. Ce que l'on appelle un *plus grand élément* de  $E$ , c'est un élément  $x$  de  $E$  plus grand que tous les autres, c'est-à-dire vérifiant  $y \leq x$  pour tout  $y$  dans  $E$ . La propriété d'antisymétrie prouve directement que s'il existe un plus grand élément, alors celui-ci est unique.

Il est important de ne pas confondre cette notion avec la notion d'élément maximal. Un *élément maximal* de  $E$ , c'est un élément  $x$  de  $E$  tel qu'il n'existe pas de  $y$  strictement supérieur (ie supérieur et différent) à  $x$ . Pour illustrer la distinction, il est intéressant de remarquer que si  $E$  est un ensemble muni de la relation "égalité" (ie  $x \leq y$  si et seulement si  $x = y$ ) qui est une relation d'ordre, alors tout élément de  $E$  est un élément maximal mais  $E$  n'admet pas de plus grand élément dès qu'il est de cardinal plus grand que 2. Il est intéressant aussi de remarquer que cet exemple prouve qu'un élément maximal n'est pas du tout forcément unique.

Il est cependant vrai que si  $E$  est *totalement ordonné*, alors un élément maximal est forcément unique et que les notions d'élément maximal et de plus grand élément coïncident. Il est également vrai que si

$E$  est un ensemble partiellement ordonné qui admet un plus grand élément  $x$ , alors il admet un unique élément maximal qui est précisément  $x$ .

Reprenons maintenant  $E$  un ensemble partiellement ordonné. Si  $A$  est une partie de  $E$ , la relation d'ordre,  $\leq$  disons, se restreint à  $A$  (formellement il s'agit de faire l'intersection de l'ensemble  $\leq$  avec l'ensemble  $A \times A$ ). On dit que  $A$  est *majoré* dans  $E$  s'il existe un élément  $x$  de  $E$  plus grand que tous les éléments de  $A$ , c'est-à-dire tel que  $y \leq x$  pour tout  $y$  dans  $A$ . On dit que  $A$  est une *chaîne* si l'ordre induit sur  $A$  est total. On dit que  $E$  est *inductif* si toute chaîne de  $E$  est majorée.

Finalement, on dit que  $E$  est *bien ordonné* si toute partie  $A$  non vide admet un plus petit élément (oui, je sais, je n'ai pas défini plus petit élément mais bon :-). Bien entendu, on peut donner encore plein de définitions et de propriétés intéressantes sur les ordres mais ici sont rassemblées celles qui vont nous servir par la suite.

Ouf. On est maintenant en mesure d'énoncer quelques équivalents de l'axiome du choix. Commençons par le théorème de maximalité de Hausdorff. Il dit la chose suivante. On prend  $E$  un ensemble partiellement ordonné. On peut regarder alors les sous-ensembles de  $\mathcal{P}(E)$  formé des chaînes. Cet ensemble est muni d'un ordre naturel, celui donné par l'inclusion. Le théorème de maximalité de Hausdorff dit que ce dernier ensemble muni de ce dernier ordre admet un élément maximal. On résume cela en général en disant que tout ensemble partiellement ordonné admet une chaîne "maximale".

Une autre formulation plus courante de cet énoncé est le lemme de Kuratowski-Zorn, sans doute plus connu sous le nom de lemme de Zorn. Il dit que tout ensemble partiellement ordonné inductif admet un élément maximal. Voyons peut-être rapidement le pourquoi de l'équivalence de ces deux énoncés.

Supposons dans un premier temps le théorème de maximalité de Hausdorff et prenons  $E$  un ensemble partiellement ordonné inductif. Il s'agit de prouver que  $E$  admet un élément maximal. On considère pour cela  $A$  un sous-ensemble de  $E$  qui est une chaîne maximale. Elle est majorée par hypothèse, notons  $x$  un majorant. S'il existait dans  $E$   $y$  strictement supérieur à  $x$ , alors l'ensemble  $A \cup \{y\}$  serait une chaîne de  $E$  contenant strictement  $A$ , ce qui est exclu. Cela prouve bien que  $x$  est un élément maximal de  $E$ .

Réciproquement, supposons le lemme de Zorn. Soit  $E$  un ensemble partiellement ordonné. On considère  $X$  le sous-ensemble de  $\mathcal{P}(E)$  formé des chaînes de  $E$  que l'on ordonne par inclusion. J'affirme que cet ensemble est inductif. En effet, étant donné une partie  $X'$  de  $X$  (bien réfléchir à ce dont il s'agit), il est immédiat de constater que la réunion de  $X'$  (qui est une partie de  $E$ ) majore  $X'$ . Le lemme de Zorn appliqué à  $X$  fournit précisément ce que l'on cherche.

Un autre énoncé est le théorème de Zermelo qui stipule que tout ensemble peut être muni d'un bon ordre. Précisément pour tout ensemble  $E$ , il existe une partie de  $E \times E$  qui est un bon ordre sur  $E$ . Celui-ci aussi est équivalent à l'axiome du choix.

Un dernier. L'axiome du choix est encore équivalent à ce que l'on appelle le lemme de trichotomie. Il dit que si  $X$  et  $Y$  sont deux ensembles quelconques, alors soit il existe une injection de  $X$  dans  $Y$ , soit il existe une injection de  $Y$  dans  $X$ . Pour une bonne définition de cardinal, il dit que les cardinaux sont totalement ordonnés.

Nous démontrerons au paragraphe 4.5 l'équivalence de toutes ces propriétés avec l'axiome du choix mais admettons-les pour le moment et voyons comment on les utilise.

### 3.5 Quelques exemples

Pour un nombre beaucoup plus impressionnant d'énoncés équivalents, plus faibles, plus forts, strictement plus faibles, strictement plus forts que l'axiome du choix, vous pouvez aller voir :

1. <http://www.eleves.ens.fr:8080/home/nesme/maths/choix.html>
2. [http://www.eleves.ens.fr:8080/home/madore/math/ac\\\_var.html](http://www.eleves.ens.fr:8080/home/madore/math/ac\_var.html)
3. <http://math.vanderbilt.edu/~schectex/coc/choice.html> (en anglais).

### 3.5.1 Existence de bases dans les espaces vectoriels

Prenons  $k$  un corps quelconque et  $E$  un espace vectoriel sur  $k$ . Le but est de montrer que  $E$  admet une base sur  $k$ . Pour cela, on considère l'ensemble  $F$  des familles libres d'éléments de  $E$ . On ordonne cet ensemble par inclusion. On obtient ainsi un ensemble partiellement ordonné inductif. En effet si  $F'$  est un sous-ensemble de  $F$  totalement ordonné, il n'est pas très difficile de voir que l'union de  $F'$  est encore une famille libre. Le lemme de Zorn s'applique donc et nous fournit ainsi une famille libre maximale. Montrer qu'il s'agit d'une base est encore un exercice simple que nous n'allons pas faire ici.

Évidemment, la démonstration que nous venons de présenter utilise l'axiome du choix, via justement le lemme de Zorn. Évidemment aussi, le fait de donner une démonstration qui utilise l'axiome du choix ne démontre aucunement que le résultat l'utilise. Ici, c'est le cas. On peut construire des modèles de ZF dans lesquels il existe un espace vectoriel qui n'admet pas de bases. On peut faire les choses un peu plus explicitement comme par exemple construire des modèles de ZF dans lesquels  $\mathbb{R}$  n'admet pas de base en tant que  $\mathbb{Q}$ -espace vectoriel, et même dans lesquels les seules endomorphismes  $\mathbb{Q}$ -linéaires de  $\mathbb{R}$  sont les multiplications par les éléments de  $\mathbb{R}$ .

### 3.5.2 Théorème de Tychonov

Ce paragraphe traite essentiellement de topologie générale. Comme l'objet de cet article n'est pas de parler de cela, nous n'allons pas rappeler les définitions usuelles. Ainsi, si vous n'avez jamais entendu les mots "quasi-compact" ou "ultrafiltre", vous pouvez passer directement à la section suivante.

Une application directe du lemme de Zorn est le fait que tout filtre se prolonge en un ultrafiltre. En effet étant donné un ensemble  $X$  et un filtre  $F$  sur  $X$ , il suffit de regarder l'ensemble des filtres  $F'$  prolongeant  $F$ . Il est alors facile de voir que cet ensemble est inductif. Le lemme de Zorn fournit alors l'existence d'un filtre maximal, ie d'un ultrafiltre, prolongeant  $F$ .

Utilisant la puissance des filtres et des ultrafiltres, il est facile de voir que :

1. un espace topologique est quasi-compact si et seulement si tout filtre admet une valeur d'adhérence si et seulement si tout ultrafiltre est convergent.
2. un ultrafiltre sur un produit est convergent si et seulement si chacune de ses projections l'est.

Il est alors facile d'en déduire qu'un produit d'espaces topologiques quasi-compacts est encore quasi-compact.

On présente plus souvent le théorème de Tychonov en disant qu'un produit quelconque d'espaces topologiques compacts est compact. Mais cette version se déduit directement de la précédente. Il est amusant de remarquer que la version avec "quasi-compact" est équivalente à l'axiome du choix alors que la version avec simplement "compact" est strictement plus faible mais nécessite quand même l'axiome du choix. Là encore, nous n'allons donner aucune démonstration.

### 3.5.3 Théorème de Cantor-Bernstein

Prenons  $A$  et  $B$  deux ensembles. Le théorème de Cantor-Bernstein dit que s'il existe une injection de  $A$  dans  $B$  et une injection de  $B$  dans  $A$ , alors il existe une bijection de  $A$  dans  $B$ .

Voyons comment on peut le démontrer. Tout d'abord notons  $B'$  l'image de  $B$  par l'injection de  $B$  dans  $A$ . C'est un sous-ensemble de  $A$  qui est en bijection avec  $B$  (justement par l'injection en question). Il s'agit donc simplement de construire une bijection de  $B'$  dans  $A$  sachant que l'on dispose d'une injection  $i : A \rightarrow B'$ . On commence pour cela par définir l'ensemble  $C = A - B'$  et on construit une suite (c'est-à-dire une fonction d'ensemble de départ  $\mathbb{N}$ , que l'on n'a toujours pas construit effectivement mais ça viendra :-)) de sous-ensembles de  $A$  par la formule de récurrence suivante :

1.  $C_0 = C$
2.  $C_{n+1} = i(C_n)$

( $i(C_n)$  est l'image de  $C_n$  par l'injection  $i$ , on laisse au lecteur le soin de montrer qu'il s'agit bien d'un ensemble)

Comme nous l'avons déjà utilisé mais toujours pas prouvé (voir 3.5.6), cette construction définit bien une suite.

On note finalement  $C_\infty$  la réunion des ensembles  $C_n$  (cela existe comme nous l'avons déjà mentionné). La bijection  $f : A \rightarrow B'$  se définit alors de manière simple :

1.  $f(x) = x$  si  $x$  n'est pas dans  $C_\infty$
2.  $f(x) = i(x)$  sinon

On laisse encore le lecteur avide de rigueur vérifier que cet ensemble existe bien (encore une fois via l'axiome de compréhension) et qu'il définit bien une bijection telle qu'on la voulait.

Il est important de remarquer que la démonstration précédente n'a pas fait intervenir l'axiome du choix. Ainsi le théorème de Cantor-Bernstein est vrai indépendamment de l'axiome du choix. Toutefois, souvent, il est commode d'utiliser certains de ses corollaires dans lesquels il intervient des surjections. Et le hic c'est que construire une injection à partir d'une surjection est quelque chose qui utilise l'axiome du choix. Je ne prétends rien démontrer mais moralement cela provient du fait que l'énoncé toute surjection ensembliste est "scindée" est équivalent à l'axiome du choix. Ainsi les deux énoncés suivants qui ressemblent beaucoup au théorème de Cantor-Bernstein, eux, utilisent l'axiome du choix :

1. Soient  $A$  et  $B$  deux ensembles tels qu'il existe une injection et une surjection de  $A$  dans  $B$ , alors il existe une bijection de  $A$  dans  $B$ .
2. Soient  $A$  et  $B$  deux ensembles tels qu'il existe une surjection de  $A$  dans  $B$  et une injection de  $B$  dans  $A$ , alors il existe une bijection de  $A$  dans  $B$ .

### 3.5.4 Dénombrabilité de $\mathbb{Q}$

À partir du théorème de Cantor-Bernstein, il est plus ou moins aisé de déduire la dénombrabilité de  $\mathbb{Q}$ . Ce que l'on a à construire, c'est une bijection entre  $\mathbb{N}$  et  $\mathbb{Q}$ . Il suffit donc pour cela de construire une injection de  $\mathbb{N}$  dans  $\mathbb{Q}$  et une injection de  $\mathbb{Q}$  dans  $\mathbb{N}$ . L'injection de  $\mathbb{N}$  dans  $\mathbb{Q}$  est déjà toute trouvée. Il ne reste donc plus que l'injection de  $\mathbb{Q}$  dans  $\mathbb{N}$ . Mais on se rappelle que construire une bijection entre  $\mathbb{N}$  et  $\mathbb{N}^2$  n'est pas quelque chose de monstrueusement difficile. Par exemple l'application  $(n, m) \mapsto (2n + 1) \cdot 2^m - 1$  convient. Il suffit donc finalement de trouver une injection de  $\mathbb{Q}$  dans  $\mathbb{N}^2$ . Mais cela est possible et pas très difficile. Je vous laisse écrire une formule explicite qui convient...

On remarque si l'on mène cette démonstration jusqu'à terme qu'en fait, elle n'utilise pas l'axiome du choix. Ainsi  $\mathbb{Q}$  est dénombrable même sans l'axiome du choix, ce qui est somme toute assez rassurant, et ce qui va nous permettre de faire plein d'autres choses aussi étrange que cela puisse paraître. Par exemple, voilà tout de suite une première application.



### 3.5.5 Produits d'ouverts dans $\mathbb{R}$

Soit  $I$  un ensemble et soit  $(U_i)$  une famille d'ouverts non vides de  $\mathbb{R}$  (bien entendu, celui que l'on a défini dans la première partie). On va prouver sans utiliser l'axiome du choix que le produit des  $U_i$  est non vide. Pour ce faire, il va falloir être capable de définir un élément particulier sans chacun des  $U_i$ . C'est là qu'intervient  $\mathbb{Q}$  ainsi que le fait qu'il soit dénombrable.

En effet fixons  $f$  une bijection entre  $\mathbb{Q}$  et  $\mathbb{N}$ . L'ordre naturel sur  $\mathbb{N}$  va se transporter via  $f$  en un certain ordre sur  $\mathbb{Q}$ . Ce nouvel ordre va rester un bon ordre, dans le sens où toute partie non vide de  $\mathbb{Q}$  va admettre pour cet ordre un plus petit élément. Ainsi  $\mathbb{Q}$  va admettre une fonction de choix : je parle ici de la fonction qui à une partie non vide de  $\mathbb{Q}$  associe justement ce plus petit élément. On a déjà plus ou moins vu que cette fonction existe bien. Voilà, un bon point.

Voyons maintenant comment cela permet de résoudre notre problème. Notons par exemple  $g$  la fonction de choix que l'on vient de définir. Le fait que les  $U_i$  soient des ouverts de  $\mathbb{R}$  prouve que ces  $U_i$  intersectent  $\mathbb{Q}$  puisqu'il est dense dans  $\mathbb{R}$ . Je dis alors qu'un élément du produit des  $U_i$  est par exemple la fonction  $x$  définie par  $x(i) = g(\mathbb{Q} \cap U_i)$ , comme il est facile de le vérifier.

Bien entendu, cet exemple peut se généraliser abondamment. Tout d'abord au cas de  $\mathbb{R}^n$ . Il s'agit d'abord de prouver que  $\mathbb{Q}^n$  est dénombrable mais cela se fait par récurrence. En effet, on commence par dire que, comme  $\mathbb{Q}$  est dénombrable,  $\mathbb{Q}^2$  est en bijection avec  $\mathbb{N}^2$  et est donc dénombrable. Ainsi  $\mathbb{Q}^3 = \mathbb{Q}^2 \times \mathbb{Q}$  est lui aussi en bijection avec  $\mathbb{N}^2$  et donc dénombrable, et ainsi de suite. Le même raisonnement que celui fait précédemment prouve illico que l'on n'a pas besoin de l'axiome du choix pour construire un élément du produit des  $U_i$  où les  $U_i$  forment une famille d'ouverts non vides de  $\mathbb{R}^n$  indexée par un ensemble  $I$ .

Le résultat important de ce paragraphe qu'il faut retenir, c'est qu'un ensemble dénombrable admet toujours une fonction de choix. Plus généralement tout ensemble qui admet un bon ordre admet également une fonction de choix. En fait, la réciproque est même vraie, c'est-à-dire qu'un ensemble admet une fonction de choix si et seulement s'il admet un bon ordre. Nous démontrerons ce résultat par la suite.

### 3.5.6 Constructions par récurrence

Avant de poursuivre, il devient nécessaire de faire un petit topo sur ce que l'on appelle les constructions par récurrence. Énonçons juste en fait un théorème qui va préciser tout cela.

Soient  $E$  un ensemble non vide et  $\varphi : \mathbb{N} \times E \rightarrow E$  une fonction. On se donne également  $x$  un élément de  $E$ . Alors il existe une fonction  $u : \mathbb{N} \rightarrow E$  telle que :

1.  $u(0) = x$
2.  $u(n+1) = \varphi(n, u(n))$

Autrement dit, il est possible de construire une fonction partant de  $\mathbb{N}$  par récurrence. Je vous conseille d'aller regarder à nouveau l'énoncé de l'axiome du choix dépendant et de vous persuader intimement qu'il ne s'agit pas du tout de la même chose.

Bien sûr étant donné que nous n'avons toujours pas défini  $\mathbb{N}$ , il ne nous est pour l'instant pas possible de prouver quoi que ce soit. Admettons cela momentanément, admettons aussi que ce résultat n'utilise pas l'axiome du choix, une preuve de tout cela sera plus ou moins fournie au paragraphe 4.3.

### 3.5.7 Théorème de Baire

Une autre application de la dénombrabilité est le fait que le théorème de Baire sur un espace métrique complet séparable n'utilise aucune forme de l'axiome du choix. La démonstration que l'on donne classiquement et qui marche sans hypothèse de séparabilité, elle, utilise l'axiome du choix dépendant. Nous allons simplement l'adapter un peu dans ce qui suit.

Rappelons peut-être avant de commencer la définition de "séparable" et l'énoncé du théorème de Baire. Un espace topologique  $X$  est dit *séparable* s'il existe une partie de  $X$  à la fois dense et dénombrable. Par exemple  $\mathbb{R}$  est séparable, et ce même sans l'axiome du choix, parce que l'on vient de voir de  $\mathbb{Q}$  est dénombrable et dense dans  $\mathbb{R}$ . De même  $\mathbb{R}^n$  est séparable.

Le théorème de Baire dit que si  $X$  est un espace métrique complet et si  $(U_n)$  est une famille d'ouverts denses indexée par  $\mathbb{N}$ , alors l'intersection des  $U_n$  est encore dense.

Montrons donc ce théorème sans utiliser l'axiome du choix. On part donc d'un espace métrique  $X$  que l'on suppose complet et séparable. On fixe  $A$  une partie dense et dénombrable de  $X$ . Comme  $A$  est dénombrable, il existe une fonction de choix sur  $A$ . Fixons-en une que l'on notera  $f$ . On considère en outre une famille  $(U_n)$  indexée par  $\mathbb{N}$  d'ouverts denses de  $X$ . Il s'agit de montrer que l'intersection des  $U_n$  que l'on va noter  $U$  est dense dans  $X$ . Soit pour cela un élément  $x$  de  $X$  et un réel  $\varepsilon$  strictement positif. Il s'agit de construire un élément  $y$  dans  $U$  qui soit tel que  $d(x, y) < \varepsilon$ ,  $d$  désignant la distance sur  $X$ . Pour cela on va construire par récurrence une suite  $V_n$  d'ouverts de  $X$  inclus dans la boule de centre  $x$  et de rayon  $\varepsilon$ ,  $V_n$  étant inclus dans l'intersection des  $(U_k)$  pour  $k < n$  et de diamètre inférieur à  $\frac{\varepsilon}{n}$ . Il s'agit donc pour cela de définir une fonction  $\varphi$  qui à un couple  $(n, V)$  associe un ouvert  $V'$ . Comment fait-on cela ?

On part donc d'un couple  $(n, V)$ .  $V$  étant un ouvert de  $X$ , il intersecte l'ouvert dense  $U_n$ . Cette intersection est encore un ouvert et donc elle intersecte à son tour  $A$ . Notons disons  $B$  l'intersection de  $V$  avec  $U_{n+1}$  et avec  $A$ , ce que l'on vient de dire c'est que  $B$  est non vide. En particulier l'élément  $f(B)$  est bien défini. D'autre part comme l'intersection  $(U_n \cap V)$  est un ouvert, l'ensemble des  $\eta > 0$ ,  $\eta < \frac{\varepsilon}{n}$  tels que la boule de centre  $f(B)$  et de rayon  $\eta$  soit incluse dans  $(U_n \cap V)$  est non vide et majoré et donc admet une borne supérieure. Appelons  $s$  cette borne supérieure. L'ouvert  $V'$  que j'associe au couple  $(n, V)$  est alors la boule ouverte de centre  $f(B)$  et de rayon  $\frac{s}{2}$ .

Le lecteur pourra alors vérifier par lui-même que si l'on choisit pour  $V_0$  la boule ouverte de centre  $x$  et de rayon  $\varepsilon$ , la suite construite par le théorème du paragraphe précédent vérifie bien les conditions que l'on voulait.

Maintenant il est assez simple de conclure. Pour tout  $n$  de  $\mathbb{N}$ , l'intersection de  $V_n$  et de  $A$  est non vide. Je définis une suite  $(y_n)$  en posant  $y_n = f(V_n \cap A)$ . Je dis qu'il est alors immédiat que  $(y_n)$  est une suite de Cauchy et que sa limite fournit un  $y$  tel qu'on le désirait.

### 3.5.8 Complétude de $\mathbb{R}^n$

Afin de prouver que le théorème de Baire a une quelconque utilité, nous allons montrer que  $\mathbb{R}^n$ , muni de la norme infinie disons (il est encore vrai que toutes les normes sur  $\mathbb{R}^n$  sont équivalentes sans l'axiome du choix mais passons) est complet et ce encore indépendamment de l'axiome du choix. Bien entendu, il suffit de le faire pour  $\mathbb{R}$ , ensuite on conclut simplement par récurrence.

Rappelons que l'on avait décrit  $\mathbb{R}$  comme étant l'ensemble des suites de Cauchy à valeurs dans  $\mathbb{Q}$  quotienté par la relation d'équivalence disant que deux suites sont équivalentes si et seulement si leur différence converge vers 0. Considérons  $(x_n)$  une suite de Cauchy de réels. Il s'agit de construire un réel  $\ell$ , limite de la suite  $(x_n)$ . Par définition, ce réel est simplement une suite de Cauchy de rationnels  $(\ell_n)$ . Nous

aurons besoin pour cela d'une fonction de choix sur  $\mathbb{Q}$ . Comme nous l'avons déjà maintenant souvent dit, une telle fonction existe même sans l'axiome du choix, simplement par dénombrabilité de  $\mathbb{Q}$ . Notons  $f$  une telle fonction de choix.

On considère  $n$  un entier, c'est-à-dire un élément de  $\mathbb{N}$ . On définit alors  $\ell_n$  comme l'image par  $f$  de l'intersection non vide de  $[x_n - \frac{1}{n}, x_n]$  avec  $\mathbb{Q}$ . Il est alors facile de vérifier que la suite  $(\ell_n)$  est de Cauchy donc définit un réel et d'autre part que la différence  $\ell_n - x_n$  converge vers 0 et que donc le réel défini est bien la limite de la suite  $(x_n)$ .

## 4 Étude des bons ordres

Les quelques exemples précédents ont, je l'espère, montré l'importance des ensembles bien ordonnés pour se passer de l'axiome du choix. Nous allons par la suite étudier ceux-ci un peu plus en détail.

### 4.1 Présentation intrinsèque

On commence par regarder la classe des bons ordres, c'est-à-dire des couples  $(E, \leq)$  où  $\leq$  est une relation de bon ordre sur  $E$ . Il n'est pas très difficile de se convaincre qu'il n'existe aucun ensemble dont les éléments sont précisément tous ces couples, c'est la raison pour laquelle nous préférons employer le terme de "classe".

Soient  $(E, \leq)$  et  $(F, \leq)$  (il y a ici un abus de notation, les deux relations d'ordre ne sont pas du tout les mêmes en général) deux bons ordres. On dit qu'ils sont isomorphismes s'il existe une bijection  $f : E \rightarrow F$ , telle que :

$$\forall x \in E, \forall y \in E, (x \leq y) \Rightarrow (f(x) \leq f(y))$$

( $f$  vérifiant cette formule est dite tout simplement croissante). On notera par la suite  $E \sim F$  pour dire que les bons ordres  $(E, \leq)$  et  $(F, \leq)$  sont isomorphes.

En fait, la classe des bons ordres peut être munie d'une "relation" de pré-ordre. Si  $(E, \leq)$  et  $(F, \leq)$  sont deux bons ordres, on dit que  $E$  est plus petit que  $F$ , et on note  $E \leq F$ , si  $E$  est isomorphe à un segment initial de  $F$ , un *segment initial* de  $F$  étant un sous-ensemble  $F'$  de  $F$  tel que si  $x$  appartient à  $F'$  tout élément inférieur à  $x$  lui appartient également.

Il est assez simple de vérifier que cette relation est réflexive et transitive. C'est donc un pré-ordre. Que se passe-t-il si  $E$  et  $F$  sont deux bons ordres tels que  $E \leq F$  et  $F \leq E$ ?  $E$  est alors isomorphe à un segment initial de lui-même, disons  $E'$ . Montrons que cette bijection, disons  $f$ , ne peut être que l'identité de  $E$ , et donc du coup qu'en fait  $E = E'$ . Supposons que ce ne soit pas le cas, alors il existe un plus petit élément  $x$  de  $E$  tel que  $f(x) \neq x$ . Mais alors, si  $y < x$ , on a  $f(y) = y < x$ . Ainsi,  $f(x) > x$ , puisque  $f$  est bijective. On en déduit par croissance que si  $y \geq x$ , alors  $f(y) > x$ . Ceci prouve que  $x$  n'est pas atteint et pourtant  $f(x) > x$  l'est manifestement, on aboutit ainsi à une contradiction. On en déduit que  $E = E'$  et donc que  $E$  et  $F$  étaient en fait isomorphes. Finalement, la "relation" de pré-ordre que l'on vient de définir induit une "relation" d'ordre sur les classes d'isomorphismes de bons ordres. Les guillemets sont là pour garder en mémoire que l'"ensemble" des bons ordres ou des classes d'équivalence de bons ordres n'en est justement pas un, et donc que cela n'est pas à prendre dans un sens formel.

Cette "relation" d'ordre est même un bon ordre dans le sens où si les  $(E_i)$  sont des ensembles bien ordonnés, alors il existe un  $j$  tel que  $E_j$  soit plus petit que tous les autres. Disons rapidement comment l'on prouve cela. On choisit un ensemble quelconque parmi les  $E_i$ , disons  $E$ , et on regarde la réunion des segments initiaux de  $E$  qui sont plus petits que tous les  $E_i$ . On montre ensuite que cet ensemble est isomorphe en tant qu'ensemble bien ordonné à l'un des  $E_j$  et qu'il est plus petit que tous les  $E_i$ .

En particulier, cette “relation” d’ordre est totale. Cela veut dire qu’étant donné deux bons ordres  $E$  et  $F$ , on a soit  $E \leq F$ , soit  $F \leq E$ .

## 4.2 Les ordinaux

Ce que l’on va appeler un ordinal, c’est un représentant particulier de chacune des classes que l’on vient de définir. Mais comment choisir un tel représentant ? Ce que l’on constate, c’est que si  $E$  est un ensemble bien ordonné, l’ensemble de ses segments initiaux stricts (ie différents de  $E$ ) muni de l’inclusion forme également un ensemble bien ordonné qui est en fait isomorphe à  $E$  (en effet étant donné un élément  $x$  de  $E$ , l’ensemble  $S_x$  des éléments de  $E$  strictement plus petits que  $x$  forme un segment initial et réciproquement étant donné un segment initial strict  $S$  de  $E$ , l’ensemble  $E \setminus S$  est non vide et admet donc un plus petit élément  $x$ , il est alors facile de voir que  $S = S_x$ ). On pense donc à remplacer  $E$  par l’ensemble de ses segments initiaux stricts, chacun de ces segments initiaux est un bon ordre on lui applique alors la même transformation et ainsi de suite... et de fait ça marche. Voyons comment ça marche sur les premiers bons ordres.

Commençons par l’ensemble vide. Il est muni d’un unique ordre, l’ordre vide, qui a toutes les propriétés requises pour être un bon ordre. Il est même tout seul dans sa classe d’équivalence, c’est donc nécessairement lui qu’il faut choisir. Il est même facile de voir qu’il s’agit du plus petit ordinal, on le note  $0$ .

Prenons maintenant un ensemble  $E$  à un unique élément, disons  $E = \{x\}$ .  $E$  encore est muni d’un unique ordre qui encore est un bon ordre.  $E$  admet un unique segment initial strict qui est l’ensemble vide. Le représentant que l’on va choisir dans la classe de  $E$  sera donc le singleton  $\{0\} = \{\emptyset\}$ . C’est lui le deuxième plus petit ordinal, on le note  $1$ .

Si maintenant  $E$  a deux éléments,  $E = \{x, y\}$ , et est muni de la relation de bon ordre définie par  $x < y$ , les segments initiaux de  $E$  sont  $\emptyset$  et  $\{x\}$ . On remplace ensuite chacun de ces segments initiaux par leur représentant. Ici donc le représentant choisi dans la classe de  $E$  sera  $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$ . Et voici le troisième plus petit ordinal, on le note  $2$ .

Et on continue ainsi...

L’ordinal  $n$  serait alors l’ensemble  $\{0, 1, \dots, n - 1\}$  sur lequel on a mis le bon ordre auquel on pense. De façon plus générale, un ordinal n’est autre que l’ensemble des ordinaux plus petits que lui.

Ce qu’il y a d’intéressant, c’est que les opérations classiques que l’on peut imaginer sur les classes d’équivalence de bons ordres se transposent très simplement sur les ordinaux.

Tout d’abord, si  $E$  est un ensemble bien ordonné d’ordinal  $\alpha$ , il est légitime de s’intéresser à la classe venant juste après celle de  $E$ , ie formellement à la plus petite classe qui soit strictement supérieure à celle de  $E$ . Il lui correspond un ordinal  $\beta$ . Il n’est pas bien difficile de voir que d’après la construction que l’on a fait, l’ordinal  $\beta$  s’exprime simplement par  $\beta = \alpha \cup \{\alpha\}$ .  $\beta$  est alors appelé l’ordinal successeur de  $\alpha$ . Un ordinal qui est le successeur d’un autre est appelé un *ordinal successeur*. Un ordinal non successeur et non nul est appelé un *ordinal limite*.

Prenons maintenant une famille  $(E_i)$  de bons ordres indexée par un ensemble  $I$ . Notons  $\alpha_i$  l’ordinal de  $E_i$  et intéressons-nous au plus petit bon ordre qui majore simultanément tous les  $E_i$ , ce que l’on pourrait appeler la borne supérieure des  $E_i$ . Notons  $E$  ce bon ordre. L’ordinal de  $E$  est là encore assez facile à décrire, il s’agit simplement de la réunion des  $\alpha_i$  comme il est encore assez facile de s’en convaincre.

Remarquez que pour l’instant nous n’avons donné aucune définition rigoureuse. En effet, étant donné un ensemble, on est à ce stade plus ou moins incapable de dire s’il s’agit d’un ordinal ou si ce n’est pas le

cas. Cependant, il existe bien une formule qui permet de faire cela. Plus précisément  $\alpha$  est un ordinal s'il vérifie les deux conditions suivantes :

1. (*transitivité*)  $\forall x \forall y ((x \in y) \text{ et } (y \in \alpha)) \Rightarrow (x \in \alpha)$
2. la relation d'appartenance entre les éléments de  $\alpha$  constitue une relation de bon ordre strict

Une chose d'important et assez facile à prouver est qu'il n'existe pas d'ensemble ayant précisément tous les ordinaux pour éléments. Une façon de le voir est de remarquer qu'un tel ensemble serait lui-même un ordinal, et donc serait un élément de lui-même... ce qui n'est pas possible au vu de la définition.

### 4.3 Construction de $\mathbb{N}$

On est maintenant en mesure de construire cet ensemble  $\mathbb{N}$  dont on n'arrête pas de parler depuis si longtemps. L'axiome de l'infini que nous n'avons pas encore utilisé assure l'existence d'un ordinal non nul et non successeur. Nous n'allons pas démontrer cela, le lecteur soucieux pourra le faire par lui-même.

En particulier, d'après les propriétés des ordinaux, il existe un plus petit ordinal non nul et non successeur. C'est cet ensemble que l'on appelle  $\mathbb{N}$ , ou plus souvent  $\omega$ . Il s'agit précisément de l'ensemble des ordinaux finis, un *ordinal fini* étant par définition un ordinal successeur ou nul et tel que tous les ordinaux strictement plus petits que lui soient également successeurs ou nuls. Ces ordinaux finis sont la traduction dans notre modèle de ZF des entiers naturels.

Maintenant sur  $\mathbb{N}$ , et d'ailleurs plus généralement sur les ordinaux on peut construire des opérations, à savoir l'addition et la multiplication. Commençons par construire l'addition. Prenons  $\alpha$  et  $\beta$  deux ordinaux. Prenons  $A$  (resp.  $B$ ) un ensemble bien ordonné d'ordinal  $\alpha$  (resp.  $\beta$ ). Sur l'union disjointe de  $A$  et de  $B$ , on peut mettre un bon ordre naturel : dit avec les mains, on met d'abord les éléments de  $A$  que l'on classe comme ils le sont déjà puis on rajoute derrière les éléments de  $B$  sans encore toucher à l'ordre. Ce bon ordre là est donné par un ordinal, c'est celui-ci que l'on définit comme étant la somme de  $\alpha$  et de  $\beta$  et que l'on note  $\alpha + \beta$ .

Il faut faire attention à ce que cette opération ne possède pas toutes les propriétés que l'on souhaiterait. Cette addition par exemple n'est pas commutative (par exemple  $\omega + 1$  est le successeur de  $\omega$  – et plus généralement  $\alpha + 1$  est toujours le successeur de  $\alpha$  – mais  $1 + \omega$  est  $\omega$ ). Toutefois, l'associativité, elle, reste valable. Toutefois également, si l'on se restreint aux ordinaux finis, cette opération fournit une application de  $\mathbb{N}$  dans  $\mathbb{N}$ , l'addition, qui elle est bien commutative.

Voyons maintenant la multiplication. Comme précédemment on part de deux ensembles bien ordonnés  $A$  et  $B$  d'ordinal respectif  $\alpha$  et  $\beta$ . On regarde ce coup-ci le produit  $A \times B$  que l'on munit de l'ordre lexicographique en donnant priorité aux éléments de  $B$ . Autrement dit, le couple  $(a, b)$  sera strictement plus petit que le couple  $(a', b')$  si  $b < b'$  ou si  $b = b'$  et  $a < a'$ . Ceci fournit un bon ordre sur le produit  $A \times B$ . Il lui correspond un ordinal, c'est le produit  $\alpha \cdot \beta$ .

Là encore, il faut faire attention au fait que la multiplication n'est pas commutative. Elle est distributive sur l'addition simplement d'un seul côté... on laisse en exercice au lecteur le soin de trouver lequel :-). Toutefois encore si l'on se restreint aux ordinaux finis, on obtient une application de  $\mathbb{N}$  dans  $\mathbb{N}$  qui a les bonnes propriétés de la multiplication que l'on manie depuis notre plus tendre enfance.

Les propriétés générales de ces opérations se démontrent grâce au principe d'induction que l'on détaillera dans le paragraphe suivant. Les propriétés valables seulement pour les ordinaux finis se démontrent, elles, grâce au principe de récurrence (qui est un cas particulier du principe d'induction) que nous énonçons tout de suite.

Soit  $F(x)$  une formule possédant une variable libre. Si  $F(0)$  est vraie et si pour tout ordinal fini  $n$ ,  $F(n)$  implique  $F(n + 1)$ , alors la formule  $\forall n \in \mathbb{N}, F(n)$  est également vraie.

Une application plus ou moins directe et encore laissée au lecteur de ce principe de récurrence est la démonstration de la propriété énoncée dans le paragraphe 3.5.6.

#### 4.4 Principe d'induction

Le principe d'induction dit la chose suivante. Soit  $F(x)$  une formule à une variable libre. On suppose que :

$$\forall \alpha \text{ ordinal } (\forall \beta \text{ ordinal } < \alpha, F(\beta)) \Rightarrow F(\alpha)$$

Alors on en déduit que  $\forall \alpha \text{ ordinal } F(\alpha)$

La démonstration est la suivante. Supposons que la conclusion soit fausse. Alors il existe au moins un ordinal  $\alpha$  tel que  $F(\alpha)$  soit fausse. Considérons le plus petit tel  $\alpha$ . Par définition tous les  $F(\beta)$  pour  $\beta < \alpha$  sont vraies, mais alors  $F(\alpha)$  est vraie grâce à l'hypothèse. D'où la contradiction et le théorème.

On remarquera qu'il n'est pas nécessaire de faire une hypothèse supplémentaire d'initialisation dans ce théorème, cette initialisation étant impliquée par l'hypothèse en prenant  $\alpha = 0$ .

On pourra aussi remarquer que ce principe d'induction implique le principe de récurrence énoncé précédemment. Toutefois, il est peut-être encore plus simple, afin de prouver le principe de récurrence, d'adapter le raisonnement donné ci-dessus.

#### 4.5 Retour sur les équivalents de l'axiome du choix

Les énoncés équivalents à l'axiome du choix auxquels nous allons nous intéresser ici sont le lemme de Zorn, le théorème de Zermelo. Les énoncés de ces propriétés ont été donnés et plus ou moins commentés dans le paragraphe 3.4. Nous nous proposons ici de donner des indications sur la preuve de l'équivalence de toutes ces propriétés en utilisant la puissance des ordinaux.

##### 4.5.1 Théorème de Zermelo

Prouvons dans un premier temps que l'axiome du choix implique le théorème de Zermelo. Prenons donc  $E$  un ensemble quelconque. On cherche à construire un bon ordre sur  $E$ . Rappelons-nous que par hypothèse, on dispose d'une fonction de choix sur  $E$ , disons  $f : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$ . On va définir notre bon ordre par induction sur les ordinaux. Plus précisément, on va définir pour tout ordinal  $\alpha$ , une partie  $E_\alpha$  de  $E$  munie d'un bon ordre et ce de telle façon que si  $\beta < \alpha$ ,  $E_\beta$  soit inclus dans  $E_\alpha$  et le restriction du bon ordre sur  $E_\alpha$  à  $E_\beta$  coïncide avec le bon ordre sur  $E_\beta$ . D'après le principe d'induction, pour faire cela, il suffit de dire comment construire  $E_\alpha$  à partir des  $E_\beta$ ,  $\beta < \alpha$ .

C'est assez simple en fait. On regarde  $E'$  défini comme la réunion de ces  $E_\beta$ . Avec les hypothèses faites,  $E'$  est muni d'un bon ordre. On regarde maintenant l'ensemble  $E \setminus E'$ . S'il est vide, on pose  $E_\alpha = E'$ . Sinon on regarde l'élément  $x = f(E \setminus E')$  qui bien sûr n'appartient pas à  $E'$  et on met sur l'union  $E' \cup \{x\}$  un bon ordre en disant que  $x$  est plus grand que tout le monde. Cela convient.

Il faut ensuite se persuader qu'il existe un  $\alpha$  tel que  $E_\alpha = E$ . On remarque pour cela que si ce n'est pas le cas, par construction  $E_\beta$  est strictement inclus dans  $E_\alpha$  pour  $\beta < \alpha$ . Mais cela n'est pas possible... on aurait ainsi une injection de la classe des ordinaux dans un ensemble  $E$ , ce qui prouverait que la classe des ordinaux est un ensemble, ce qui est faux.

La réciproque, quant à elle est toute simple. Étant donné un bon ordre sur  $E$ , on construit une fonction de choix en associant à une partie non vide de  $E$  son plus petit élément.

On remarquera que l'on a démontré ici un peu plus que l'équivalence entre l'axiome du choix et le théorème de Zermelo. On a prouvé qu'un ensemble  $E$  admet une fonction de choix si et seulement s'il admet un bon ordre.

#### 4.5.2 Lemme de Zorn

Prouver le lemme de Zorn à partir de l'axiome du choix se fait encore avec les ordinaux. Nous n'allons en fait pas détailler cette démonstration, les idées qui interviennent étant essentiellement celles décrites dans le paragraphe précédent.

Voyons la réciproque. On montre ici la deuxième forme de l'axiome du choix, celle avec les produits. Soit donc  $I$  un ensemble non vide et  $(X_i)$  une famille d'ensembles non vides indexée par  $I$ . On considère l'ensemble des fonctions  $f$  définies sur une partie  $J$  de  $I$  et telles que pour tout élément  $i$  de  $J$ ,  $f(i)$  appartienne à  $X_i$ . Ces fonctions sont ordonnées par inclusion. Il n'est pas bien dur de voir que cet ensemble est inductif, une chaîne admettant naturellement pour majorant l'union des éléments qui la constituent. Le lemme de Zorn fournit alors un élément maximal, c'est un élément du produit des  $X_i$  qui est donc non vide.

### 4.6 D'autres applications

#### 4.6.1 $E$ est-il en bijection avec $2E$ ?

Disons tout d'abord que  $2E$  est par définition le produit  $2 \times E$ , ou encore  $\{0, 1\} \times E$ . Regardons tout d'abord le cas où  $E$  peut être muni d'un bon ordre (ou ce qui revient au même d'une fonction de choix). En fait on peut même regarder le plus petit bon ordre que l'on peut obtenir ainsi. Cet ordinal désigne ce que l'on appelle communément le cardinal de  $E$ .

Il y a une définition disons intrinsèque d'un cardinal. Il s'agit d'un ordinal qui n'est en bijection avec aucun ordinal strictement plus petit. Il est immédiat de se convaincre que l'ordinal associé ci-dessus est bien un cardinal et même que tout cardinal est l'"associé" d'un certain ensemble (par exemple lui-même). Tout ça pour dire que pour prouver le résultat lorsque  $E$  admet un bon ordre, on peut supposer que  $E$  est un cardinal que l'on va appeler  $\kappa$ .

Une dernière chose à savoir sur les cardinaux, c'est que ceux-ci sont bien ordonnés. C'est évident car la classe des cardinaux forme une sous classe de la classe des ordinaux qui est bien ordonnée. Remarquez que ceci n'utilise pas l'axiome du choix et n'est pourtant pas du tout en contradiction avec le fait que le lemme de trichotomie l'utilise. On rappelle en effet que l'on n'a pas associé un cardinal à tout ensemble, mais simplement aux ensembles qui peuvent être munis d'un bon ordre.

En particulier le principe d'induction s'applique encore sur les cardinaux. Plus précisément pour montrer que  $\kappa$  est en bijection avec  $2 \times \kappa$  pour tout cardinal  $\kappa$ , il suffit de prouver qu'étant donné  $\kappa$  un cardinal,  $\kappa$  est en bijection avec  $2 \times \kappa$  sous l'hypothèse que pour tout cardinal  $\kappa' < \kappa$ , on a  $\kappa'$  en bijection avec  $2 \times \kappa'$ . Mais bien sûr, on ne va pas pouvoir montrer cela puisqu'il est clair que ce n'est pas vrai si  $\kappa$  est un cardinal fini non nul. Un *cardinal fini* est par définition un élément de  $\mathbb{N}$  (on pourra se convaincre que tout élément de  $\mathbb{N}$  est un cardinal successeur et que la réciproque est même vraie). Un cardinal qui n'est pas fini sera dit *infini*. Dans le paragraphe suivant, nous allons montrer par induction sur les cardinaux infinis que  $2 \times \kappa$  est toujours en bijection avec  $\kappa$ .

Allons-y. On va construire une injection de  $2 \times \kappa$  dans  $\kappa$  par induction sur l'ordinal  $\alpha \leq \kappa$ , le théorème de Cantor-Bernstein permettra alors de conclure. Cela signifie que l'on va construire pour tout ordinal  $\alpha \leq \kappa$  une injection de  $2 \times \alpha$  dans  $\kappa$ , ces injections étant compatibles dans un sens évident.

Si  $\alpha = 0$ , il n'y a rien à construire. Supposons maintenant que  $\alpha = \beta + 1$  est un ordinal successeur. Par hypothèse d'induction on a une injection  $f : 2 \times \beta \rightarrow \kappa$ . Si le cardinal de  $\beta$  est infini,  $2 \times \beta$  est en bijection avec  $\beta$  par la première hypothèse d'induction et  $\beta < \kappa$  (car  $\alpha \leq \kappa$ ) n'est pas en bijection avec  $\kappa$  puisque  $\kappa$  est un cardinal. D'autre part, si le cardinal de  $\beta$  est fini, celui de  $2 \times \beta$  l'est également (ce que l'on peut montrer indépendamment par récurrence) et donc il n'est pas non plus en bijection avec  $\kappa$ . Dans tous les cas, la fonction  $f$  ne peut être surjective. Considérons le plus petit élément de  $\kappa$  qui n'est pas dans l'image de  $f$ , appelons le  $x$ . On peut prolonger  $f$  en posant  $f(0, \beta) = x$ . Pour les mêmes raisons que précédemment,  $f$  ainsi prolongée n'est toujours pas surjective. Appelons  $y$  le plus petit élément de  $\kappa$  qui n'est pas dans son image et prolongeons encore  $f$  en posant  $f(1, \beta) = y$ . On obtient ainsi une injection de  $2 \times \alpha$  dans  $\kappa$ , ce qui est précisément ce que l'on voulait.

Maintenant si  $\alpha$  est un ordinal limite, il suffit de prendre pour  $f$  la réunion de toutes les fonctions  $f$  construites pour les ordinaux  $\alpha < \beta$ . Celle-ci convient.

Ainsi exhiber une bijection entre  $E$  et  $2E$  peut se faire sans l'axiome du choix dès que  $E$  peut être muni d'un bon ordre. Nous n'allons pas le prouver mais dans le cas général, l'axiome du choix est requis...

#### 4.6.2 $E$ est-il en bijection avec $E^2$ ?

Là encore, on va commencer par traiter le cas où  $E$  est un ensemble qui admet un bon ordre. Comme précédemment, on se ramène au cas où  $E$  est un cardinal  $\kappa$  infini et comme précédemment on peut supposer que le résultat est démontré pour tout cardinal  $\kappa'$  infini strictement inférieur à  $\kappa$ . Il s'agit ce coup-ci de construire une injection de  $\kappa^2$  dans  $\kappa$ , ce que l'on fait par induction sur l'ordinal  $\alpha \leq \kappa$ .

Il s'agit donc, vous l'auriez deviné, de construire une injection de  $\alpha^2$  dans  $\kappa$ . Supposons dans un premier temps que  $\alpha$  soit un ordinal limite, alors comme précédemment la réunion des fonctions précédemment construites convient. Supposons donc maintenant que  $\alpha$  soit un ordinal successeur, par exemple  $\alpha = \beta + 1$ . Comme  $\alpha \leq \kappa$ , on a  $\beta < \kappa$  et du coup  $\alpha < \kappa$ . On dispose d'une injection  $f : \beta^2 \rightarrow \kappa$  et il s'agit donc de la prolonger en lui attribuant des valeurs sur l'ensemble  $(\alpha^2) \setminus (\beta^2)$ . Mais cet ensemble peut être muni d'un bon ordre. Il suffit par exemple de le voir comme l'union disjointe  $(\{\alpha\} \times \alpha) \cup (\alpha \times \{\alpha\}) \cup (\{(\alpha, \alpha)\})$  que l'on munit d'un bon ordre en décrétant que les éléments de la première composante sont plus petits que ceux de la deuxième, eux mêmes plus petits que ceux de la troisième. Comme précédemment  $f$  n'est pas surjective et même encore par un argument de cardinalité (que nous laissons au lecteur),  $\kappa$  privé de l'image de  $f$  est un ensemble bien ordonné de cardinal  $\kappa$ . Ainsi l'union disjointe précédente est isomorphe à un segment initial de  $\kappa$  privé de l'image de  $f$ . Ceci permet de prolonger  $f$  tel qu'on le désirait.

Là encore si  $E$  est un ensemble quelconque, ceci n'est plus vrai sans l'axiome du choix. Un peu plus fort même, le fait que  $E$  soit en bijection avec  $E^2$  pour tout ensemble  $E$  infini est un énoncé équivalent à l'axiome du choix. Nous n'allons pas démontrer cette dernière affirmation non plus.

#### 4.6.3 Clôture algébrique

La question ici est la suivante. Soit  $K$  un corps. Peut-on construire une clôture algébrique de  $K$  sans l'axiome du choix ? Ça ne paraît pas évident, en tout cas la démonstration classique utilise le lemme de Krull qui est connu pour être une conséquence de l'axiome du choix. Voyons tout de même ce que l'on peut faire.

Bien entendu, au vu des exemples précédents, on va commencer par supposer que  $K$  peut être muni d'un bon ordre. Ce que l'on doit faire, c'est ajouter à  $K$  les racines de tous les polynômes (irréductibles) sur  $K$ . On commence donc par lister tous les polynômes à coefficients dans  $K$ . Cet ensemble peut être



muni d'un bon ordre en disant par exemple que l'on commence à ordonner ces polynômes en regardant les degrés puis qu'à l'intérieur d'un même degré on utilise l'ordre lexicographique. Notons par exemple  $\alpha$  l'ordinal associé à ce bon ordre.

Ce que l'on va faire c'est construire par induction sur l'ordinal  $\beta \leq \alpha$ , des corps  $K_\beta$  extensions compatibles de  $K$  qui vont être munis d'un bon ordre et qui seront tels que tous les polynômes indexés par un ordinal  $\leq \beta$  auront au moins une racine dans  $K_\beta$ . Le corps  $K_\alpha$  ainsi construit sera une clôture algébrique de  $K$ .

Commençons par construire  $K_0$ . Il s'agit d'ajouter à  $K$  une racine du polynôme  $P_0$ . Pour faire cela, on commence par décomposer  $P_0$  en produits de polynômes irréductibles et on choisit un de ces facteurs. Bien entendu, on ne choisit pas n'importe lequel, on prend par exemple celui qui est le plus petit pour le bon ordre défini sur l'ensemble des polynômes à coefficients dans  $K$ . Si  $P$  désigne ce polynôme irréductible, on prend pour  $K_0$  le corps  $K[X]/P$ . Il ne reste plus qu'à mettre un bon ordre sur  $K_0$  mais tout élément de  $K_0$  peut être vu comme un polynôme de degré inférieur au degré de  $P$ , l'ordre lexicographique peut donc être utilisé.

Et en fait, on applique exactement la même construction pour passer de  $K_\beta$  à  $K_{\beta+1}$ . Si  $\beta$  est un ordinal limite, on commence par regarder la limite inductive des  $K_{\beta'}$  pour  $\beta' < \beta$  et on applique la construction précédente à cette limite inductive. Cela fonctionne.

On vient donc de construire une clôture algébrique de  $K$  et on a même un petit bonus : dès que  $K$  est fini, cette clôture algébrique est dénombrable, si  $K$  est infini, elle a le même cardinal que celui de  $K$ . Qu'en est-il de l'unicité ? Voyons cela. Prenons donc  $L$  une clôture algébrique de  $K$  et essayons de construire un isomorphisme entre  $K_\alpha$  et  $L$  (en gardant les notations précédentes). Cet isomorphisme va se construire par induction sur l'ordinal  $\beta \leq \alpha$ . Il s'agit donc simplement à chaque étape de choisir dans  $L$  une racine du polynôme  $P$ . Aïe, mais nous n'avons rien supposé sur  $L$ , il n'admet pas forcément de fonction de choix. On laisse le lecteur écrire proprement la démonstration que sous l'hypothèse que  $L$  est bien ordonnable alors il existe une bijection entre  $K_\alpha$  et  $L$ .

Toutefois cela n'est pas vrai en général. Il existe des modèles de ZF dans lesquels le corps des rationnels  $\mathbb{Q}$  admet une clôture algébrique qui n'est pas dénombrable. De fait, elle ne sera pas isomorphe à la clôture algébrique de  $\mathbb{Q}$  donnée par la construction précédente. D'après ce que l'on vient de dire, il s'agira là d'un ensemble n'admettant pas de fonction de choix...

Finalement, on peut signaler que si  $A$  est une clôture algébrique de  $\mathbb{Q}$ , il est toujours vrai que  $A$  est réunion dénombrable d'ensembles finis, à savoir l'ensemble des racines d'un polynôme à coefficients rationnels donné. Notamment, une réunion dénombrable d'ensembles finis n'est pas forcément dénombrable, comme nous allons le redire juste en dessous. :-)

## 4.7 Quelques désillusions

Nous espérons vous avoir plus ou moins convaincu dans ce qui précède que les bons ordres sont quelque chose d'intimement lié à l'axiome du choix et que souvent quand on en dispose il est possible de faire nombre de constructions sans utiliser justement l'axiome du choix.

Toutefois il y a des écueils à ce principe. Nous allons citer un unique exemple mais qui vaut son pesant d'or. Sans l'axiome du choix, il n'est pas vrai qu'une union dénombrable d'ensembles dénombrables est forcément dénombrable. Pour pouvoir utiliser la magie des bons ordres, il faudrait soit mettre simultanément un bon ordre sur chaque ensemble dénombrable (et dit comme cela ceci requiert manifestement l'axiome du choix) ou à la limite mettre un bon ordre sur l'union mais justement a priori on ne sait pas que celle-ci est dénombrable.

Peut-être, allez-vous me dire : “Mais non, notons par exemple  $U_n$  les ensembles dénombrables dont on veut prendre l’union. Ben, pour tout  $n$ ,  $U_n$  est en bijection avec  $\mathbb{N}$ , donc l’union des  $U_n$  s’injecte dans  $\mathbb{N}^2$  et Cantor-Bernstein permet de conclure”. Eh ben, non, ce raisonnement est faux car pour construire l’injection de l’union des  $U_n$  dans  $\mathbb{N}^2$ , il faut disposer simultanément de toutes les bijections  $U_n \rightarrow \mathbb{N}$  et cela requiert l’axiome du choix, dénombrable seulement certes mais quand même.

Si vous êtes encore sceptique, essayez de formaliser proprement cette démonstration, vous verrez qu’elle bogue à un moment.

## 5 Conclusion

L’axiome du choix, dans sa plus grande généralité, est aujourd’hui largement accepté dans le monde mathématique. Il est à la base de nombreux résultats classiques et fondamentaux que l’on ne peut pas prétendre remettre en cause.

Toutefois, c’est aussi quand même lui qui affirme l’existence de “monstres” dirons-nous. C’est lui qui permet de construire une partie de  $\mathbb{R}$  non mesurable. Un résultat du même gabarit encore plus spectaculaire est sans doute le paradoxe de Banach-Tarski. Il dit que si  $U$  et  $V$  sont deux parties bornées de  $\mathbb{R}^3$  d’intérieur non vide, alors on peut trouver un entier  $n$ , une partition  $\{U_1, \dots, U_n\}$  de  $U$ , une partition  $\{V_1, \dots, V_n\}$  de  $V$  et des isométries  $\sigma_i$  de  $\mathbb{R}^3$  qui envoient précisément l’ensemble  $U_i$  sur l’ensemble  $V_i$ . Autrement dit, partant d’une orange, il est possible de la découper en un nombre fini de parties et de reconstituer une boule de la taille du soleil en déplaçant et en recomposant ces parties...

Il serait peut-être finalement intéressant de parler d’autres axiomes plus ou moins répandus dans le monde mathématique. L’hypothèse du continu est sans doute la plus médiatisée. Elle dit qu’un sous-ensemble de  $\mathbb{R}$  est soit fini, soit dénombrable, soit en bijection avec  $\mathbb{R}$ . Cet énoncé aussi est indécidable dans ZF et même dans ZFC... on peut donc choisir de le rajouter à la liste ou pas. Il semble que la tendance actuelle soit de ne pas le rajouter, de le remplacer plutôt par d’autres axiomes moins évidents à décrire mais qui reflètent mieux ce que l’on aimerait voir. Nous n’allons cependant pas détailler ces axiomes.

Pour finir, j’aimerais parler de l’axiome de détermination. Commençons par prendre une partie  $A$  de l’intervalle  $[0, 1]$ . Prenons également deux joueurs et faisons les jouer au jeu suivant. Le premier joueur choisit un chiffre en base 2, c’est-à-dire soit 0, soit 1. C’est le premier chiffre après la virgule de l’écriture binaire d’un nombre. Le deuxième joueur choisit un second chiffre, ce sera le deuxième chiffre... et ainsi de suite jusqu’à la fin des temps. Le premier joueur gagne si le nombre écrit au final est dans la partie  $A$ , perd sinon. Vous pourrez vous amuser à montrer par exemple que si  $A$  est un intervalle, il y a toujours un joueur qui a une stratégie gagnante. Un peu plus dur est de montrer que si  $A = \mathbb{Q} \cap [0, 1]$ , le deuxième joueur a une stratégie gagnante. On peut même montrer que si  $A$  est un borélien, alors un des deux joueurs a une stratégie gagnante. L’axiome de détermination dit que pour toute partie de  $[0, 1]$ , un de deux joueurs a une stratégie gagnante. C’est bien joli tout ça, mais cet axiome contredit l’axiome du choix. En effet, via l’axiome du choix, on peut construire une partie  $A$  de  $[0, 1]$  pour laquelle aucun de deux joueurs n’a de stratégie gagnante... Cet axiome a cependant des conséquences assez intéressantes comme par exemple le fait que toute partie de  $\mathbb{R}$  devient mesurable.

Que faut-il prendre comme axiome alors ? L’axiome du choix ? L’axiome de détermination ? Encore autre chose, comme celui qui dit que tout ensemble doit être constructible ? Vaste question... L’axiome du choix a l’air de très bien s’imposer aujourd’hui, et les raisons de cela sont vraiment importantes, mais qui sait ?