Théorie des Ensembles L3

Thomas Seiller
seiller@iml.univ-mrs.fr

1er semestre 2010/2011

Table des matières

1 Introduction

Theorie naive des ensembles - Paradoxe de Russell

§1.1 Intuitivement, un ensemble est une collection d'objets qui satisfont une certaine propriété. On est donc tenté de donner la règle suivante pour la définition d'ensembles.

> **Schéma de compréhension.** Si P est une propriété (avec éventuellement des paramètres $u_1, \ldots, u_n$), alors quelque soient les paramètres $\vec{u}$, il existe un ensemble $X = \{x \mid P(x, \vec{u})\}$.

On peut alors définir toutes les opérations habituelles sur les ensembles. Si $X = \{x \mid P_X(x)\}$ et $Y = \{x \mid P_Y(x)\}$ sont des ensembles, alors :

- $X \subset Y$ si et seulement si $P_X(x) \Rightarrow P_Y(x)$.
- on définit $X \cup Y = \{x \mid P_X(x) \vee P_Y(x)\}$
- on définit $X \cap Y = \{x \mid P_X(x) \wedge P_Y(x)\}$
- on définit $\mathcal{C}_X Y = \{x \mid P_X(x) \wedge \neg P_Y(x)\}$
- on définit $\mathcal{P}(X) = \{Y \mid Y \subset X\}$

§1.2 Cependant, ce principe est faux. En effet, considérons l'ensemble S défini par $S = \{X \mid X \notin X\}$. Est-ce que $S \in S$?

- Si $S \in S$, alors $S \notin S$ par définition de S.
- Si $S \notin S$, alors S est tel que $S \in S$.

Dans les deux cas, on arrive à une contraction. On est obligé de conclure que S n'est pas un ensemble. On doit donc redéfinir la notion d'ensemble afin d'exclure la construction de S, ou d'un autre ensemble posant des problèmes similaires.

§1.3 La manière la plus sûre d'éliminer les paradoxes de ce type est d'abandonner le schéma de compréhension, et d'en garder une version affaiblie : le schéma de séparation.

> **Schema de séparation.** Si P est une propriété (avec des paramètres $\vec{u}$) et $x, \vec{u}$ sont des ensembles, alors il existe un ensemble $y = \{z \mid z \in x \wedge P(z, \vec{u})\}$.

Une fois le schéma de compréhension éliminé, le paradoxe de Russell n'est plus aussi inquiétant. Il nous donne même une précieuse information : l'ensemble des tous les ensembles n'existe pas.

§1.4 Cependant, le schéma de séparation qui remplace le schéma de compréhension est trop faible pour développer la théorie des ensembles avec ses opérations et constructions usuelles. En particulier, il est impossible de montrer l'existence de l'union de deux ensembles. Cela ne suffit même pas à prouver qu'il existe au moins un ensemble !

On doit donc ajouter des axiomes supplémentaires afin d'obtenir une théorie des ensembles satisfaisante.

2 Axiomes de ZFC

§2.1 Dans ce chapitre, nous allons présenter la théorie axiomatique des ensembles de Zermelo-Fraenkel. Il s'agit d'une théorie axiomatique du premier ordre, construite sur le langage $\{\in, =\}$. Les objets dont parle cette théorie, c'est-à-dire les éléments (points) d'un modèle de ZF sont les ensembles : toute variable représente un ensemble et il n'existe pas d'autres types d'objets.

Classes et Formules

§2.2 Avant de parler d'ensembles, on va introduire la notion de *classe*, i.e. des collections d'objets qui ne sont pas nécessairement des ensembles. Par exemple, on pourra parler de la classe de tous les ensembles, qui n'est pas un ensemble. C'est une notion informelle (en réalité il existe d'autres axiomatisations de la théorie des ensembles qui formalisent la notion de classe, par exemple l'axiomatisation de Bernays-Gödel) qui est plus pratique que celle de formule. Il faut cependant toujours penser qu'une classe *n'est pas nécessairement un ensemble*, mais simplement la "collection" des éléments (ensembles) qui satisfont une formule donnée. Parler d'une classe, c'est juste une manière de parler de la collection des éléments qui satisfont une formule donnée.

Si $\phi(x)$ est une formule, on appelle

$$C = \{x \mid \phi(x)\}$$

une classe. Les éléments de C sont les éléments (ensembles) qui satisfont $\phi(x)$:

$$x \epsilon C \text{ si et seulement si } \phi(x)$$

§2.3 On dira que deux classes sont égales lorsqu'elles contiennent les mêmes éléments. Si

$$C = \{x \mid \phi(x)\} \text{ et } D = \{x \mid \psi(x)\}$$

alors $C = D$ si et seulement si pour tout x

$$\phi(x) \Leftrightarrow \psi(x)$$

i.e. si les formules ϕ et ψ sont logiquement équivalentes.

On peut en particulier définir la classe de tous les ensembles, appelée *l'univers*, par $\mathcal{U} = \{x \mid x = x\}$.

§2.4 On peut définir l'inclusion des classes :

$$C \subset D \text{ si et seulement si } \forall x, x \epsilon C \Rightarrow x \epsilon D$$

On définit les opérations suivantes sur les classes

$$\begin{aligned} C \cap D &= \{x \mid x \epsilon C \text{ et } x \epsilon D\} \\ C \cup D &= \{x \mid x \epsilon C \text{ ou } x \epsilon D\} \\ C - D &= \{x \mid x \epsilon C \text{ et } x \not\epsilon D\} \end{aligned} \tag{1}$$

On peut aussi définir le complémentaire d'une classe dans $\mathcal{U}$.

$$\bar{C} = \{x \mid x \not\in C\}$$

Axiome d'extensionalité (A1)

§2.5 L'axiome d'extensionalité permet de définir l'égalité entre ensemble à partir du symbole d'appartenance.

> Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

$$\forall x \forall y (\forall z (z \in x) \Leftrightarrow (z \in y)) \Leftrightarrow (x = y)$$

L'une des deux implications est en fait une conséquence du calcul des prédicats. Certains auteurs écrivent donc cet axiome sous la forme

$$\forall x \forall y \forall z ((z \in x) \Leftrightarrow (z \in y)) \Rightarrow (x = y)$$

Cet axiome exprime l'idée naturelle qu'un ensemble est déterminé par ses éléments. On peut remarquer que la notion d'égalité entre classes est définie de manière similaire.

Axiome de la paire

§2.6 L'axiome de la parie s'énonce ainsi :

> Si x et y sont deux ensembles, il existe un ensemble $\{x, y\}$ dont les éléments sont exactement x et y.

$$\forall x \forall y \exists z \forall t ((t \in z) \Leftrightarrow ((t = x) \vee (t = y)))$$

Par l'axiome d'extensionalité, cet ensemble est unique, et l'on peut définir la *paire*

$$\{a, b\} = \text{ l'unique } c \text{ tel que } \forall t ((t \in c) \Leftrightarrow ((t = x) \vee (t = y)))$$

On peut également définir le *singleton* $\{a\}$ comme l'ensemble $\{a, a\}$. Comme $\{a, b\} = \{b, a\}$; on définit également la *paire ordonnée*

§2.7 **Definition.** Soient a, b deux ensembles. On définit la paire ordonnée (a, b) par

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

§2.8 **Exercice.** Si $(a, b) = (c, d)$, alors $a = c$ et $b = d$.

Solution. On distingue deux cas.

Si $a = b$, alors $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$. Par extensionalité, (c, d) n'a qu'un seule élément, égal à $\{a\}$, donc $\{c, d\} = \{c\} = \{a\}$, et on a donc $c = d = a$.

Si $a \neq b$, alors (a, b) a deux éléments $\{a\}$ et $\{a, b\}$, donc (c, d) a également deux éléments $\{c\}$ et $\{c, d\}$, donc $c \neq d$. Comme $\{a\}$ ne peut être égal à $\{c, d\}$ puisqu'ils n'ont pas le même nombre d'éléments, on en déduit que $\{a\} = \{c\}$ et $\{a, b\} = \{c, d\}$, donc $a = c$ et $b = d$. □

§2.9 **Definition.** Pour tout entier n, on définit le n-tuple ordonné $(a_1, \ldots, a_n)$ par récurrence en utilisant la relation

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$$

§2.10 **Proposition.** *Deux n-tuples ordonnés $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ sont égaux si et seulement si $a_i = b_i$ pour tout i.*

Démonstration. Simple récurrence. □

Axiome de la réunion (A2)

§2.11 Attention, l'axiome de la réunion définit la réunion des éléments d'un ensemble x, et non l'union de plusieurs ensembles.

Si x est un ensemble, il existe un ensemble $y = \cup x$ dont les élément sont les éléments des éléments de x.

$$\forall x \exists y \forall z((z \in y) \Leftrightarrow (\exists t(z \in t) \wedge (t \in x))$$

En d'autres termes, y est l'union des éléments de x.

Si x est un ensemble, on note donc $\cup x$ l'ensemble défini par $\forall z((z \in \cup x) \Leftrightarrow (\exists t(z \in t) \wedge (t \in x))$.

§2.12 *Exemple.* Posons $x = \{a, b\}$, alors $\cup x$ est l'ensemble des éléments t tel que t est élément de a ou bien t est élément de b. Donc $\cup\{a, b\}$ définit l'union des deux ensembles a et b.

§2.13 **Exercice.** Soit $y = \{\{a, b, c\}, \{\{a, b\}\}, \{a\}, \{\{d\}\}\}$, quels sont les éléments de $\cup y$?

Solution. On a $\cup y = \{a, b, c, \{a, b\}, \{d\}\}$. □

§2.14 **Exercice.** Montrer que si a, b, c sont des ensembles, on peut définir un ensemble d dont les éléments sont exactment a,b et c. On notera $d = \{a, b, c\}$.

Solution. On définit $d = \cup\{\{a, b\}, \{c\}\}$. □

De manière plus générale, on peut définir par récurrence l'ensemble $\{a_1, \ldots, a_n\}$ en utilisant la définition

$$\{a_1, \ldots, a_n\} = \cup\{\{a_1, \ldots, a_{n-1}\}, \{a_n\}\}$$

Axiome des parties (A3)

§2.15

> Si x est un ensemble, il existe un ensemble y dont les éléments sont les sous-ensembles de x.

$$\forall x \exists y \forall t((t \in y) \Leftrightarrow (\forall v(v \in t) \Rightarrow (v \in x)))$$

Soient a et b deux ensembles. L'énoncé $\forall x x \in a \Rightarrow x \in b$ exprime l'inclusion des ensembles. On abrègera les énoncé en remplacant cette formule par $a \subset b$. L'axiome des parties peut alors se réecrire de manière abrégée

$$\forall x \exists y \forall t((t \in y) \Leftrightarrow (t \subset x))$$

Cet axiome énonce donc que si x est un ensemble, il existe un ensemble, que l'on notera $\mathcal{P}(x)$, *l'ensemble des parties* de x, dont les éléments sont exactement les sous-ensembles de x.

Classes de relations, classes de fonctions

§2.16 On définit la classe $\mathcal{U}^2$ des couples ordonnés d'ensembles par

$$\mathcal{U}^2 = \{v \mid \exists x \exists y, v = \{\{x\}, \{x, y\}\}\}$$

De manière similaire, on peut définir les classes $\mathcal{U}^n$ pour tout entier n.

§2.17 **Definition** (Classe de relation)**.** Une classe R est une classe de relation *n-aire* si on a $R \subset \mathcal{U}^n$.

§2.18 On peut alors définir les notions de (classes de) relations d'équivalence, (classes de) relations d'ordres stricts ou larges.

Une classe de relation binaire R est une classe de relation d'équivalence si elle satisfait les formules

$$\begin{aligned} \forall a \forall b \quad & R(a, b) \Rightarrow R(b, a) \\ \forall a \forall b \forall c \quad & (R(a, b) \wedge R(b, c)) \Rightarrow R(a, c) \end{aligned}$$

La classe $D(R) = \{a \mid R(a, a)\}$ est appelé le *domaine* de la relation R. On peut alors définir la classe d'équivalence d'un ensemble $a \epsilon D(R)$ comme

$$\tilde{a} = \{b \mid R(a, b)\}$$

§2.19 On définit les (classes de) relation d'ordre large comme les classes de relation binaires satisfaisant les formules

$$\begin{aligned} \forall a \forall b \quad & R(a, b) \Rightarrow (R(a, a) \wedge R(b, b)) \\ \forall a \forall b \quad & (R(a, b) \wedge R(b, a)) \Rightarrow a = b \\ \forall a \forall b \forall c \quad & ((R(a, b) \wedge R(b, c)) \Rightarrow R(a, c) \end{aligned}$$

On appelle la classe $D = \{x \mid R(x, x)\}$ le *domaine* de la (classe de) relation d'ordre R.

§2.20 Soit $D \subset \mathcal{U}$ une classe. On définit les (classes de) relation d'ordre strict de domaine D comme les classes de relation binaires satisfaisant les formules

$$\begin{aligned} \forall a \forall b \quad & R(a,b) \Rightarrow (D(a) \wedge D(b)) \\ \forall a \forall b \quad & \neg(R(a,b) \wedge R(b,a)) \\ \forall a \forall b \forall c \quad & (R(a,b) \wedge R(b,c)) \Rightarrow R(a,c) \end{aligned}$$

§2.21 **Definition** (Classe de Fonction)**.** Une classe de relation $n+2$-aire F est dite *fonctionnelle* si elle satisfait la formule

$$Fonc(F) = (x_1, \ldots, x_{n+1}, y) \in R \wedge (x_1, \ldots, x_{n+1}, y') \in R \Rightarrow y = y'$$

On parlera de classe de fonction à $n+1$ arguments.

§2.22 Etant donné une classe de fonction F à $n+1$ arguments, on peut définir son domaine par

$$Dom(F) = \{(x_1, \ldots, x_{n+1}) \mid \ \exists y, (x_1, \ldots, x_{n+1}, y) \in F\}$$

On définit de même son image par

$$Im(F) = \{y \mid \exists x_1 \exists x_2 \ldots \exists x_{n+1} (x_1, \ldots, x_{n+1}, y) \in F\}$$

Schema de remplacement (S1)

§2.23 Le schéma de remplacement dit que l'image d'un ensemble par une fonction est un ensemble. Il faut un axiome par fonction.

> Si $x, \vec{u}$ sont des ensembles, et F une fonction (avec paramètres $\vec{u}$), alors il existe $y = \{F(z, \vec{u}) \mid z \in x\}$ l'ensemble image de x par F.

$$Fonc(F, \vec{u}) := \forall v((F(v, \vec{u}, y) \wedge F(v, \vec{u}, y')) \Rightarrow (y = y'))$$

$$\forall x \forall \vec{u}\ Fonc(F, \vec{u}) \Rightarrow (\exists y \forall t((t \in y) \Leftrightarrow (\exists w(w \in x) \wedge F(w, \vec{u}, t)))))$$

Comme conséquence des axiomes de remplacement, nous avons le schéma de séparation.

Schema de séparation

§2.24 Le schéma de séparation dit que l'on peut utiliser le shéma de compréhension sur les éléments d'un ensemble.

> Si P est une propriété (avec des paramètres $\vec{u}$) et $x, \vec{u}$ sont des ensembles, alors il existe un ensemble $y = \{z \mid z \in x \wedge P(z, \vec{u})\}$.

$$\forall x \forall \vec{u} \exists y, \forall z, ((z \in y) \Leftrightarrow (z \in x) \wedge P(z, \vec{u}))$$

§2.25 **Proposition.** *Il existe un unique ensemble qui n'a aucun élément, que l'on note* $\emptyset$*.*

Démonstration. Soit a un ensemble. On applique le schéma de séparation à a avec l'énoncé $x \neq x$. Alors l'ensemble $\emptyset$ dont l'axiome affirme l'existence n'a aucun élément. Son unicité est une conséquence immédiate de l'axiome d'extensionalité. □

§2.26 **Exercice.** Montrer que l'axiome de la paire est une conséquence du schéma de substitution et de l'axiome de la réunion.

Solution. On a déjà montré qu'il existait un ensemble vide $\emptyset$. En utilisant l'axiome de la réunion, on en déduit l'existence de l'ensemble $\mathcal{P}(\emptyset)$. Cet ensemble contient un seul élément $\emptyset$, ce qui montre l'existence de $\{\emptyset\}$. Ce dernier ensemble a un seul élément, donc si $a \subset \{\emptyset\}$, on a $a = \emptyset$ ou $a = \{\emptyset\}$. Ce qui montre l'existence de l'ensemble $\{\emptyset, \{\emptyset\}\} = \mathcal{P}(\{\emptyset\})$. Maintenant, soient a, b des ensembles, on définit la relation $(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$ qui est clairement fonctionelle à un argument. En appliquant le schéma de substitution à cette relation et à l'ensemble $\{\emptyset, \{\emptyset\}\}$, on obtient l'existence d'un ensemble dont les éléments sont exactement a et b. □

§2.27 **Definition.** Etant donné deux ensembles a et b, on définit les ensembles $\{x \in a \mid x \in b\}$ et $\{x \in a \mid x \notin b\}$, appelés respectivement *intersection* et *différence ensembliste* de a et b, et noté $a \cap b$ et $a - b$.

§2.28 **Definition.** Etant donnés deux ensembles a et b, on définit le produit $a \times b$ comme la classe des couples (x, y) tels que $x \in a$ et $y \in b$.

§2.29 **Exercice.** Soient a, b deux ensembles. Montrer que $a \times b$ est un ensemble.

Solution. Si $x \in a$ et $y \in b$, alors le couple (x, y) appartient à l'ensemble $\mathcal{P}(\mathcal{P}(a \cup b))$. Donc $X(z) = \exists x \exists y[z = \{\{x\}, \{x, y\}\} \wedge x \in a \wedge y \in b]$ est équivalent à $X(z) \wedge z \in \mathcal{P}(\mathcal{P}(\cup\{a, b\}))$. Donc $a \times b$ est un ensemble par le schéma de séparation. □

Axiome de l'infini

§2.30 Un ensemble x est dit *inductif* lorsqu'il satisfait la formule :

$$\emptyset \in x \wedge \forall y(y \in x \Rightarrow y \cup \{y\} \in x))$$

§2.31 L'axiome de l'infini s'énonce ainsi :

> Il existe un ensemble qui contient l'ensemble vide et le singleton de chacun de ses éléments.

$$\exists x(\emptyset \in x \wedge \forall y(y \in x \Rightarrow y \cup \{y\} \in x))$$

Cet axiome est nécessaire pour pouvoir affirmer l'existence d'un ensemble contenant une infinité d'éléments. On verra dans le prochain chapitre que l'on peut le remplacer par un énoncé qui dit que la classe des entiers naturels **N** est un ensemble.

Axiome du choix - ZFC

§2.32 Il existe plusieurs versions de l'axiome du choix. Son introduction était très controversée, car il a des conséquences intuitivement étranges. Cependant, il est nécessaire pour montrer de nombreux résultats mathématiques. Nous en parlerons plus en détails dans le dernier chapitre. Ici, nous nous contenterons d'énoncer l'axiome du choix (C), mais nous verrons plus tard l'axiome du choix dénombrable (C_ω) et l'axiome du choix dépendant (C_d). La théorie de Zermelo-Fraenkel à laquelle on ajoute l'axiome du choix est appelée ZFC.

§2.33 Soit x un ensemble, et $\mathcal{P}(x)*$ l'ensemble de ses parties non vides. Une *fonction de choix* sur x est une application h de domaine $\mathcal{P}(x)*$ et d'image x telle que pour toute partie non vide y de x, on ait $h(y) \in y$.

On peut alors énoncer l'axiome du choix :

> Pour tout ensemble a, il existe une fonction de choix.

§2.34 Un autre énoncé, équivalent, est le suivant :

> Pour chaque ensemble x dont les éléments sont non vides et disjoints deux à deux, il existe un ensemble dont l'intersection avec chaque élément de x est un ensemble à un seul élément.

Ce que l'on peut écrire :

$$\forall x((\forall y(y \in x \Rightarrow y \neq \emptyset) \wedge \forall y \forall z((y \in x \wedge z \in x) \Rightarrow (y = z \vee y \cap z = \emptyset))) \\ \Rightarrow \exists a \forall y \exists w(y \in x \Rightarrow y \cap a = \{w\}))$$

Exercices

§2.35 **Exercice.** Si $(a, b) = (c, d)$, alors $a = c$ et $b = d$.

Solution. On distingue deux cas.

Si $a = b$, alors $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$. Par extensionalité, (c, d) n'a qu'un seule élément, égal à $\{a\}$, donc $\{c, d\} = \{c\} = \{a\}$, et on a donc $c = d = a$.

Si $a \neq b$, alors (a, b) a deux éléments $\{a\}$ et $\{a, b\}$, donc (c, d) a également deux éléments $\{c\}$ et $\{c, d\}$, donc $c \neq d$. Comme $\{a\}$ ne peut être égal à $\{c, d\}$ puisqu'ils n'ont pas le même nombre d'éléments, on en déduit que $\{a\} = \{c\}$ et $\{a, b\} = \{c, d\}$, donc $a = c$ et $b = d$. □

§2.36 **Exercice.** Soit $y = \{\{a, b, c\}, \{\{a, b\}\}, \{a\}, \{\{d\}\}\}$, quels sont les éléments de $\cup y$?

Solution. On a $\cup y = \{a, b, c, \{a, b\}, \{d\}\}$. □

§2.37 **Exercice.** Montrer que si a, b, c sont des ensembles, on peut définir un ensemble d dont les éléments sont exactment a,b et c. On notera $d = \{a, b, c\}$.

Solution. On définit $d = \cup\{\{a, b\}, \{c\}\}$. □

§2.38 **Exercice.** Soient a, b deux ensembles. Montrer que $a \times b$ est un ensemble.

Solution. Si $x \in a$ et $y \in b$, alors le couple (x, y) appartient à l'ensemble $\mathcal{P}(\mathcal{P}(a \cup b))$. Donc $X(z) = \exists x \exists y[z = \{\{x\}, \{x, y\}\} \wedge x \in a \wedge y \in b]$ est équivalent à $X(z) \wedge z \in \mathcal{P}(\mathcal{P}(\cup\{a, b\}))$. Donc $a \times b$ est un ensemble par le schéma de séparation. □

§2.39 **Exercice.** Montrer que l'axiome de la paire est une conséquence du schéma de substitution et de l'axiome des parties.

Solution. On a déjà montré qu'il existait un ensemble vide $\emptyset$. En utilisant l'axiome de la réunion, on en déduit l'existence de l'ensemble $\mathcal{P}(\emptyset)$. Cet ensemble contient un seul élément $\emptyset$, ce qui montre l'existence de $\{\emptyset\}$. Ce dernier ensemble a un seul élément, donc si $a \subset \{\emptyset\}$, on a $a = \emptyset$ ou $a = \{\emptyset\}$. Ce qui montre l'existence de l'ensemble $\{\emptyset, \{\emptyset\}\} = \mathcal{P}(\{\emptyset\})$. Maintenant, soient a, b des ensembles, on définit la relation $(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$ qui est clairement fonctionelle à un argument. En appliquant le schéma de substitution à cette relation et à l'ensemble $\{\emptyset, \{\emptyset\}\}$, on obtient l'existence d'un ensemble dont les éléments sont exactement a et b. □

§2.40 **Exercice.** Montrer que le schéma de séparation est une conséquence du schéma de remplacement.

Solution. Soit x un ensemble, et ϕ une formule, eventuellement avec des paramètres. On définit la classe de fonction

$$F = \{(x, x) \mid \phi(x)\}$$

Alors $F(x) = \{x \in x \mid \phi(x)\}$ est un ensemble par le schéma de remplacement. □

3 Ordinaux

Ordres

§3.1 **Definition** (Relation)**.** Une relation n-aire r sur un ensemble a est une classe de relation telle que $r \subset a^n$.

On en déduit les notions de relations d'équivalence, d'ordre strict et d'ordre large sur un ensemble. On dira d'une relation d'ordre r sur un ensemble a qu'elle est *totale* lorsqu'elle satisfait la formule

$$\forall x \in a \forall y \in a \ ((x, y) \in r) \vee (x = y) \vee ((y, x) \in r)$$

§3.2 **Definition.** Soit r une relation d'ordre sur un ensemble a, soit $b \subset a$ avec $b \neq \emptyset$, et soit $x \in a$. Alors :

- x est *un élément maximal* de b si $x \in b$ et $\forall y \in b, \neg(x < y)$;
- x est *un élément minimal* de b si $x \in b$ et $\forall y \in b, \neg(y < x)$;
- x est *le plus grand élément* de b si $x \in b$ et $\forall y \in b, y < x$;
- x est *le plus petit élément* de b si $x \in b$ et $\forall y \in b, x < y$;
- x est *une borne supérieure* de b si $\forall y \in b, y \leqslant x$;
- x est *une borne inférieure* de b si $\forall y \in b, x \leqslant y$;
- x est *le suprémum* de b si c'est la plus petite borne supérieure de b ;
- x est *l'infimum* de b si c'est la plus grande borne inférieure de b ;

§3.3 **Exercice.** Trouver :

1. Deux ensembles $b \subset a$ avec un ordre sur a tels que b possède plusieurs éléments maximaux
2. Deux ensembles $b \subset a$ avec un ordre sur a tels que b ne possède pas de plus grand élément
3. Deux ensembles $b \subset a$ avec un ordre sur a tels que b ne possède pas d'infimum

§3.4 **Definition** (Morphismes d'ordre)**.** Si $(a, <)$ et $(b, <)$ sont deux ensembles ordonnés, une fonction $f : a \to b$ est un *morphisme (d'ordre)* si elle préserve l'ordre, i.e. si $x < y \Rightarrow f(x) < f(y)$.

Un *isomorphisme* entre $(a, <)$ et $(b, <)$ est une fonction bijective $f : a \to b$ telle que f et f^{-1} sont des morphismes. Si $(a, <) = (b, <)$, on parle d'*automorphisme*.

§3.5 Si r est un ensemble et $<$ est un ordre strict sur r, on dira que r est un ensemble ordonné, et on écrira $(r, <)$. L'ordre strict $<$ défini un ordre large $\leqslant$ par $x \leqslant y \Leftrightarrow x = y \vee x < y$.

Bons Ordres

§3.6 **Definition** (Bon ordre)**.** Un ordre total strict $<$ sur un ensemble a est un *bon ordre* lorsque tout sous-ensemble non nul de P a un plus petit élément.

§3.7 **Lemme.** *Si $(r, <)$ est un ensemble bien ordonné, et $f : r \to r$ est une fonction croissante, alors $f(x) \geqslant x$ pour tout $x \in r$.*

Démonstration. On suppose que l'ensemble $a = \{x \in r \mid f(x) < x\}$ est non vide, et on pose z le plus petit élément de a. Alors $w = f(z)$ vérifie $f(w) < w$, ce qui est une contradiction. □

§3.8 **Corollaire.** *Le seul automorphisme d'un ensemble bien ordonné est l'identité.*

Démonstration. Pour tout x, $f(x) \geqslant x$ et $f^{-1}(x) \geqslant x$ donc $x \leqslant f(x) \leqslant x$. □

§3.9 **Exercice.** Montrer que si deux bons ordres $(r, <)$ et $(q, <)$ sont isomorphes, alors l'isomorphisme de $(r, <)$ sur $(q, <)$ est unique.

Solution. Soient f et g deux isomorphismes de $(r, <)$ sur $(q, <)$. Alors fg^{-1} est un automorphisme de $(q, <)$ et gf^{-1} est un automorphisme de $(r, <)$. On conclue par le corollaire §3.8. □

§3.10 **Definition** (Segment initial)**.** Si $(r, <)$ est un bon ordre et $a \in r$, alors $\{x \in r \mid \ x < a\}$ est un *segment initial* de r (défini par a).

§3.11 **Lemme.** *Un bon ordre ne peut être isomorphe à l'un de ses segments initiaux.*

Démonstration. Si $Dom(f) = \{x \mid x < a\}$, alors $f(a) < a$ ce qui contredit le lemme §3.7. □

§3.12 **Théorème.** *Si $(r, <)$ et $(q, <)$ sont deux bons ordres, alors on est nécessairement dans l'un des cas suivants :*
- *$r(, <)$ est isomorphe à $(q, <)$;*
- *$(r, <)$ est isomorphe à un segment initial de $(q, <)$;*
- *$(q, <)$ est isomorphe à un segment initial de $(r, <)$.*

Démonstration. Pour x un élement de r (resp. pour y un élément de q), on écrira $p(x)$ (resp. $q(y)$) le segment initial de p (resp. de q) défini par x (resp. par y). On définit

$$f = \{(x, y) \in p \times q \mid p(x) \cong q(y)\}$$

Utilisant le lemme §3.11, il est facile de voir que f est une fonction injective. Si h est un isomorphisme entre $p(x)$ et $q(y)$ et que $x' < x$, alors $p(x')$ et $q(h(x'))$ sont isomorphes. Il s'ensuit que f préserve l'ordre.

Si le domaine de f est égal à p, et l'image de f est égale à q, alors on est dans le premier cas.

Si $y_1 < y_2$ et $y_2 \in \mathrm{Im}(f)$, alors $y_1 \in \mathrm{Im}(f)$. Alors si $\mathrm{Im}(f) \neq q$ et y_0 est le plus petit élément de $q - \mathrm{Im}(f)$, on a $\mathrm{Im}(f) = q(y_0)$. On a alors

necessairement $\mathrm{Dom}(f) = p$, car sinon, en prenant x_0 le plus petit élément de $X - \mathrm{Dom}(f)$, on aurait $(x_0, y_0) \in f$. On est alors dans le second cas.

De manière similaire, si $\mathrm{Dom}(f) \neq q$, on montre que l'on est dans le troisième cas.

Le fait que l'on soit dans un seul de ces cas est une conséquence du lemme §3.11. □

Ordinaux

§3.13 L'idée est de définir les ordinaux de manière que

$$\alpha < \beta \text{ si et seulement si } \alpha \in \beta, \text{ et } \alpha = \{\beta \mid \beta < \alpha\}$$

§3.14 **Definition.** Un ensemble x est *transitif* si chaque élément de x est un sous-ensemble de x.

§3.15 **Definition.** Un ensemble est un *ordinal* si il est transitif et bien ordonné par $\in$ (en particulier, $\in$ est un ordre strict).

On écrira les ordinaux par des lettres grecques minuscules. La classe des ordinaux est notée Ord. On définit $\alpha < \beta$ si et seulement si $\alpha \in \beta$.

§3.16 **Lemme.** *On a les propriétés suivantes :*

1. *$\emptyset$ est un ordinal.*
2. *Si α est un ordinal et $\beta \in \alpha$, β est un ordinal.*
3. *Si $\alpha \neq \beta$ sont des ordinaux et $\alpha \subset \beta$, alors $\alpha \in \beta$.*
4. *Si α, β sont des ordinaux, alors soit $\alpha \subset \beta$, soit $\beta \subset \alpha$.*

Démonstration. Dans l'ordre :

1. Par définition.
2. Si α est un ordinal et $\beta \in \alpha$, alors $\beta \subset \alpha$. Donc β est un sous-ensemble d'un ensemble transitif et est par conséquent lui-même transitif. De plus, $\in$ est un bon ordre sur α donc aussi sur tout sous-ensemble de α, en particulier sur β.
3. Si $\alpha \subset \beta$, alors on pose γ le plus petit élément de $\beta - \alpha$. Comme α est transitif, α est le segment initial de β défini par γ. Donc $\alpha = \{\xi \mid \xi < \gamma\} = \gamma$, donc $\alpha \in \beta$.
4. On a clairement que $\beta \cap \alpha = \gamma$ est un ordinal. On a alors soit $\gamma = \alpha$ soit $\gamma = \beta$, par le point précédent. En effet, sinon on aurait $\gamma \in \gamma$, ce qui contredit la définition d'un ordinal ($\in$ est un ordre *strict*). □

§3.17 En utilisant le lemme §3.16, on peut montrer les propriétés suivantes des ordinaux :

- $<$ est un ordre total sur la classe Ord.
- Pour chaque α, $\alpha = \{\beta \mid \beta < \alpha\}$.

– Si C est une classe non vide d'ordinaux, alors $\bigcap C$ est un ordinal, $\bigcap C \in C$, et $\bigcap C = \inf C$.
– Si X est un ensemble non vide d'ordinaux, alors $\bigcup X$ est un ordinal, et $\bigcup X = \sup X$.
– Pour tout α, $\alpha \cup \{\alpha\}$ est un ordinal et $\alpha \cup \{\alpha\} = \inf\{\beta \mid \beta > \alpha\}$.

On définira $\alpha + 1 = \alpha \cup \{\alpha\}$, le successeur de α.

§3.18 **Exercice.** Montrer que Ord n'est pas un ensemble.

§3.19 **Théorème.** *Tout ensemble bien ordonné est isomorphe à un unique ordinal.*

Démonstration. L'unicité est une conséquence du lemme §3.11. Etant donné un ensemble bien ordonné r, on trouve un isomorphisme comme suit :

On définit $F(x) = \alpha$ si α est isomorphe au segment initial de r défini par x. Si un tel α existe, il est unique. En utilisant l'axiome de remplacement, $F(r)$ est un ensemble. Pour tout $x \in r$, un tel α existe (sinon, on considère le plus petit x pour lequel il n'existe pas de tel α et cela nous mène à une contradiction). Si γ est le plus petit ordinal tel que $\gamma \notin F(r)$, alors $F(r) = \gamma$, et on a un isomorphisme entre r et γ. □

§3.20 Si $\alpha = \beta + 1$, on dit que α est un ordinal successeur. Si ce n'est pas un ordinal successeur, on a $\alpha = \sup\{\beta \mid \beta < \alpha\} = \bigcup \alpha$, et on dit que α est un ordinal limite. On considèrera aussi $0 = \emptyset$ comme un ordinal limite, et on définit $\sup \emptyset = 0$.

§3.21 **Definition** (Ordinaux finis)**.** Un ordinal α est dit *fini* si tout ordinal $\beta \leqslant \alpha$, avec $\beta \neq 0$, a un predécesseur.

§3.22 **Proposition** (Principe de récurrence)**.** *Soit P une classe telle que $0 \in P$ et pour tout ordinal fini α on ait $\alpha \in P \Rightarrow \alpha \cup \{\alpha\} \in P$. Alors P contient tous les ordinaux finis.*

Démonstration. Supposons qu'il y ait au moins un ordinal fini qui ne soit pas dans P. Soit β le plus petit ordinal fini qui n'est pas dans P. Dans ce cas, $\beta \neq 0$ car $0 \in P$. Donc $\beta = \alpha \cup \{\alpha\}$ pour un ordinal α. Comme $\alpha < \beta$, on a $\alpha \in P$ par définition de β, et donc $\beta \in P$ par hypothèse, ce qui est une contradiction. □

§3.23 **Axiome de l'infini.** On a vu l'axiome de l'infini dans la première section §2.31. On va montrer que cet axiome est équivalent à l'énoncé qui affirme l'existence d'un ordinal infini.

§3.24 **Proposition.** *Les énoncés suivants sont équivalents :*

1. *il existe un ensemble inductif (c'est l'axiome de l'infini) ;*
2. *il existe un ordinal limite.*
3. *il existe un ordinal non fini ;*
4. *la collection des ordinaux finis est un ensemble ;*

Démonstration. On montre les implications :

1⇒ 2 Soit a un ensemble inductif, et soit α le plus petit ordinal qui n'est pas dans a. Alors $\alpha \neq 0$ et n'a pas de prédécesseur : si $\alpha = \beta \cup \{\beta\}$, alors $\beta < \alpha$ donc $\beta \in a$, et finalement $\alpha = \beta \cup \{\beta\} \in a$ car a est inductif, ce qui est une contradiction. Donc il existe un ordinal limite.

2⇒ 3 Si α est un ordinal limite, alors il n'est pas fini.

3⇒ §3.27 On désigne par ω le premier ordinal non fini. Alors ω est l'ensemble des ordinaux finis : si α est un ordinal fini, on ne peut avoir $\omega \leqslant \alpha$ sinon ω serait fini, donc $\alpha < \omega$, donc $\alpha \in \omega$; d'autre part, si $\gamma \in \omega$, alors $\gamma < \omega$ et γ est fini par définition de ω.

§3.27⇒1 Soit ω l'ensemble des ordinaux finis. On a $0 \in \omega$ et si $\gamma \in \omega$, cela signifie que γ est un ordinal fini, donc $\gamma \cup \{\gamma\}$ aussi, ce qui signifie que $\gamma \cup \{\gamma\} \in \omega$. En d'autres termes, γ est un ensemble inductif. □

§3.25 **Definition** (Entiers Naturels)**.** On définit le plus petit ordinal limite non nul par ω ou $\mathbf{N}$. Les ordinaux plus petits que ω sont appelés les *ordinaux finis*, ou *entiers naturels*.

$$0 = \emptyset, \quad 1 = 0 + 1, \quad 2 = 1 + 1, \quad 3 = 2 + 1, \quad \text{etc.}$$

Un ensemble x est dit *fini* s'il existe une fonction injective de x sur un élément $n \in \omega$. Un ensemble infini est un ensemble qui n'est pas fini.

§3.26 **Definition** (Axiomatisation des entiers naturels)**.** On donne généralement l'axiomatisation suivante des entiers naturels, sur le langage $\{=, s, 0\}$ où s est une fonction unaire et 0 est une constante :

1. $\forall n, (n \neq 0 \Rightarrow \exists m, n = s(m))$
2. $\forall n, \forall m, (s(m) = s(n) \Rightarrow m = n)$
3. pour toute formule $\phi(x, y_1, \ldots, y_n)$ du langage, l'axiome

$$\forall \vec{y}, ((\phi(0, \vec{y}) \wedge (\forall n(\phi(n, \vec{y}) \Rightarrow \phi(s(n), \vec{y})))) \Rightarrow \forall x(\phi(x, \vec{y}))$$

§3.27 **Proposition.** *L'ordinal ω, dans lequel on interprète le successeur par $x \mapsto x \cup \{x\}$ et la constante 0 par $\emptyset$ est un modèle de la théorie axiomatique des entiers.*

Démonstration. Le premier axiome est bien satisfait puisque par définition un ordinal fini non nul est nécessairement le successeur d'un autre ordinal fini. Le second axiome est également clairement satisfait. Le schéma d'axiome de récurrence est lui aussi satisfait, c'est la proposition §3.22. □

Induction, Recursion

§3.28 **Théorème** (Induction transfinie)**.** *Soit C une classe d'ordinaux vérifiant :*

– $0 \in C$ *;*

– *Si $\alpha \in C$, alors $\alpha + 1 \in C$;*
– *Si α est un ordinal limite non nul, et $\beta \in C$ pour tout $\beta < \alpha$, alors $\alpha \in C$;*

Alors C est la classe de tous les ordinaux.

Démonstration. Supposons que ce n'est pas le cas, et posons α le plus petit ordinal $\alpha \notin C$. En appliquant l'une des trois propriétés, on arrive à une contradiction. □

§3.29 Une fonction dont le domaine est ω est appelée une *suite*. On écrira les suites

$$\langle a_n : n < \omega \rangle$$

Une *suite transfinie* est une fonction dont le domaine est un ordinal :

$$\langle a_\xi : \xi < \alpha \rangle$$

Une suite de domaine α, α un ordinal, sera appelée un α-suite.

On appelera une *suite ordinale* une (classe de) fonction dont le domaine est Ord.

§3.30 **Definition.** Soit $\alpha > 0$ un ordinal limite, et $\langle \gamma_\xi : \xi < \alpha \rangle$ une suite d'ordinaux non décroissante ($\xi < \eta \Rightarrow \gamma_\xi \leqslant \gamma_\eta$). On définit la *limite* de la suite par

$$\lim_{\xi \to \alpha} \gamma_\xi = \sup\{\gamma_\xi : \xi < \alpha\}$$

Une suite d'ordinaux est dite *normale* lorsqu'elle est croissante et *continue*, i.e. pour tout ordinal limite α, $\gamma_\alpha = \lim_{\xi \to \alpha} \gamma_\xi$.

§3.31 **Théorème** (Récurrence transfinie)**.** *Soit G une (classe de) fonction sur $\mathcal{U}$. Alors il existe une unique fonction F de domaine Ord telle que, pour tout α :*

$$F(\alpha) = G(F\restriction\alpha)$$

Démonstration. Posons

$$\begin{aligned} F(\alpha) = x \quad \Leftrightarrow \quad & \exists \langle a_\xi : \xi < \alpha \rangle \text{ tel que :} \\ & \forall \xi < \alpha, \alpha_\xi = G(\langle a_\eta : \eta < \xi \rangle) \qquad (2) \\ & x = G(\langle a_\xi : \xi < \alpha \rangle) \qquad (3) \end{aligned}$$

Pour tout α, s'il existe une α-suite satisfaisant 2, alors cette suite est unique : si l'on prends deux α-suites $\langle a_\xi : \xi < \alpha \rangle$ et $\langle b_\xi : \xi < \alpha \rangle$ qui satisfont cette equation 2, alors on montre $a_\xi = b_\xi$ par induction sur ξ. Donc $F(\alpha)$ est défini par l'equation 3 et unique, donc F est une (classe de) fonction. On a, à nouveau par induction, que pour chaque α il existe une α-suite satisfaisant 2 (pour les ordinaux limites, on utilise le schéma de remplacement pour

obtenir l'α-suite comme l'union des ξ-suites, pour $\xi < \alpha$). Donc F est de domaine Ord, et satisfait

$$F(\alpha) = G(F\restriction\alpha)$$

L'unicité de F se montre par induction. □

Arithmétique Ordinale

§3.32 **Definition.** Pour tout ordinal α, on défini la fonction $\xi \mapsto \alpha+\xi$ en utilisant le théorème de récurrence transfinie :

- $\alpha + 0 = \alpha$;
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ pour tout $\beta > 0$;
- $\alpha + \beta = \lim_{\xi\to\beta}(\alpha + \xi)$ pour tout ordinal limite β.

§3.33 **Proposition.** *L'addition est associative, mais non commutative.*

Démonstration. **En exercice.** Pour voir qu'elle n'est pas commutative, prenons $\omega + 1$ et $1 + \omega$.

Pour montrer qu'elle est associative, on procède par induction sur γ pour montrer que pour tous α, β, γ,

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$

□

§3.34 **Definition.** Soient $(r, <)$ et $(q, <)$ deux ensembles bien ordonnés. On définit la somme de $(r, <)$ et $(q, <)$ comme l'ensemble $p \uplus q = p \times \{1\} \cup q \times \{2\}$ union disjointe de p et q, muni de l'ordre :

$$(x, i) < (y, j) \Leftrightarrow (i < j) \vee (i = j \wedge x < y)$$

§3.35 **Proposition.** *Soient α, β des ordinaux. La somme de $(\alpha, \in)$ et $(\beta, \in)$ est isomorphe à l'ordinal $\alpha + \beta$.*

Démonstration. Par induction. □

§3.36 **Definition.** Pour tout ordinal α, on défini la fonction $\xi \mapsto \alpha.\xi$ en utilisant le théorème de récurrence transfinie :

- $\alpha.0 = 0$;
- $\alpha.(\beta + 1) = \alpha.\beta + \alpha$ pour tout $\beta > 0$;
- $\alpha.\beta = \lim_{\xi\to\beta}(\alpha.\xi)$ pour tout ordinal limite β.

§3.37 **Proposition.** *La multiplication est associative, mais non commutative.*

Démonstration. **En exercice.** Pour voir qu'elle n'est pas commutative, prenons $\omega.2$ et $2.\omega$.

Pour montrer qu'elle est associative, on procède par induction sur γ pour montrer que pour tous α, β, γ,

$$\alpha.(\beta.\gamma) = (\alpha.\beta).\gamma$$

□

§3.38 **Definition.** Soient $(r, <)$ et $(q, <)$ deux ensembles bien ordonnés. On définit le produit de $(r, <)$ et $(q, <)$ comme l'ensemble $p \times q$ muni de l'ordre :

$$(x, y) < (x', y') \Leftrightarrow (y < y') \vee (y = y' \wedge x < x')$$

§3.39 **Proposition.** *Soient α, β des ordinaux. Le produit de $(\alpha, \in)$ et $(\beta, \in)$ est isomorphe à l'ordinal $\alpha.\beta$.*

Démonstration. Par induction. □

§3.40 **Definition.** Pour tout ordinal α, on définit la fonction $\xi \mapsto \alpha^\xi$ en utilisant le théorème de récurrence transfinie :

- $\alpha^0 = 1$;
- $\alpha^{\beta+1} = \alpha^\beta.\alpha$ pour tout $\beta > 0$;
- $\alpha^\beta = \lim_{\xi \to \beta}(\alpha^\xi)$ pour tout ordinal limite β.

Exercices

§3.41 **Exercice.** Montrer que la relation $(r, <)$ est isomorphe à $(q, <)$ est une relation d'équivalence sur les ensembles ordonnés.

§3.42 **Exercice.** Montrer que α est un ordinal limite si et seulement si $\beta < \alpha$ implique $\beta + 1 < \alpha$.

§3.43 **Exercice.** Montrer que si $(r, <)$ est un ensemble bien ordonné, alors il n'existe pas de suite $\langle a_n : n \in \omega \rangle$ d'éléments de r telle que $a_0 > a_1 > a_2 > \dots$.

§3.44 **Exercice.** Montrer que pour tout ordinal α, il existe un ordinal β limite tel que $\beta > \alpha$.

§3.45 **Exercice.** Montrer que tout suite normale $\langle \alpha_\gamma : \gamma \in \mathrm{Ord}, \alpha_\gamma \in \mathrm{Ord} \rangle$ a des points fixes arbitrairement grands, i.e. pour tout $\xi \in \mathrm{Ord}$, il existe un ordinal $\gamma > \xi$ tel que $\alpha_\gamma = \gamma$.

§3.46 **Exercice.** Montrer que pour tous ordinaux α, β, γ :

1. $\alpha.(\beta + \gamma) = \alpha.\beta + \alpha.\gamma$
2. $\alpha^{\beta+\gamma} = \alpha^\beta.\alpha^\gamma$
3. $(\alpha^\beta)^\gamma = \alpha^{\beta.\gamma}$

§3.47 **Exercice.** Montrer que $(\omega + 1).2 \neq \omega.2 + 1.2$, et que $(\omega.2)^2 \neq \omega^2.2^2$.

§3.48 **Exercice.** Montrer que si $\alpha < \beta$, alors $\alpha + \gamma \leqslant \beta + \gamma$, $\alpha.\gamma \leqslant \beta.\gamma$ et $\alpha^\gamma \leqslant \beta^\gamma$.

§3.49 **Exercice.** Montrer que si $\alpha > 0$, et γ est un ordinal, il existe un unique β et un unique $\rho < \alpha$ tel que $\gamma = \alpha.\beta + \rho$.

§3.50 **Exercice** (Théorème de forme normale de Cantor)**.** Tout ordinal $\alpha > 0$ peut être représenté de manière unique sous la forme :

$$\alpha = \omega^{\beta_1}.k_1 + \omega^{\beta_2}.k_2 + \dots + \omega^{\beta_n}.k_n$$

où $n \geqslant 1$ est un entier naturel, $\alpha \geqslant \beta_1 > \beta_2 > \dots > \beta_n$ et $k_1, \dots, k_n$ sont des entiers.

§3.51 **Exercice.** Existe-t-il un ordinal ϵ tel que $\omega^\epsilon = \epsilon$?

4 Cardinaux

On notera A^B l'ensemble des fonctions de B dans A.

Cardinalité

§4.1 **Definition.** Etant donné deux ensembles A et B, on dira qu'ils sont équipotents s'il existe une bijection de A sur B. On notera $|A| = |B|$, et $|A|, |B|$ sont le cardinal de A et B.

§4.2 **Definition.** On définit un ordre (large) sur les cardinaux d'ensembles par $|A| \leqslant |B|$ si et seulement si il existe une injection de A dans B. Il est clair que cette relation est transitive et réflexive. Le théorème §4.4 montrera qu'il s'agit bien d'un ordre, et le fait que ce soit un ordre total est une conséquence de l'axiome du choix.

§4.3 **Théorème** (Cantor)**.** *Pour tout ensemble x, $|x| < |\mathcal{P}(x)|$.*

Démonstration. Soit f une fonction de x sur $\mathcal{P}(x)$. L'ensemble

$$y = \{a \in x \mid x \notin f(x)\}$$

n'est pas dans le domaine de $f(x)$: si $z \in x$ est tel que $f(z) = y$, alors $z \in y$ si et seulement si $z \notin y$, une contradiction. Alors f n'est pas une fonction surjective. Donc $|x| \neq |\mathcal{P}(x)|$.

Comme la fonction $x \mapsto \{x\}$ est une injection de x sur $\mathcal{P}(x)$, on a $|x| \leqslant |\mathcal{P}(x)|$, donc $|x| < |\mathcal{P}(x)|$. □

§4.4 **Théorème** (Cantor-Bernstein)**.** *Si $|a| \leqslant |b|$ et $|b| \leqslant |a|$, alors $|a| = |b|$.*

Démonstration. Si $f_1 : a \to b$ et $f_2 : b \to a$ sont injectives, alors en posant $b' = f_2(b)$ et $a_1 = f_2(f_1(a))$, on a $a_1 \subset b' \subset a$, et $|a_1| = |a|$. On va donc supposer que $a_1 \subset b \subset a$ et que f est une fonction injective de a sur a_1. On va montrer que $|a| = |b|$.

On définit, par induction sur $n \in \omega$:

$$\begin{array}{ll} a_0 = a & a_{n+1} = f(a_n) \\ b_0 = b & b_{n+1} = f(b_n) \end{array}$$

Soit g la fonction sur a définie par :

$$g(x) = \begin{cases} f(x) & \text{si } x \in a_n - b_n \text{ pour un } n \in \omega \\ x & \text{sinon} \end{cases}$$

Alors g est une fonction bijective de a sur b. Donc $|a| = |b|$. □

§4.5 **Théorème.** *L'axiome du choix est équivalent à l'énoncé suivant :*

Tout ensemble est bien ordonnable.

Démonstration. On montre tout d'abord que l'axiome du choix implique l'existence d'un bon ordre sur tout ensemble. Soit X un ensemble, et f une fonction de choix $\mathcal{P}(X) - \{\emptyset\} \to X$. On définit une suite $\langle x_\xi \rangle$ de la manière suivante :

$$\begin{aligned} x_0 &= f(X) \\ x_\xi &= f(X - \{x_\gamma \mid \gamma < \xi\}) \end{aligned}$$

Cette suite définit un bon ordre sur X (c'est une bijection sur un ordinal).

Inversement, soit X un ensemble. X étant bien ordonnable, on choisit un bon ordre sur X. On peut alors définir une fonction de choix en posant, pour toute partie $A \neq \emptyset$ de X, $f(A)$ comme le plus petit élément de A. □

§4.6 **Lemme.** *Si* $|a| = \kappa$*, alors* $|\mathcal{P}(a)| = 2^\kappa = \{\emptyset, \{\emptyset\}\}^\kappa$.

Démonstration. Pour tout $x \subset a$, soit χ_x la fonction :

$$\chi_x(y) = \begin{cases} 1 & \text{si } y \in x \\ 0 & \text{si } y \in a - x \end{cases}$$

La fonction $f : x \mapsto \chi_x$ est une bijection entre $\mathcal{P}(a)$ et $\{0,1\}^a$. □

Alephs

§4.7 **Definition.** Le cardinal d'un ensemble r est le plus petit ordinal α en bijection avec r, on notera $|r| = \alpha$. Un cardinal est un ordinal qui n'est en bijection avec aucun ordinal plus petit.

§4.8 **Proposition.** *Les ordinaux finis sont des cardinaux.*

Démonstration. On montre le résultat par induction. Il est clair que 0 est un cardinal. Supposons alors que α soit un ordinal fini qui est un cardinal et que $\alpha+1$ n'en soit pas un. Il existe alors un ordinal $\gamma < \alpha+1$ et une bijection f de $\alpha + 1$ sur γ. On a alors que $\gamma \neq 0$ car $\alpha + 1 \neq \emptyset$. Donc $\gamma = \beta + 1$, et comme $\gamma < \alpha + 1$ on a $\beta < \alpha$.

Si $f(\alpha) = \beta$, alors $f\restriction\alpha$ est une bijection de α sur β, ce qui est impossible puisque α est un cardinal. Donc $f(\alpha) = \xi \neq \beta$; comme f est bijective, il existe $\eta \in \alpha + 1$ tel que $f(\eta) = \beta$; comme $\eta \neq \alpha$, $\eta \in \alpha$. On définit une fonction g de domaine α en posant $g(x) = f(x)$ pour tout $x \neq \eta, x \in \alpha$ et $g(\eta) = \xi$. On a ainsi définit une bijection de α sur β, ce qui est impossible. □

§4.9 **Lemme.** *On montre que :*

- *Pour tout α il existe un cardinal plus grand que α.*
- *Si x est un ensemble de cardinaux, alors* $\sup x$ *est un cardinal.*

Démonstration. Dans l'ordre :

- Pour tout ensemble x, on pose $h(x)$ le plus petit ordinal α tel qu'il n'existe pas d'injection de α dans x. On doit montrer que cette fonction est bien définie. Par le schéma de séparation, on peut définir l'ensemble des sous-ensembles de x qui sont bien ordonnables. Donc la classe des ordinaux β tels qu'il existe une injection de β sur x est un ensemble, et par conséquent $h(x)$ est bien défini.
  Si γ est un ordinal, alors $|\alpha| < |h(\alpha)|$ par définition de $h(\alpha)$.
- Soit x un ensemble de cardinaux, et $\alpha = \sup x$. Si f est une fonction injective de α dans un ordinal $\beta < \alpha$, on prends $\kappa \in x$ tel que $\beta < \kappa \leqslant \alpha$. Alors $|\kappa| = |\{f(\xi) \mid \xi < \kappa\}| \leqslant \beta$, ce qui est une contradiction. Donc α est un cardinal.

□

§4.10 En utilisant le lemme précédent, on peut définir la hiérarchie des Alephs. En écrivant κ^+ le plus petit cardinal strictement supérieur à κ, on pose :

$$\begin{array}{rcccl} \aleph_0 & = & \omega_0 & = & \omega \\ \aleph_{\alpha+1} & = & \omega_{\alpha+1} & = & \aleph_\alpha^+ \\ \aleph_\beta & = & \omega_\beta & = & \sup\{\omega_\beta \mid \beta < \alpha\} \text{ pour } \beta \text{ limite} \end{array}$$

Un peu d'arithmétique cardinale

§4.11 On définit les opérations arithmétiques sur la classe des cardinaux :

$$\begin{array}{rcll} \kappa + \lambda & = & |A \cup B| & \text{où } |A| = \kappa,\ |B| = \lambda, \text{ et } A, B \text{ sont disjoints} \\ \kappa.\lambda & = & |A \times B| & \text{où } |A| = \kappa,\ |B| = \lambda \\ \kappa^\lambda & = & |A^B| & \text{où } |A| = \kappa,\ |B| = \lambda \end{array}$$

§4.12 **Proposition.** *On montre alors que :*

1. *L'addition et la multiplication sont commutatives, associatives et distributives ;*
2. $(\kappa.\lambda)^\mu = \kappa^\mu.\lambda^\mu$ *;*
3. $\kappa^{\lambda+\mu} = \kappa^\lambda.\kappa^\mu$ *;*
4. $(\kappa^\lambda)^\mu = \kappa^{\lambda.\mu}$ *;*

Démonstration. Exercice. □

§4.13 On peut définir un bon ordre sur la classe Ord × Ord. On définit :

$$(\alpha, \beta) < (\gamma, \delta) \Leftrightarrow \begin{cases} \text{soit} & \max\{\alpha, \beta\} < \max\{\gamma, \delta\} \\ \text{soit} & \max\{\alpha, \beta\} = \max\{\gamma, \delta\} \wedge \alpha < \gamma \\ \text{soit} & \max\{\alpha, \beta\} = \max\{\gamma, \delta\} \wedge \alpha = \gamma \wedge \beta < \delta \end{cases}$$

Cette relation est un ordre total sur Ord × Ord. Tout segment S_ξ avec $\xi = (\alpha_0, \beta_0)$ est un ensemble : si $\gamma_0 = \max\{\alpha_0, \beta_0\}$, la collection S_ξ des couples $(\alpha, \beta) < (\alpha_0, \beta_0)$ est contenue dans l'ensemble $(\gamma_0 + 1)^2$.

§4.14 De plus, si x est un ensemble non vide dont tous les éléments sont dans Ord^2, l'ensemble des $\max\{\alpha,\beta\}$ pour $(\alpha,\beta)\in x$ a un plus petit élément γ_0 ; l'ensemble des α tels qu'il existe β avec $(\alpha,\beta)\in x$ et $\max\{\alpha,\beta\}=\gamma_0$ a un plus petit élément α_0 ; l'ensemble des β tels que $\max\{\alpha_0,\beta\}=\gamma_0$ et $(\alpha_0,\beta)\in x$ a un plus petit élément β_0. Il est alors clair que (α_0,β_0) est le plus petit élément de x, donc l'ordre que nous avons défini est bien un bon ordre.

§4.15 Comme Ord^2 est une collection bien ordonnée qui n'est pas un ensemble, il existe une relation fonctionnelle J qui établit un isomorphisme entre Ord^2 et Ord et définie par :

$$J(\alpha,\beta)= \text{ l'ordinal isomorphe à } \{(\xi,\eta)\mid(\xi,\eta)<(\alpha,\beta)\}$$

En posant $\gamma(\alpha)=J(0,\alpha)$ (on peut remarquer que $\alpha\times\alpha$ est le segment initial définit par $(0,\alpha)$) on a $\gamma(\omega)=\omega$. La fonction γ étant croissante, on a donc $\gamma(\alpha)\geqslant\alpha$ pour tout α. Comme γ est de plus continue donc $\gamma(\alpha)=\alpha$ pour des ordinaux α arbitrairement grands.

§4.16 **Proposition.** *Pour tout ordinal α, $\aleph_\alpha^2=\aleph_\alpha$.*

Preuve du Jech (sans AC). On considère la bijection J de de Ord^2 dans Ord. On va montrer que $J(\omega_\alpha\times\omega_\alpha)=\omega_\alpha$. C'est vrai vrai pour $\alpha=0$. On fixe α le plus petit ordinal tel que $J(\omega_\alpha\times\omega_\alpha)\neq\omega_\alpha$. Soient $\beta,\gamma<\omega_\alpha$ tels que $J(\beta,\gamma)=\omega_\alpha$. On choisit $\delta>\beta$ et $\delta>\gamma$. Comme $\delta\times\delta$ est un segment initial de $\mathrm{Ord}\times\mathrm{Ord}$ et contient (β,γ), on a $\omega_\alpha\subset J(\delta\times\delta)$, donc $|\delta\times\delta|\geqslant\aleph_\alpha$. Cependant, $|\delta\times\delta|=|\delta||\delta|=|\delta|<\aleph_\alpha$ par la minimalité de α, ce qui est une contradiction. □

Preuve du Krivine (avec AC). Soit ρ le plus petit ordinal tel que $\aleph_\rho^2\neq\aleph_\rho$ s'il en existe. Il est clair que $\aleph_\rho^2\geqslant\aleph_\rho$ donc il suffit de montrer que $\aleph_\rho^2\leqslant\aleph_\rho$. Or J restreinte à $\aleph_\rho\times\aleph_\rho$ est injective, et il suffit donc de prouver que $J(\alpha,\beta)\in\aleph_\rho$ pour $\alpha,\beta\in\aleph_\rho$. Comme $J(\alpha,\beta)$ est l'ensemble des ordinaux strictement inférieurs à $J(\alpha,\beta)$, c'est l'image par J de l'ensemble des $(\alpha',\beta')<(\alpha,\beta)$. Or, si $\gamma=\max\{\alpha,\beta\}$, l'ensemble de ces couples est contenu dans $(\gamma+1)^2$. Son cardinal est donc inférieur ou égal à $|(\gamma+1)^2|$. Comme $\gamma<\aleph_\rho$, on a $\gamma+1<\aleph_\rho$ et donc, par définition de ρ, ou bien $\gamma+1$ est fini, ou bien $|(\gamma+1)^2|=|\gamma+1|<\aleph_\rho$. Dans les deux cas, on a $|J(\alpha,\beta)|<\aleph_\rho$, et donc $J(\alpha,\beta)<\aleph_\rho$. □

§4.17 **Corollaire.**

$$\aleph_\alpha+\aleph_\beta=\aleph_\alpha\aleph_\beta=\max\{\aleph_\alpha,\aleph_\beta\}$$

Exercices

§4.18 **Exercice.** Montrer que :

1. L'addition et la multiplication sont commutatives, associatives et distributives ;
2. $(\kappa.\lambda)^\mu = \kappa^\mu.\lambda^\mu$;
3. $\kappa^{\lambda+\mu} = \kappa^\lambda.\kappa^\mu$;
4. $(\kappa^\lambda)^\mu = \kappa^{\lambda.\mu}$;

§4.19 **Exercice.**
On considère la théorie ZFC_{fin} qui est la théorie ZF (schéma de remplacement, axiome des parties, axiome de la réunion, axiome d'extensionalité) avec l'axiome du choix et l'axiome de fondation (voir le premier devoir). Le but de l'exercice est de donner un modèle de ZFC_{fin} qui ne satisfait pas l'axiome de l'infini.

Pour tout entier q, on définit $[q]$ comme l'unique ensemble d'entiers $\{p_1, \ldots, p_n\}$ tel que $q = \sum_{i=1}^{n} 2^{p_i}$ (penser à l'écriture de q en base 2).

On définit la relation binaire E sur $\mathbb{N}$ par :

$$pEq \Leftrightarrow p \in [q]$$

Montrer que :

1. la structure $(\mathbf{N}, E)$ satisfait l'axiome d'extensionnalité ;
2. pour tout entier q, l'ensemble $[q]$ des E-éléments de q est fini ;
3. pour tout ensemble fini d'entiers $\{p_1, \ldots, p_n\}$, il existe un unique entier q tel que $[q] = \{p_1, \ldots, p_n\}$;
4. la structure $(\mathbf{N}, E)$ est un modèle de ZFC_{fin}, et que l'axiome de l'infini n'est pas satisfait dans cette structure.

§4.20 **Exercice.**
Cet exercice prolonge l'exercice précédent pour montrer l'indépendance de l'axiome de fondation dans le système ZFC^-_{fin}=$\mathrm{ZFC}_{fin} - \{AF\}$. On montre plus précisément l'existence d'un modèle de ZFC^-_{fin}+AF et d'un modèle de ZFC^-_{fin}+$\neg$AF.

Soit ϕ une bijection entre $\mathbf{N}$ et les parties finies de $\mathbf{N}$, et soit $\in_\phi$ la relation binaire définie par $x \in_\phi y$ si et seulement si $x \in \phi(y)$.

1. Montrer que la structure $U_\phi = (\mathbf{N}, \in_\phi)$ est un modèle de ZFC^-_{fin}.
2. Montrer que, si pour tous $p, q \in \mathbf{N}$, on a $p \in_\phi q$ implique $p < q$ pour l'ordre usuel de $\mathbf{N}$, alors U_ϕ satisfait l'axiome de fondation.
3. Donner une bijection ϕ tlele que U_ϕ satisfasse $\neg$AF.

§4.21 **Exercice.**
Calculer les expressions suivantes, en utilisant l'arithmétique ordinale :

1. $3 + \omega$
2. $\omega + 3$
3. $\omega + 15 + \omega + 9 + 3 + \omega$
4. $\omega.3$
5. $(\omega.3).(\omega.5)$
6. $\omega^2.\omega$
7. $\omega.\omega^2$
8. $(\omega + 3).4$
9. $4.(\omega + 3)$
10. $(\omega + 3).\omega$
11. $\omega.(\omega + 3)$
12. $10.\omega.7.3.\omega$
13. $\omega^3.\omega^2.9 + 7.\omega^4 + 3.(\omega + 2)$
14. $2.\omega^3.3 + \omega^6 + (\omega + 3).12$

Même question en utilisant l'arithmétique cardinale.

§4.22 **Exercice.**

1. Combien y-a-t-il de bons ordres sur ω ?
2. Combien y-a-t-il de bons ordres sur ω, "à isomorphisme près" ?
3. Mêmes questions pour ω_1.
4. Quel est le cardinal de l'ensemble $\{R$: il existe un $n \in \mathbf{N}$ tel que R est un bon ordre sur $\aleph_n\}$ à isomorphisme près ?

5 Construire les réels

Les entiers naturels

§5.1 Nous avons montré que les ordinaux (cardinaux) finis satisfont l'axiomatisation des entiers naturels (paragraphe §3.26). De plus, les opérations d'addition et de multiplication sont associatives. Nous allons montrer que ces opérations sont commutatives sur les ordinaux finis.

§5.2 **Proposition.** *Soient α, β deux ordinaux finis. On a $\alpha + \beta = \beta + \alpha$.*

Démonstration. □

§5.3 **Proposition.** *Soient α, β deux ordinaux finis. On a $\alpha.\beta = \beta.\alpha$.*

Démonstration. □

§5.4 **Definition** (Arithmétique de Peano)**.** L'axiomatisation de l'arithmétique classique (arithmétique de Peano) est la théorie du premier ordre sur le langage $\{=, s, +, \times, 0\}$ constituée des axiomes suivants :

1. $\forall n(n \neq 0 \Leftrightarrow \exists m(n = s(m)))$
2. $\forall n \forall m(s(m) = s(n) \Rightarrow m = n)$
3. $\forall n(n + 0 = n)$
4. $\forall n \forall m(n + s(m) = s(n + m))$
5. $\forall n(n \times 0 = 0)$
6. $\forall n \forall m(n \times s(m) = n \times m + n$
7. Pour toute formule $\phi(x, \vec{y})$, l'axiome

$$\forall \vec{y}((\phi(0, \vec{y}) \wedge (\forall n(\phi(n, \vec{y}) \Rightarrow \phi(s(n), \vec{y})))) \Rightarrow \forall x(\phi(x, \vec{y}))$$

§5.5 **Proposition.** *Le modèle $(\omega, =, s : x \mapsto x \cup \{x\}, +, \times, \emptyset)$ avec $+, \times$ les opérations d'addition et multiplication cardinales est un modèle de l'arithmétique de Peano.*

Démonstration. La proposition paragraphe §3.27 montre que les deux premiers axiomes et le schéma de récurrence sont satisfaits dans cette structure. Les axiomes $3, 4$ et $5, 6$ sont satisfaits par définition (de l'addition pour les premiers, de la multiplication pour les seconds). □

Les entiers relatifs

§5.6 Les entiers naturels ne forment pas un ensemble satisfaisant par rapport aux opérations arithmétiques. En effet, il est impossible de définir la soustraction de deux entiers naturels quelconques, et il en est de même de la division. Nous allons donc commencer par étendre les entiers naturels de manière à obtenir un groupe (i.e. tous les inverses par rapport à l'opération d'addition) pour obtenir les entiers relatifs. Nous verrons dans la section suivante comment ajouter les inverses pour la multiplication et ainsi construire l'ensemble des rationnels.

§5.7 **Definition.** On définit une relation $\sim_{\mathbf{Z}}$ sur $\omega \times \omega$ par

$$(x, x') \sim_{\mathbf{Z}} (y, y') \Leftrightarrow x + y' = y + x'$$

§5.8 **Lemme.** *Soient a, b, k des entiers naturels. Si $a + k = b + k$, alors $a = b$.*

Démonstration. On prouve le résultat par induction sur k. Si $k = 0$, alors par définition $a = a + 0 = b + 0 = b$. En supposant le résultat vrai pour un entier k, on a $(a + k) + 1 = a + (k + 1) = b + (k + 1) = (b + k) + 1$, donc $a + k = b + k$, et en utilisant l'hypothèse d'induction on a $a = b$. □

§5.9 **Proposition.** *La relation $\sim_{\mathbf{Z}}$ est une relation d'équivalence.*

Démonstration. La réflexivité est claire, ainsi que la symétrie. Supposons que $(x, x') \sim_{\mathbf{Z}} (y, y')$ et $(y, y') \sim_{\mathbf{Z}} (z, z')$ pour des éléments x, x', y, y', z, z' de ω. On a alors :

$$x + z' + y' = x' + y + z' = x' + z + y'$$

En utilisant le lemme précédent, on obtient $x + z' = x' + z$, donc $(x, x') \sim_{\mathbf{Z}} (z, z')$. □

§5.10 **Definition.** On définit $\mathbf{Z}$ comme l'ensemble des classes d'équivalences de la relation d'équivalence $\sim_{\mathbf{Z}}$.

On définit l'addition sur les couples, et on montre que c'est une opération compatible avec l'équivalence.

§5.11 **Proposition.** *On définit l'addition terme à terme $(k, n) + (k', n') = (k + k', n + n')$; cette opération est compatible avec la relation d'équivalence et induit une addition sur $\mathbf{Z}$.*

Démonstration. L'addition est bien compatible avec la relation d'équivalence. Soient $k, k', n, n', p, p', q, q'$ des entiers, et supposons que $(k, n) \sim_{\mathbf{Z}} (p, q)$ et $(k', n') \sim_{\mathbf{Z}} (p', q')$. On a :

$$\begin{aligned} (k, n) + (k', n') &= (k + k', n + n') \\ (p, q) + (p', q') &= (p + p', q + q') \end{aligned}$$

Or $k + k' + q + q' = (k + q) + (k' + q') = (n + p) + (n' + p') = n + n' + p + p'$. □

On définit maintenant de la même manière la multiplication en étendant la multiplication sur les entiers.

§5.12 **Proposition.** *Soient a, b, c, d des entiers. On définit la multiplication par $(a, b) \times (c, d) = (ac + bd, ad + bc)$. Cette opération est compatible avec la relation d'équivalence et définit donc une opération sur $\mathbf{Z}$.*

Démonstration. On montre que la multiplication est effectivement compatible avec la relation d'équivalence. Soient k, k', n, n', p, q des entiers, et supposons que $(k, n) \sim_{\mathbf{Z}} (p, q)$ et $(k', n') \sim_{\mathbf{Z}} (p', q')$. On a :

$$\begin{aligned}(k, n) \times (k', n') &= (kk' + nn', kn' + nk') \\ (p, q) \times (k', n') &= (pk' + qn', pn' + qk')\end{aligned}$$

Or $kk' + nn' + pn' + qk' = (k + q)k' + (n + q)n' = (n + p)k' + (n + q)n' = kn' + nk' + pk' + qn'$. □

§5.13 **Proposition.** *Les opérations d'addition et de multiplication sont associatives et commutatives sur $\omega \times \omega$ et donc sur $\mathbf{Z}$. De plus, la multiplication distribue sur l'addition.*

Démonstration. Vérification laissée au lecteur. □

§5.14 **Lemme.** *Soient m, n, k des entiers. On a $(m + k, n + k) \sim_{\mathbf{Z}} (m, n)$.*

Démonstration. Par associativité et commutativité, $(m + k) + n = m + (k + n) = m + (n + k)$. □

§5.15 **Lemme.** *Soient $m \leqslant n$ des éléments de ω. Il existe $k \in \omega$ tel que $m + k = n$.*

Démonstration. Si $m = n$, le résultat est trivial. On suppose dans la suite que $m < n$.

Supposons que pour tout $k \in \omega$, $m + k < n$. Dans ce cas, on a $n \geqslant \sup\{m + k : k \in \omega\} = \omega$. Donc $n \notin \omega$. On vient donc de montrer que l'ensemble des entiers k tels que $m + k \leqslant n$ est non vide.

On prends alors le plus petit $k \in \omega$ tel que $m + k \geqslant n$. Remarquons tout d'abord que $k \neq 0$, puisque $m \neq n$. Si $m + k > n$, alors en posant $k = l + 1$, on a $m + l + 1 > n$ donc $m + l \geqslant n$; comme $l < k$ et que k était supposé minimal, cela contredit l'hypothèse. On a donc $m + k = n$. □

§5.16 **Proposition.** *Soit $(m, n) \in \omega \times \omega$. Il existe $k \in \omega$ tel que $(m, n) \sim_{\mathbf{Z}} (k, 0)$ ou bien $(m, n) \sim_{\mathbf{Z}} (0, k)$.*

Démonstration. Si $m = n$, on montre que $(m, n) \sim_{\mathbf{Z}} (0, 0)$ en utilisant le lemme §5.14.

Si $m < n$, le lemme §5.15 nous assure de l'existence de $k \in \omega$ tel que $m + k = n$. Dans ce cas, en utilisant le lemme §5.14 on a que $(m, m + k) \sim_{\mathbf{Z}} (0, k)$.

Si $m > n$, on écrit $m = n + k$ par le lemme §5.15 et on montre de même que $(n + k, n) \sim_{\mathbf{Z}} (k, 0)$ (lemme §5.14). □

Cette proposition nous permet de prendre comme représentant de chaque classe un couple où l'un des entiers au moins est nul. On identifiera $(0, k)$ avec sa classe.

§5.17 **Proposition.** *La relation définie par* $(0, k) < (0, k') < (0, 0) < (l', 0) < (l, 0)$ *pour tous entiers non nuls* $k > k', l > l'$ *est un ordre strict total sur* $\mathbf{Z}$.

Démonstration. La relation est totale sur $\mathbf{Z}$ par définition (proposition paragraphe §5.16). C'est un ordre strict car définit à partir d'un ordre strict sur ω. □

§5.18 **Lemme.** *Si* a, b, k *sont des entiers,* $a + k < b + k$ *si et seulement si* $a < b$. *De plus, si* k *est un entier strictement positif,* $ak < bk$ *si et seulement si* $a < b$.

Démonstration. Pour la première équivalence, si $k = 0$, c'est évident, ensuite, on montre par induction le cas $k > 0$. Pour le cas $k < 0$, c'est une seconde induction.

La seconde équivalence se montre directement par induction sur $k > 0$, en utilisant la première équivalence. □

§5.19 **Proposition.** *La structure* $(\mathbf{Z}, +)$ *forme un groupe commutatif.*

Démonstration. Le fait que l'addition soit associative, commutative et d'élément neutre 0 est clair. On montre qu'il existe un inverse pour chaque élément de $\mathbf{Z}$.

Soit $(0, k) \in \mathbf{Z}$. On a $(0, k) + (k, 0) = (k, k) \sim_{\mathbf{Z}} (0, 0)$.
Soit $(k, 0) \in \mathbf{Z}$. On a $(0, k) + (k, 0) = (k, k) \sim_{\mathbf{Z}} (0, 0)$. □

On a donc ajouté les inverses pour l'addition. On voudrait maintenant faire de même pour la multiplication. Avant de faire cela, on adoptera les notation habituelles :

- $(k, 0)$ est noté k
- $(0, k)$ est noté $-k$ (en particulier $-0 = 0$)
- On écrit $k + n$ l'addition et kn la multiplication.

Les rationnels

§5.20 On veut maintenant ajouter les inverses pour la multiplication. On va pour cela utiliser exactement la même méthode que pour ajouter les inverses pour l'addition dans ω.

§5.21 **Definition.** On définit une relation $\sim_{\mathbf{Q}}$ sur les couples ordonnés dans $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ par

$$(a, b) \sim_{\mathbf{Q}} (c, d) \Leftrightarrow ad = bc$$

§5.22 **Lemme.** *Si a, b, c sont des éléments de $\mathbf{Z}$ et que $c \neq 0$, alors $ac = bc \Rightarrow a = b$.*

Démonstration. Si $b < 0$, on peut remplacer a, b, c par $-a, -b, -c$ et on a $(-a)(-c) = ac = bc = (-b)(-c)$, avec $-b > 0$. On peut donc se ramener à $b > 0$, et on montre alors le résultat par induction sur b.

Si $b = 0$, $ac = bc = 0$, donc $a = 0$, puisque $c \neq 0$.

Si $b = k + 1$, et que le résultat a été démontré pour k, on a

$$ac = (k + 1)c = kc + c$$

On a $a \neq 0$, sinon $ac = 0$ et $(k + 1)c \neq 0$, ce qui est impossible. On pose $a = a' + 1$. On a alors

$$a'c + c = (a' + 1)c = ac = kc + c$$

Par le lemme §5.8, on obtient que $a'c = kc$, et par induction $a' = k$, c'est-à-dire $a = b$. □

§5.23 **Proposition.** *Cette relation est une relation d'équivalence.*

Démonstration. Si $(a, b) \sim_{\mathbf{Q}} (c, d) \sim_{\mathbf{Q}} (e, f)$ on a $(af)d = (ad)f = (bc)f = b(cf) = b(de) = (be)d$, donc $af = be$, car $d \neq 0$. □

§5.24 **Definition.** On définit l'ensemble $\mathbf{Q}$ des nombres rationnels comme l'ensemble des classes d'équivalence de la relation $\sim_{\mathbf{Q}}$.

§5.25 **Definition.** On définit sur $\mathbf{Z} \times (\mathbf{Z} - \{0\})$ les opérations d'addition et de multiplication par :

$$\begin{aligned} (a, b) + (c, d) &= (ad + cb, bd) \\ (a, b) \times (c, d) &= (ac, bd) \end{aligned}$$

§5.26 **Proposition.** *Les opérations d'addition et de multiplication que l'on a définies sont associatives et commutatives, et la multiplication distribue sur l'addition.*

Démonstration. C'est une conséquence directe de l'associativité et la commutativité des opérations définies sur $\mathbf{Z}$. □

§5.27 **Proposition.** *Les opérations d'addition et de multiplication sont compatibles avec la relation d'équivalence.*

Démonstration. Soient a, b, c, d, e, f des éléments de $\mathbf{Z}$ tels que b, d, f soient non nuls, et que $(a, b) \sim_{\mathbf{Q}} (e, f)$. On a alors

$$\begin{aligned}(a, b) + (c, d) &= (ad + cb, bd)\\ (e, f) + (c, d) &= (ed + cf, fd)\end{aligned}$$

On a que $(ad + cb)fd = (ad)(fd) + (cb)(fd) = (af)(dd) + (cb)(fd) = (be)(dd) + (cb)(fd) = (bd)(ed) + (bd)(cf) = bd(ed + cf)$.

De même,

$$\begin{aligned}(a, b) \times (c, d) &= (ac, bd)\\ (e, f) \times (c, d) &= (ec, fd)\end{aligned}$$

Or $(bd)(ec) = (be)dc = (af)dc = (ac)(fd)$. □

§5.28 **Lemme.** *Soit $(a, b) \in \mathbf{Z} \times (\mathbf{Z} - \{0\})$, et $k \in \mathbf{Z}$. On a $(a, b) \sim_{\mathbf{Q}} (ka, kb)$.*

Démonstration. Par associativité et commutativité de la multiplication, on obtient $a(kb) = (ak)b = (ka)b$. □

§5.29 **Lemme.** *Si $(a, b) \in \mathbf{Z} \times (\mathbf{Z} - \{0\})$, on a $(a, b) \sim_{\mathbf{Q}} (-a, -b)$.*

Démonstration. Clairement $a(-b) = b(-a)$. □

§5.30 **Definition.** On définit le pgcd de deux entiers a, b non nuls comme le plus grand entier naturel (donc positif) k tel qu'il existe a' et b' avec $a = ka'$ et $b = kb'$. Si $pgcd(a, b) = 1$, on dit que a et b sont premiers entre eux.

Démonstration. Le pgcd est bien défini. En effet, 1 est un diviseur commun à a et b, car $1a = a$ et $1b = b$. De plus, si $k > ab$, quelque soit les entiers a' et b', on a $ka' > a$ et $kb' > b$, donc l'ensemble des diviseurs communs de a et b est un sous-ensemble de $\{1, \ldots, ab\}$. □

§5.31 **Proposition.** *Soit $(a, b) \in \mathbf{Z} \times (\mathbf{Z} - \{0\})$. Il existe $a' \in \mathbf{Z}$ et $b' \in (\omega - \{0\})$ tels que a et b soient premiers entre eux et $(a, b) \sim_{\mathbf{Q}} (a', b')$. A partir de maintenant, on notera la classe de (a, b) par a'/b' si $b' \neq 1$, et par a' si $b' = 1$.*

Démonstration. Soit k le pgcd de $a = kc$ et $b = kd$. Alors par le lemme §5.28, $(a, b) \sim_{\mathbf{Q}} (c, d)$. Si $d > 0$, on a terminé, sinon on prends $(-c, -d)$. □

§5.32 **Proposition.** *Soit $(a, b) \in \mathbf{Q}$. Alors $(a, b) + (-a, b) \sim_{\mathbf{Q}} 0$.*

Démonstration. On a $(a, b) + (-a, b) = (ab - ab, bb) = (0, bb)$. Or $(0, bb) \sim_{\mathbf{Q}} (0, 1)$. □

§5.33 **Proposition.** *Soit $(a, b) \in \mathbf{Q}$, $a \neq 0$. Alors $(a, b)(b, a) \sim_{\mathbf{Q}} 1$.*

Démonstration. On a $(a,b)(b,a) = (ab,ab)$ car la multiplication est commutative, or $(ab,ab) \sim_{\mathbf{Q}} (1,1)$ par le lemme §5.28, d'où le résultat. □

§5.34 **Proposition.** *On définit une relation sur* $\mathbf{Q}$ *par*

$$(a,b) < (c,d) \Leftrightarrow ad < bc$$

Cette relation est une relation d'ordre strict total sur $\mathbf{Q}$*.*

Démonstration. Cette relation est transitive, car si $ad < bc$ et $cf < de$, on a $(af)d = (ad)f < (bc)f = b(cf) < b(de) = (be)d$. Or, cela implique que $af < be$ car $d > 0$.

Elle est antisymétrique, car si $ad < bc$ et $ad > bc$, on a $ad = bc$, et donc $(a,b) \sim_{\mathbf{Q}} (c,d)$ (lemme §5.18).

Elle est totale, car la relation d'ordre sur $\mathbf{Z}$ est totale. □

§5.35 **Proposition.** *L'ensemble* $\mathbf{Q}$ *est dénombrable, i.e.* $|\mathbf{Q}| = |\omega|$.

Démonstration. On a clairement $|\omega| \leqslant |\mathbf{Q}|$ par l'injection $x \mapsto (x,1)$. Pour l'implication inverse, on a que $|\omega \times \omega| = |\omega|$, donc $|(\omega \times \omega) \times (\omega \times \omega)| = |\omega|$. Or $\mathbf{Q} \subset \omega^4$, donc $|\mathbf{Q}| \leqslant |\omega|$. Par le théorème de Cantor-Bernstein, on en conclue que $|\mathbf{Q}| = |\omega|$. □

§5.36 **Definition.** Un ensemble ordonné qui n'a ni plus grand ni plus petit élément est dit *sans extrémités.*

§5.37 **Definition.** Soit r un ensemble muni d'un ordre strict total $<$. On dit que l'ordre $<$ (ou $r, <$) est dense si pour tous $a, b \in r$, il existe $c \in r$ tel que $a < c < b$.

§5.38 **Proposition.** *L'ordre défini sur* $\mathbf{Q}$ *est dense sans extrémités.*

Démonstration. Soit $(a,b) \in \mathbf{Q}$. Alors $(a,b)+(1,1) < (a,b) < (a,b)+(-1,1)$ donc $\mathbf{Q}$ n'a pas d'extrémités. Maintenant, soient $(a,b) < (c,d)$ des éléments de $\mathbf{Q}$. On définit $((a,b)+(c,d)) \times (1,2) = (ad+bc, 2bd)$. On peut alors voir que

$$\begin{array}{rcccl} (ad+bc)d & < & (bc+bc)d & = & (2bd)c \\ (ad+bc)b & > & (ad+ad)b & = & (2bd)a \end{array}$$

□

On regroupe les résultats précédents, et on obtient le théorème suivant, qui caractérise l'ensemble des rationnels.

§5.39 **Théorème.** *La structure* $(\mathbf{Q}, +, \times, 0, 1, <)$ *est un corps commutatif dénombrable, de caractéristique nulle, totalement ordonné, dense et sans extrémités.*

Les réels

§5.40 Le passage des rationnels aux réels est une opération de *complétion*. Pour comprendre cela, il suffit de remarquer que tout sous-ensemble de $\mathbf{Q}$ ne possède pas nécessairement de supremum. En effet, on peut définir l'ensemble $\{x \in \mathbf{Q} : x^2 \leqslant 2\}$ qui ne possède pas de supremum dans $\mathbf{Q}$. On commence par formaliser la notion d'ensemble ordonné complet.

§5.41 **Definition.** Soit $(r, <)$ un ensemble totalement ordonné et dense. On dit que r est *complet* si tout sous-ensemble non vide $s \subset r$ borné supérieurement (admettant un majorant) a un supremum.

Il existe plusieurs méthodes pour compléter les rationnels. On va utiliser ici la méthode des coupures de Dedekind, mais on pourrait tout aussi bien utiliser les suites de Cauchy (en exercice). Le point important est que le résultat de la complétion est bien unique, et donc ne dépends pas de la méthode utilisée.

§5.42 **Théorème.** *Soit $(P, <)$ un ensemble totalement ordonné, dense et sans extrémités. Il existe un ensemble totalement ordonné complet $(C, \prec)$ tel que :*

- *$P \subset C$;*
- *$\forall p, q \in P, p < q \Leftrightarrow p \prec q$;*
- *P est dense dans C ;*
- *C n'a pas d'extrémités.*

De plus, $(C, \prec)$ est unique à isomorphisme près.

Preuve de l'unicité. Soient $(C, \prec)$ et $(C', \prec')$ deux ensembles totalement ordonnés complets satisfaisant les conditions du théorème. On construit un isomorphisme h entre C et C' tel que $h(x) = x$ pour tout $x \in P$.

Si $c \in C$, on pose $S_c = \{p \in P \mid p \preceq c\}$. De même, on définit $S_{c'}$ pour $c' \in C'$. Si S est un sous-ensemble non vide de P borné supérieurement (admettant un majorant), on pose $\sup S$ le supremum de S dans $(C, \prec)$ et $\sup' S$ le supremum de S dans $(C', \prec')$. On peut remarquer que $\sup S_c = c$ et $\sup' S_{c'} = c'$.

On définit alors h par $h(c) = \sup' S_c$. Cette fonction est surjective, car si $c' \in C'$, on a $c' = \sup' S_{c'}$. Or $S_{c'} = S_c$ pour $c = \sup S_{c'}$, et on a $c' = h(c)$. Le fait que ce soit un morphisme est clair : si $c \prec d$, alors il existe $q \in P$ tel que $c \prec q \prec d$ et alors on a bien $\sup' S_c \prec' q \prec' \sup' S_d$, et par conséquent $h(c) \prec' h(d)$. L'injectivité se vérifie aisément, et on en déduit le résultat. □

Pour montrer l'existence de la complétion, on utilise la méthode des coupures de Dedekind.

§5.43 **Definition** (Coupures)**.** Une *coupure* est un couple ordonné (A, B) d'ensembles tel que :

- A et B sont des sous-ensembles de P disjoints, non vides, tels que $P = A \cup B$;

– Pour tous $a \in A$ et $b \in B$, on a $a < b$.

§5.44 Comme P est dense, il n'est pas possible que A ait un plus grand élément et que B ait un plus petit élément à la fois. On est alors soit dans le cas où A n'a pas de plus grand élément, et B possède un plus petit élément, soit dans le cas où A a un plus grand élément et B n'a pas de plus petit élément, soit dans le cas où A n'a pas de plus grand élement et B n'a pas de plus petit élément. Dans les deux premiers cas, le supremum de A existe, puisqu'il s'agit soit du plus grand élément de A, soit du plus petit élément de B. On oubliera alors le premier cas.

§5.45 **Definition** (Coupures de Dedekind)**.** Une coupure (A, B) est une *coupure de Dedekind* si A ne possède pas de plus grand élément.

On a deux types de coupures de Dedekind, :
– les coupures (A, B) telles que B ne possède pas de plus petit élément ;
– les coupures (A, B) avec $B = \{x \in P \mid x \geqslant p\}$ pour un $p \in P$; on notera ces coupures $[p]$.

On définit alors un ordre sur l'ensemble des coupures de Dedekind en posant

$$(A, B) \preceq (A', B') \Leftrightarrow A \subset A'$$

§5.46 **Exercice.** Montrer que la relation $\preceq$ ainsi définie sur les coupures de Dedekind est un ordre total.

Preuve de l'existence de la complétion. Si p, q sont dans P et tels que $p < q$, on a $[p] \prec [q]$. L'ensemble ordonné $(P', \prec)$ avec $P' = \{[p] \mid p \in P\}$ est donc isomorphe à $(P, <)$. On va montrer que $(C, \prec)$ est une complétion de $(P', \prec)$.

Pour montrer que P' est dense dans C, on pose $c, d \in C$ avec $c \prec d$, i.e. $c = (A, B)$ et $d = (A', B')$ avec $A \subset A'$. Soit $p \in P$ tel que $p \in A'$ et $p \notin A$. On peut supposer que p n'est pas le plus petit élément de B. On a alors $(A, B) \prec [p] \prec (A', B')$. Donc P' est dense dans C.

De plus, si $(A, B) \in C$, il existe $p \in B$ qui n'est pas le plus petit élément de B, et on a $(A, B) \prec [p]$. Donc C n'est pas de plus grand élément. De manière similaire, on montre que C n'a pas de plus petit élément.

On montre maintenant que C est complet. On pose S un sous-ensemble non vide de C borné supérieurement (admettant un majorant). Il existe donc (A_0, B_0) dans C tel que $A \subset A_0$ pour tout $(A, B) \in S$. On pose alors :

$$A_s = \bigcup \{A \mid (A, B) \in S\} \qquad B_s = P - A_s = \bigcap \{B \mid (A, B) \in S\}$$

On vérifie alors que (A_s, B_s) est une coupure, en remarquant que B est nécessairement non vide car $B_0 \subseteq B_s$. C'est même une coupure de Dedekind : A_s n'a pas de plus grand élément car aucun des A (avec $(A, B) \in S$) n'en ont.

Comme $A \subseteq A_s$ pour tout $(A, B) \in S$, (A_s, B_s) est une borne supérieure de S. Il ne reste plus qu'à vérifier que c'est bien la plus petite. Si $(\tilde{A}, \tilde{B})$ est

une autre borne supérieure de S, alors $A \subset \tilde{A}$ pour tout $(A, B) \in S$ et donc $A_s = \cup\{A \mid (A, B) \in S\} \subseteq \tilde{A}$. Donc $(A_s, B_s) \preceq (\tilde{A}, \tilde{B})$. □

§5.47 **Definition.** On note $(\mathbf{R}, <)$ la complétion de $(\mathbf{Q}, <_{\mathbf{Q}})$.

§5.48 **Proposition.** *Tout ensemble dénombrable totalement ordonné, dense sans extrémités est isomorphe à* $(\mathbf{Q}, <_{\mathbf{Q}})$.

Démonstration. Soit $(P, <)$ un ensemble dénombrable totalement ordonné, dense et sans extrémités. On montre dans un premier temps un lemme sur les isomorphismes partiels.

§5.49 **Lemme.** *Soit $h : P \to \mathbf{Q}$ un isomorphisme partiel de domaine fini, et deux points $p \in P$ et $q \in \mathbf{Q}$, il existe une extension $h_{p,q}$ de h telle que $p \in Dom(h_{p,q})$ et $q \in Im(h_{p,q})$.*

Preuve du Lemme. On pose $h = \{(p_1, q_1), (p_2, q_2), \ldots, (p_n, q_n)\}$ avec, pour tous $i < j$, $p_i < p_j$ et $q_i < q_j$. Si $p \in \mathrm{Dom}(h)$, on ne fait rien. Si $p \notin \mathrm{Dom}(h)$, alors soit $p < p_1$, soit $p_i < p < p_{i+1}$, soit $p_n < p$. On choisit alors un élément $q' \in \mathbf{Q}$ tel que soit $q' < q_1$ (on utilise le fait que l'on n'a pas d'extrémités), soit $q_i < q' < q_{i+1}$ (on utilise ici la densité), soit $q_n < q'$ (sans extrémités). On définit donc $h' = h \cup \{(p, q')\}$ qui est un isomorphisme partiel tel que $h \subset h'$, et $p \in \mathrm{Dom}(h')$. Si p était dans le domaine de h, on pose simplement $h' = h$.

De manière similaire, on peut étendre h' en un isomorphisme partiel $h_{p,q}$ afin que q soit dans l'image de $h_{p,q}$. Il suffit pour cela de trouver un antécédent pour q en utilisant le même raisonnement que précédemment. □

Maintenant, comme P et $\mathbf{Q}$ sont dénombrables, il sont en bijection avec les entiers naturels. On pose alors $P = \{p_i : i \in \mathbf{N}\}$ et $\mathbf{Q} = \{q_i : i \in \mathbf{N}\}$, et on définit une suite d'isomorphismes partiels à domaine fini par induction :

$$\begin{aligned} h_0 &= \emptyset \\ h_{n+1} &= (h_{n-1})_{p_n, q_n} \end{aligned}$$

On pose alors $h = \bigcup_{n \in \mathbf{N}} h_n$, et il est aisé de montrer que c'est un isomorphisme. En effet, si p, p' sont des éléments de P tels que $p < p'$, il existe $k, k' \in \mathbf{N}$ tels que $p_k = p$ et $p_{k'} = p'$. On pose $l = \max\{k, k'\}$, et on a que $p, p' \in \mathrm{Dom}(h_l)$, qui est un isomorphisme partiel. Donc $h_l(p) < h_l(p')$, donc $h(p) < h(p')$. On montre l'implication inverse de la même manière. □

§5.50 **Corollaire.** *L'ensemble ordonné $(\mathbf{R}, <)$ est l'unique (à isomorphisme près) ensemble totalement ordonné sans extrémités contenant un sous-ensemble dénombrable dense.*

Démonstration. Soit $(C, \prec)$ un ensemble totalement ordonné sans extrémités, et P un sous-ensemble dénombrable dense de C. Alors $(p, \prec)$ est isomorphe à $(\mathbf{Q}, <)$ par la proposition précédente, et $(C, \prec)$ est donc isomorphe à la complétion de $(\mathbf{Q}, <)$ car la complétion d'un ensemble ordonné est unique à isomorphisme près. Finalement, $(C, \prec)$ est isomorphe à $(\mathbf{R}, <)$. □

§5.51 **Corollaire.** *L'ensemble* $\mathbf{R}$ *n'est pas dénombrable.*

Démonstration. Comme $(\mathbf{R}, <)$ est un ensemble totalement ordonné, dense et sans extrémités, s'il était dénombrable il serait isomorphe à $(\mathbf{Q}, <)$, et donc incomplet (le fait d'être complet est préservé par isomorphisme). C'est une contradiction. □

§5.52 **Definition.** Soient $x, y \in \mathbf{R}$. On définit :

$$\begin{aligned} x + y &= \sup\{p +_{\mathbf{Q}} q : p, q \in \mathbf{Q}, p \leqslant x, q \leqslant y\} \\ -x &= \sup\{p \in \mathbf{Q} : -p \geqslant x\} \end{aligned}$$

§5.53 On vérifie, en utilisant les propriétés du supremum et les propriétés de l'addition sur $\mathbf{Q}$, que l'addition a les propriétés suivantes :

1. $x + y = y + x$
2. $x + (y + z) = (x + y) + z)$
3. $x + 0 = x$
4. Si $x < y$, alors $x + z < y + z$
5. $(x + (-y)) + y = x$
6. $x < y$ si et seulement si $y - x > 0$

§5.54 **Definition.** On définit $|x|$ pour tout $x \in \mathbf{R}$ par $|x| = x$ si $x \geqslant 0$ et $|x| = -x$ si $x < 0$. La multiplication des réels positifs est définie par :

$$xy = \sup\{pq : p, q \in \mathbf{Q}, 0 \leqslant p \leqslant x, 0 \leqslant q \leqslant y\}$$

Cette opération est étendue à tous les réels par :

$$xy = \begin{cases} |x||y| & \text{si } x \geqslant 0, y \geqslant 0 \text{ ou bien si } x \leqslant 0, y \leqslant 0 \\ -|x||y| & \text{si } x \geqslant 0, y \leqslant 0 \text{ ou bien si } x \leqslant 0, y \geqslant 0 \end{cases}$$

§5.55 On montre alors que les propriétés suivantes sont satisfaites :

1. $xy = yx$
2. $x(yz) = (xy)z$
3. $x.1 = x$
4. $x.0 = 0$
5. $x(y + z) = xy + xz$
6. Si $xy = 0$, alors $x = 0$ ou bien $y = 0$
7. Si $x < y$ et $z > 0$, alors $xz < yz$

6 Axiome du choix

Equivalents de l'axiome du choix

§6.1 **Proposition.** *Les énoncés suivants sont équivalents :*

1. *(AC) Pour tout ensemble il existe une fonction de choix.*
2. *(AC') Pour tout ensemble a dont les éléments sont non vides et disjoints deux à deux, il existe un ensemble dont l'intersection avec chaque élément de a est un singleton un ensemble à un seul élément.*
3. *(AC") Le produit d'une famille d'ensembles non vides est non vide.*

Démonstration. On montre (AC)⇒(AC'), puis (AC')⇒(AC"), et finalement (AC")⇒(AC).

(AC)⇒(AC') Soit a un ensemble et $b = \cup a$. On applique (AC) à b et on obtient une fonction de choix $f : \mathcal{P}(b) - \{\emptyset\} \to b$. Un élément de a est une partie non vide de b, et l'ensemble $c = \{f(x) \mid x \in a\}$ intersecte chaque élément de a en un unique point.

(AC')⇒(AC") Soit $(a_i)_{i\in I}$ une famille d'ensembles non vides. On pose $b_i = \{i\} \times a_i$. La famille $(b_i)_{i\in I}$ est formée d'ensembles non vides et disjoints deux à deux. On utilise (AC') pour obtenir un ensemble c tel que $c \cap b_i$ n'ait qu'un seule élément pour tout $i \in I$. Alors $c \cap \bigcup_{i\in I} b_i \in \prod_{i\in I} a_i$ par définition du produit.

(AC")⇒(AC) Si a est un ensemble quelconque, on forme le produit $b = \prod\{x \mid x \subset a, x \neq 0\}$. Par (AC") cet ensemble est non vide. Soit $\phi \in b$, on a que $\phi(x) \in x$ pour tout partie x non vide de a, donc ϕ est une fonction de choix.

□

§6.2 **Théorème** (Voir paragraphe §4.5)**.**
L'axiome du choix est équivalent à l'énoncé "Tout ensemble est bien ordonnable."

L'axiome du choix est utilisé souvent en mathématiques sous une forme différente : le lemme de Zorn. Nous allons montrer que (AC) permet de montrer le lemme de Zorn. Parmi les preuves classiques en mathématiques qui utilisent l'axiome du choix, on peut mentionner :

- Tout espace vectoriel possède une base.
- Tout corps possède une unique clôture algébrique.
- Le théorème de Hahn-Banach.
- Le théorème de Tikhonov sur le produit d'espaces compacts.

L'axiome du choix est donc très utile en mathématiques, et c'est pourquoi il est accepté par les mathématiciens malgré le fait qu'il a aussi des conséquences paradoxales, comme par exemple l'existence d'ensembles non mesurables, ou le célèbre paradoxe de Banach-Tarski qui énonce qu'on peut

découper une boule de rayon r de manière à obtenir des morceaux permettant de recomposer deux boules de rayon r.

§6.3 **Definition.** Soit un ensemble ordonné $(P, <)$.

On dit qu'un élément $a \in P$ est *maximal* s'il n'existe pas d'élément $y \in P$ tel que $a < y$, c'est-à-dire si pour tout $y \in P$, $\neg(a < y)$.

Si X est un sous-ensemble non vide de P, alors $c \in P$ est une *borne supérieure* de X si $x \leqslant c$ pour tout $x \in P$.

Un sous-ensemble non vide $C \subset P$ est appelé une *chaine* dans P si C est totalement ordonné par $<$.

§6.4 **Théorème** (Lemme de Zorn)**.** *Si $(P, <)$ est un ensemble partiellement ordonné et non vide tel que toute chaine dans P possède une borne supérieure, alors P a un élément maximal.*

Démonstration. Cette preuve utilise l'axiome du choix (AC).

On construit une chaine P qui mène à un élément maximal de P en utilisant une fonction de choix. On définit par induction :

$$a_\alpha = \text{ un élément de } P \text{ tel que } a_\alpha > a_\xi \text{ pour tout } \xi < \alpha \text{ s'il existe}$$

Si $\alpha > 0$ est un ordinal limite, alors $C_\alpha = \{a_\xi : \xi < \alpha\}$ est une chaine dans P et a_α existe par hypothèse. Finalement, il existe un θ tel qu'il n'existe pas de $a_{\theta+1} > a_\theta$ (sinon P ne serait pas un ensemble). Donc a_θ est un élément maximal de P. □

§6.5 **Proposition.** *Le lemme de Zorn implique l'axiome du choix.*

Démonstration. On montre plus exactement :

> Si tout ensemble ordonné c tel que tout sous-ensemble ordonné possède une borne supérieure possède un élément maximal, alors (AC) est vrai.

Soit a un ensemble dont tous les éléments sont non vides et disjoints deux à deux. Soit b la réunion des éléments de a et X l'ensemble des parties de b qui rencontrent chaque élément x de a en au plus un élément. L'ensemble X est ordonné par inclusion. Soit Y un sous-ensemble de X totalement ordonné, alors $\bigcup_{y\in Y} y \in X$. En effet, si $x \in a$, ou bien $x \cap y = \emptyset$ pour tout y et donc $x \cap \bigcup_{y\in Y} y = \emptyset$, ou bien $x \cap y_0 = \{u\}$ pour un $y_0 \in Y$ et alors $x \cap \bigcup_{y\in Y} y = \{u\}$.

L'ensemble ordonné X a la propriété exigée dans l'énoncé, donc il existe un élément maximal y_0 de X. Alors $x \cap y_0$ est un ensemble a un élément pour tout $x \in a$: si $x \cap y_0 = \emptyset$ pour un élément $x \in a$, on prends $\xi \in x$ et alors $y_0 \cup \{\xi\} \in X$, ce qui contredit la maximalité de y_0. □

Références

[CL03] R. Cori and D. Lascar. *Logique mathématique, volume 2*. Dunod, Paris, 2003. ISBN 2-10-005453-8.

[Jec02] T. Jech. *Set Theory, 3rd Edition*. Springer, 2002. ISBN 3-540-44085-2.

[Kri98] J.-L. Krivine. *Théorie des ensembles*. Cassini, 1998. ISBN 2-84225-014-1.

A Devoir 1

§A.1 **Exercice.** Soit A et B deux classes. On définit la classe $A\Delta B$, la *différence symétrique* de A et B par :

$$A\Delta B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

Montrer que si a et b sont des ensembles, la classe $a\Delta b$ est un ensemble.

Solution. Soient a et b des ensembles. En utilisant l'axiome de la paire ainsi que celui de la réunion, nous savons qu'il existe un ensemble $a \cup b = \cup\{a, b\}$ tel que $x \in a \cup b \Leftrightarrow x \in a \wedge x \in b$.

Soit ϕ la formule $(x \in a \wedge x \notin b) \vee (x \in b \wedge x \notin a)$. En appliquant l'axiome de séparation sur l'ensemble $a \cup b$ avec la formule ϕ, on obtient l'existence de l'ensemble

$$s = \{x \mid x \in a \cup b \wedge \phi(x)\}$$

Or la formule $(x \in a \cup b) \wedge \phi(x)$ est équivalente à

$$(x \in a \vee x \in b) \wedge ((x \in a \wedge x \notin b) \vee ((x \in b \wedge x \notin a))$$

Cette formule est équivalente à $\phi(x)$ puisque si $x \in a$ et $x \notin b$, alors $\phi(x)$ et $x \in a \vee x \in b$ sont toutes deux satisfaites, et si $x \in b$ et $x \notin a$ alors $\phi(x)$ et $x \in a \vee x \in b$ sont toutes deux satisfaites. Donc $a\Delta b = s$. □

§A.2 **Exercice.** On appelle *axiome de fondation* la formule suivante :

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

Montrer que l'axiome de fondation implique :

1. qu'un ensemble x ne peut se contenir, c'est-à-dire que pour tout ensemble x, $x \notin x$;
2. que pour tous ensembles $x_1, \ldots, x_n$ tels que pour tout $i = 1, \ldots, n-1$ on ait $x_i \in x_{i+1}$, on a nécessairement $x_n \notin x_1$;
3. (avec axiome de l'infini) qu'il n'existe pas de suite $x_1, \ldots, x_n, \ldots$ d'ensembles tels que pour tout $i = 1, \ldots, n, \ldots$, $x_{i+1} \in x_i$.

Solution.

1. Soit x un ensemble tel que $x \notin x$. On va montrer que l'existence de x contredit l'axiome de fondation. On considère pour cela l'ensemble $\{x\}$ dont l'existence est assurée par l'axiome de la paire et l'axiome de fondation. Cet ensemble est non vide puisqu'il contient l'ensemble x. De plus, il ne contient qu'un élément, x, et l'on a $x \cap \{x\} = \{x\} \neq \emptyset$. On a alors que $\{x\} \neq \emptyset$ et $\forall y(y \in \{x\} \Rightarrow y \cap \{x\} \neq \emptyset)$,ce qui contredit l'axiome de fondation.

2. Le raisonnement est le même que dans la première question. On suppose que $x_1, \ldots, x_n$ sont des ensembles tels que $x_i \in x_{i+1}$ pour tout $i = 1, \ldots, n$, et $x_n \in x_1$. En utilisant les axiomes de la paire et de la réunion, on peut montrer par récurrence l'existence de l'ensemble $a = \{x_1, \ldots, x_n\}$. Pour tout $y \in a$, il existe i tel que $y = x_i$, donc $y \cap a = \{x_{i-1}\}$ (si $i \neq 1$) ou $y \cap a = \{x_n\}$ (si $i = 1$). On a donc $a \neq \emptyset$ et $\forall y(y \in a \Rightarrow y \cap a \neq \emptyset)$, ce qui contredit l'axiome de fondation.
3. On utilise le même raisonnement qu'auparavant. Soient x_i ($i \in \mathbf{N}$) des ensembles tels que $x_{i+1} \in x_i$ pour tout $i \in \mathbf{N}$. On considère l'ensemble $a = \{x_i \mid i \in \mathbf{N}\}$ dont l'existence ne peut être montrée qu'en utilisant l'axiome de l'infini. Pour tout $y \in a$, il existe $i \in \mathbf{N}$ tel que $y = x_i$, donc $y \cap a = \{x_{i+1}\}$. Donc a est non vide et vérifie que pour tout $y \in a$ l'intersection $y \cap a$ est non vide, ce qui contredit l'axiome de fondation.

□

§A.3 **Exercice.** Montrer que l'axiome de la paire est une conséquence du schéma de substitution et de l'axiome des parties.

Solution. Soient a et b des ensembles. On va montrer qu'il existe un ensemble $\{a, b\}$ dont les éléments sont exactement a et b en utilisant uniquement le schéma de remplacement et l'axiome des parties. Le schéma de remplacement implique le schéma de substitution qui implique l'existence d'un ensemble ne possédant aucuns éléments : l'ensemble vide $\emptyset$. En appliquant à deux reprises l'axiome des parties, on obtient l'existence de l'ensemble $\{\emptyset, \{\emptyset\}\} = \mathcal{P}(\mathcal{P}(\emptyset))$.

On considère maintenant la relation (avec paramètres a et b)

$$R(x, y) = (x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$$

Il est facile de démontrer que cette relation est fonctionnelle. On applique alors le schéma de remplacement à l'ensemble $\{\emptyset, \{\emptyset\}\}$ et la relation fonctionnelle R, et l'on obtient l'existence de l'ensemble :

$$s = \{y \mid \exists x(x \in \{\emptyset, \{\emptyset\}\} \wedge R(x, y)\}$$

Les éléments de l'ensemble s étant exactement a et b, on a montré l'existence de l'ensemble $\{a, b\}$. □

B Devoir 2

§B.1 **Exercice.**
Montrer que si $(r, <)$ est un ensemble bien ordonné, alors il n'existe pas de suite $\langle a_n : n \in \omega \rangle$ d'éléments de r telle que $a_0 > a_1 > a_2 > \dots$
En déduire qu'il n'existe pas de suite $\langle \alpha_n : n \in \omega \rangle$ d'ordinaux telle que pour tout $i \in \omega$, $a_{i+1} \in a_i$.

Solution. Supposons qu'il existe une suite $< a_n : n \in \omega >$ strictement décroissante d'éléments de r. On considère alors l'ensemble $A = \{a_n : n \in \omega\}$, et supposons que A possède un plus petit élément a. Il existe donc $i \in \omega$ tel que $a = a_i$. Or $a_{i+1} \in A$, et $a_{i+1} < a_i$, ce qui contredit la minimalité de a. Donc A n'a pas de plus petit élément, ce qui contredit le fait que r soit bien ordonné. Donc il n'existe pas de suite strictement décroissante d'éléments de r.

Supposons maintenant qu'il existe une suite strictement décroissante (pour l'appartenance) d'ordinaux $\langle \alpha_n : n \in \omega \rangle$. Alors pour tout $i \in \omega$, $\alpha_i \in \alpha_0 \subset (\alpha 0 + 1)$. Donc l'ensemble $\{\alpha_i : i \in \omega\}$ est contenu dans $\alpha_0 + 1$. Comme les ordinaux sont bien ordonnés par l'appartenance, c'est une contradiction. □

§B.2 **Exercice** (Théorème de Forme normale de Cantor)**.**

1. Montrer que si $\alpha > 0$, et γ est un ordinal, il existe un unique β et un unique $\rho < \alpha$ tel que $\gamma = \alpha.\beta + \rho$.
2. Montrer que tout ordinal $\alpha > 0$ peut être représenté de manière unique sous la forme :

$$\alpha = \omega^{\beta_1}.k_1 + \omega^{\beta_2}.k_2 + \dots + \omega^{\beta_n}.k_n$$

où $n \geqslant 1$ est un entier naturel, $\alpha \geqslant \beta_1 > \beta_2 > \dots > \beta_n$ et $k_1, \dots, k_n$ sont des entiers.

Solution. 1. Considérer β le plus grand ordinal tel que $\alpha.\beta \leqslant \gamma$.

2. On montre l'existence par induction sur α. Pour $\alpha = 1$, on a $1 = \omega^0$. Pour $\alpha > 0$, on pose β le plus grand ordinal tel que $\omega^\beta \leqslant \alpha$. La question précédente nous dit qu'il existe un unique δ et un unique $\rho < \omega^\beta$ tels que $\alpha = \omega^\beta.\delta + \rho$. Ce δ est nécessairement fini, sinon cela contredirait la maximalité de β. Il suffit maintenant d'appliquer l'hypothèse d'induction sur ρ.

   On montre l'unicité par induction également.

□

C Devoir 3

§C.1 **Exercice.** On considère la théorie ZFC_{fin} qui est la théorie ZF (schéma de remplacement, axiome des parties, axiome de la réunion, axiome d'extensionalité) avec l'axiome du choix et l'axiome de fondation (voir le premier devoir). Le but de l'exercice est de donner un modèle de ZFC_{fin} qui ne satisfait pas l'axiome de l'infini.

Pour tout entier q, on définit $[q]$ comme l'unique ensemble d'entiers $\{p_1, \ldots, p_n\}$ tel que $q = \sum_{i=1}^{n} 2^{p_i}$ (penser à l'écriture de q en base 2).

On définit la relation binaire E sur $\mathbb{N}$ par :

$$pEq \Leftrightarrow p \in [q]$$

Montrer que :

1. la structure $(\mathbf{N}, E)$ satisfait l'axiome d'extensionnalité ;
2. pour tout entier q, l'ensemble $[q]$ des E-éléments de q est fini ;
3. pour tout ensemble fini d'entiers $\{p_1, \ldots, p_n\}$, il existe un unique entier q tel que $[q] = \{p_1, \ldots, p_n\}$;
4. la structure $(\mathbf{N}, E)$ est un modèle de ZFC_{fin}, et que l'axiome de l'infini n'est pas satisfait dans cette structure.

Solution.

1. Soient $a, b \in \mathbf{N}$, avec $a = \sum_{i=1}^{n} 2^{p_i}$. Si $\forall i \in \mathbf{N}$, $iEa \Leftrightarrow iEb$, alors $[a] = [b]$, d'où $b = \sum_{i=1}^{n} 2^{p_i} = a$.
2. Soit q un entier. Il existe $p \in \mathbf{N}$ tel que $2^p > q$. Alors $[q] \subset \{0, 1, \ldots, p\}$ et c'est donc un ensemble fini. On peut également montrer le résultat par l'absurde : si $[q]$ est infini, alors la somme $\sum_{p \in [q]} 2^p$ diverge (elle est minorée par $\sum_{p \in [q]} 1$ qui diverge par hypothèse), or cette somme doit être égale à q, un entier.
3. Il suffit de prendre $q = \sum_{i=1}^{n} 2^{p_n}$. Comme l'ensemble est fini, cette somme est finie et défini bien un entier. L'unicité est conséquence de l'extensionnalité (de manière équivalente, c'est une conséquence de l'unicité de l'écriture binaire d'un entier).
4. Il nous reste :
   L'axiome de la réunion : Soit $a \in \mathbf{N}$, et $\{p_1, \ldots, p_n\} = [a]$ l'ensemble des E-éléments de a. Chaque p_i étant un entier, l'ensemble $[p_i]$ est fini (question 2). L'union des ensembles $[p_i]$ est une union finie d'ensembles finis, donc c'est un ensemble fini que l'on note B. Par la question 3, il existe un entier b tel que $[b] = B$. On vérifie ensuite aisément que les E-éléments de b sont exactement les E-éléments des E-éléments de a.
   L'axiome des parties : Soit $a \in \mathbf{N}$ et $\{p_1, \ldots, p_n\} = [a]$ l'ensemble des E-éléments de a. Pour chaque sous-ensemble $B \subset [a]$, il existe un entier b tel que $[b] = B$ (question 3). Comme $[a]$ est fini, A n'a qu'un

nombre fini de sous-ensembles. On note donc $q_1, \ldots, q_p$ les entiers associés aux sous-ensembles de A. Par la question 3, il existe un entier z tel que $[z] = \{q_1, \ldots, q_p\}$. Par construction, les E-éléments de z sont les E-sous-ensembles de a.

Le schéma de remplacement : Soit $a \in \mathbf{N}$ et $u_1, \ldots, u_k$ des entiers, $\{p_1, \ldots, p_n\} = [a]$ l'ensemble des E-éléments de a, et $F(x, y, \vec{u})$ une classe de fonction, i.e. une classe de relation (un sous-ensemble de $\mathbf{N}^{k+2}$) fonctionnelle (i.e. satisfaisant la formule $Fonc(F, \vec{u}) = \forall x(((F(x, y, \vec{u}) \wedge F(x, y', \vec{u})) \Rightarrow (y = y'))$. On peut supposer que a est inclus dans le domaine de F, quitte à considérer un sous-ensemble de a. On note alors q_i l'unique entier tel que $F(p_i, q_i, \vec{u})$ (l'unicité est conséquence de la fonctionnalité de F). Il est alors clair que la classe $\{b \ l \ \exists pEa, F(a, b, \vec{u})\}$ contient exactement les éléments q_i. Par la question 3, il existe un entier z tel que $[z] = \{q_1, \ldots, q_n\} = \{b \ l \ \exists pEa, F(a, b, \vec{u})\}$.

Il reste maintenant à vérifier que l'axiome de l'infini n'est pas satisfait. C'est immédiat : un ensemble inductif possède un nombre infini de E-éléments, et on a montré (question 2) que tout élément du modèle (tout entier) ne possède qu'un nombre fini de E-éléments.

□

§C.2 **Exercice.**

On définit la relation suivante sur Ord × Ord :

$$(\alpha, \beta) <_\times (\gamma, \delta) \Leftrightarrow \begin{cases} \text{soit} & \max\{\alpha, \beta\} < \max\{\gamma, \delta\} \\ \text{soit} & \max\{\alpha, \beta\} = \max\{\gamma, \delta\} \wedge \alpha < \gamma \\ \text{soit} & \max\{\alpha, \beta\} = \max\{\gamma, \delta\} \wedge \alpha = \gamma \wedge \beta < \delta \end{cases}$$

1. Montrer que cette relation est un bon ordre. On notera par la suite $\Gamma(\alpha, \beta)$ l'unique ordinal isomorphe au segment initial déterminé par (α, β), muni de l'ordre induit par $<_\times$.
2. Montrer que $(\alpha, \beta) <_\times (\gamma, \delta)$ si et seulement si $\Gamma(\alpha, \beta) < \Gamma(\gamma, \delta)$.
3. Remarquer que $\Gamma(0, \omega) = \omega$, puis montrer que $\Gamma(0, \omega_\alpha) = \omega_\alpha$.
4. En déduire que pour tout cardinal infini $\aleph_\alpha$, on a $|\aleph_\alpha \times \aleph_\alpha| = \aleph_\alpha$.

Solution. 1. Si x est un ensemble non vide dont tous les éléments sont dans Ord^2, l'ensemble des $\max\{\alpha, \beta\}$ pour $(\alpha, \beta) \in x$ a un plus petit élément γ_0 ; l'ensemble des α tels qu'il existe β avec $(\alpha, \beta) \in x$ et $\max\{\alpha, \beta\} = \gamma_0$ a un plus petit élément α_0 ; l'ensemble des β tels que $\max\{\alpha_0, \beta\} = \gamma_0$ et $(\alpha_0, \beta) \in x$ a un plus petit élément β_0. Il est alors clair que (α_0, β_0) est le plus petit élément de x, donc l'ordre que nous avons défini est bien un bon ordre.

2. Si $(\alpha, \beta) <_\times (\gamma, \delta)$, alors il est clair que $\Gamma(\alpha, \beta) < \Gamma(\gamma, \delta)$. En effet, si $\Gamma(\alpha, \beta) \geqslant \Gamma(\gamma, \delta)$, il existe un isomorphisme de (γ, δ) avec l'un de ses

segments initiaux.

$$(\gamma, \delta) \to \Gamma(\gamma, \delta) \subset \Gamma(\alpha, \beta) \to (\alpha, \beta) \subsetneq (\gamma, \delta)$$

L'implication inverse se fait de manière similaire.

3. On a $\Gamma(0, \omega_0) = \Gamma(0, \omega) = \omega = \omega_0$. Soit α le plus petit ordinal tel que $\Gamma(0, \omega_\alpha) \neq \omega_\alpha$. Soient $\beta, \gamma < \omega_\alpha$ tels que $\Gamma(\beta, \gamma) = \omega_\alpha$. On choisit $\delta < \omega_\alpha$ tel que $\delta > \beta$ et $\delta > \gamma$. Comme le segment initial de Ord^2 avec l'ordre $<_\times$ déterminé par $\delta \times \delta$ contient (β, γ), on a $\omega_\alpha \subset \Gamma(0, \delta)$, et donc $|\delta \times \delta| \geqslant \aleph_\alpha$. Or $|\delta \times \delta| = |\delta|.|\delta|$, donc par minimalité de α, $|\delta|.|\delta| = |\delta| < \aleph_\alpha$, une contradiction.
4. Pour tout cardinal $\aleph_\alpha$, le segment initial de Ord^2 avec l'ordre $<_\times$ déterminé par $(0, \aleph_\alpha)$ est par définition isomorphe à l'ordinal $\aleph_\alpha \times \aleph_\alpha$. On a alors $|\aleph_\alpha \times \aleph_\alpha| = |\Gamma(0, \aleph_\alpha)| = |\aleph_\alpha| = \aleph_\alpha$ par la question précédente.

□

D Devoir 4

§D.1 **Exercice.**
Soit $< \mathfrak{U}, \in >$ un modèle de la théorie ZF. On construit dans $< \mathfrak{U}, \in >$, par induction, une relation fonctionnelle de domaine la classe des ordinaux :

$$\begin{aligned} V_0 &= \emptyset \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\alpha &= \cup_{\beta<\alpha} V_\beta \text{ si } \alpha \text{ est limite} \end{aligned}$$

On désigne par V la classe union de tous les V_α, c'est-à-dire la classe définie par la formule $V(x) = \exists \alpha \mathrm{Ord}(\alpha) \wedge x \in V_\alpha$, où $\mathrm{Ord}(\alpha)$ est la formule exprimant que α est un ordinal.

Pour chaque objet de x, on définit le *rang* de x noté $rg(x)$ comme le plus petit ordinal α tel que $x \in V_\alpha$.

1. Expliquer pourquoi le rang est bien défini ;
2. Montrer que l'axiome d'extensionnalité est satisfait dans $< V, \in >$ ($\in$ est la relation d'appartenance de $< \mathfrak{U}, \in >$ restreinte à V) ;
3. Montrer qu'un ensemble a est dans V si et seulement si tous ses éléments sont dans V, et que si a est de rang α, alors les éléments de a sont de rang strictement plus petit que α ;
4. Montrer que l'axiome de l'union est satisfait dans $< V, \in >$, et exprimer le rang de $\cup a$ en fonction du rang de a ;
5. Montrer que l'axiome des parties est satisfait dans $< V, \in >$, et exprimer le rang de $\mathcal{P}(a)$ en fonction du rang de a ;
6. Montrer que chaque ordinal est dans V, et que si α est un ordinal, $rg(\alpha) = \alpha + 1$;
7. (Facultatif) Montrer que le schéma de remplacement est satisfait dans $< V, \in >$;
8. Montrer que $< V, \in >$ satisfait l'axiome de fondation.

Solution.
1. Si $x \epsilon V$, il existe un ordinal α tel que $x \in V_\alpha$. Donc la classe des ordinaux γ tels que $x \in V_\gamma$ est non vide, et possède par conséquent un plus petit élément car la classe des ordinaux est bien ordonnée. Le rang est donc bien défini.
2. Soient $x, y \epsilon V$ tels que pour tout $z \epsilon V$, $z \in x \Leftrightarrow z \in y$, c'est-à-dire tels que
$$< V, \in > \vDash \forall z, (z \in x \Leftrightarrow z \in y) \tag{4}$$
On veut en déduire que $x = y$. Pour cela, on commence par remarquer que l'équation 4 est équivalente (par définition) à la suivante :
$$< \mathfrak{U}, \in > \vDash \forall z, V(z) \Rightarrow (z \in x \Leftrightarrow z \in y) \tag{5}$$

Or la formule $\forall z(V(x) \Rightarrow (z \in x \Leftrightarrow z \in y))$ est équivalente à la formule $\forall z(z \in x \Leftrightarrow z \in y)$ car par construction tous les éléments de x et de y sont des éléments de V (on le montre dans la question suivante). Cette dernière formule étant satisfaite dans le modèle $< \mathfrak{U}, \in >$, elle est satisfaite dans le modèle $< V, \in >$.

3. Soit a un ensemble dans V. Alors il existe un ordinal $\alpha = rg(a)$ tel que $a \in V_\alpha$ et $a \notin V_\beta$ pour tout $\beta < \alpha$. On commence par montrer que α ne peut être limite. Ceci est facile à voir, car si α était limite, on aurait $a \in V_\alpha$ et $a \notin V_\beta$ pour tout ordinal $\beta < \alpha$ impliquerait que $a \notin \cup_{\beta<\alpha} V_\beta$: comme $V_\alpha = \cup_{\beta<\alpha} V_\beta$ cela serait contradictoire. Donc α est un ordinal successeur, et l'on peut noter β son prédecesseur. On a alors $a \in \mathcal{P}(V_\beta)$ par définition de $V_{\beta+1}$, et donc $a \subset V_\beta$. On a alors que tous les éléments de a sont des éléments de V_β, et donc des éléments de V. De plus, comme ce sont des éléments de V_β, leur rang est inférieur ou égal à β, qui est strictement inférieur à α.

4. Soit a un ensemble dans V de rang α, où $\alpha = \beta + 1$. On veut montrer que :
$$< V, \in > \vDash \exists b \forall c(c \in b \Leftrightarrow \exists z(c \in z \wedge z \in a)) \tag{6}$$
C'est-à-dire :
$$< \mathfrak{U}, \in > \vDash \exists b(V(b) \wedge \forall c(V(c) \Rightarrow (c \in b \Leftrightarrow \exists z(V(z) \wedge c \in z \wedge z \in a)))) \tag{7}$$
Comme les éléments de a sont des éléments de V et que leur éléments sont eux-même nécessairement des éléments de V, on veut montrer la formule équivalente :
$$< \mathfrak{U}, \in > \vDash \exists b(V(b) \wedge \forall c(c \in b \Leftrightarrow \exists z(c \in z \wedge z \in a))) \tag{8}$$
Comme $< \mathfrak{U}, \in >$ est un modèle de ZF, l'union de a existe dans $< \mathfrak{U}, \in >$, et il suffit donc de montrer que cet ensemble est dans V. Soit $b = \cup a$ dans $< \mathfrak{U}, \in >$. Les éléments de b sont exactement les ensembles c tels qu'il existe $z \in a$ avec $c \in z$. Par la question précédente, un élément $z \in a$ est un ensemble dans V de rang $\gamma \leqslant \beta$, et tout élément de z est alors un ensemble dans V de rang $\delta < \beta$. Tous les c éléments de b sont donc dans V et de rang strictement inférieur à β. On en déduit que $b \subset V_\beta$ et donc que $b \in \mathcal{P}(V_\beta) = V_\alpha$. L'union de a existe donc bien dans V et est de rang inférieur ou égal au rang de a.

5. De la même manière qu'à la question précédente, on est simplement ramenés à montrer que l'ensemble des parties, qui existe dans $< \mathfrak{U}, \in >$, est bien dans V. Soit a un ensemble dans V de rang $\alpha = \beta + 1$, et soit b l'ensemble de ses parties. Un élément z de b est un sous-ensemble de a, donc est un ensemble qui contient uniquement des ensembles qui sont dans V, de rang inférieur ou égal à β (ce qui est équivalent à

être strictement inférieur à α). On a donc $z \subset V_\beta$, et par conséquent $z \in \mathcal{P}(V_\beta) = V_\alpha$. On en déduit que $b \subset V_\alpha$ et donc $b \in V_{\alpha+1}$, c'est-à-dire que b est un élément de V. On a montré que le rang de b est inférieur ou égal à $\alpha + 1$, et on peut montrer qu'il est en fait égal à cet ordinal. En effet, supposons b de rang strictement inférieur à $\alpha+1$. Les éléments de b sont alors de rang strictement inférieur à α. Or $a \in b$, et $rg(a) = \alpha$, ce qui est une contradiction.

6. On procède par induction :
   - On a $0 \epsilon V$ par définition et $rg(0) = 1$.
   - Si α est successeur, on pose $\alpha = \beta + 1$. Alors $\beta \epsilon V$ et $rg(\beta) = \alpha$ par hypothèse d'induction. On a alors $\beta \in V_\alpha$ et $\beta \subset V_\alpha$ (car les éléments de β sont de rang strictement inférieur à α). D'où $\beta \cup \{\beta\} \subset V_\alpha$, et donc $\alpha = \beta \cup \{\beta\} \in V_{\alpha+1} = \mathcal{P}(V_\alpha)$. De plus, le rang de α ne peut être inférieur à $\alpha + 1$ puisque α contient β de rang α.
   - Si α est un ordinal limite, tout ordinal $\beta < \alpha$ est dans V, de rang $\beta + 1$ par hypothèse d'induction. Donc pour tout $\beta \in \alpha$, $\beta \in V_{\beta+1}$, et par conséquent $\beta \in V_\alpha = \cup_{\gamma<\alpha} V_\gamma$. Donc $\alpha = \cup_{\beta:\beta<\alpha} \subset V_\alpha$ et finalement $\alpha \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$. On a donc montré que α est dans V et que son rang est inférieur ou égal à $\alpha + 1$. Supposons qu'il soit strictement inférieur à $\alpha + 1$. Il ne peut être égal à α car le rang est nécessairement un ordinal successeur. Il existe donc $\beta < \alpha$ tel que $rg(\alpha) = \beta$. Or, $\beta \in \alpha$, et $rg(\beta) = \beta + 1 > rg(\alpha)$, ce qui est une contradiction.

7. Si $F(x_1, \ldots, x_n)$ est une relation fonctionnelle dans $< V, \in >$, ce n'est pas nécessairement une relation fonctionnelle dans $< \mathfrak{U}, \in >$. Ce problème est rapidement résolu si l'on considère la relation

$$F'(x_1, \ldots, x_n) = V(x_1) \wedge \cdots \wedge V(x_n) \wedge F(x_1, \ldots, x_n)$$

qui elle est fonctionnelle dans $< \mathfrak{U}, \in >$. Soit donc un ensemble a dans V, et une relation fonctionnelle (dans V) F. Alors en utilisant le schéma de remplacement avec l'ensemble a et la relation fonctionnelle (dans $\mathfrak{U}$) F' dans le modèle $< \mathfrak{U}, \in >$, on obtient l'existence d'un ensemble b image de l'ensemble a par la relation fonctionnelle F'. Cette image contient uniquement des ensembles dans V, et elle est donc elle-même un ensemble dans V : pour montrer cela on doit montrer qu'il existe un ordinal β tel que l'ensemble b soit un élément de V_β, ce que l'on peut faire en montrant que les rangs des éléments de b ne peuvent être arbitrairement grand. Or si pour tout ordinal α il existe un élément de b tel que son rang soit supérieur à α, l'image par la relation fonctionnelle $G(x, y) \Leftrightarrow V(x) \wedge y = rg(x)$ de l'ensemble b ne peut être un ensemble (son union est la classe des ordinaux) ce qui contredit le schéma de remplacement (dans $< \mathfrak{U}, \in >$). Comme l'image de a par F dans V est égale à l'image de a par F' dans $\mathfrak{U}$, on a terminé.

8. Soit $a \neq \emptyset$ un ensemble dans V, et α le rang de a. On veut montrer que a satisfait l'axiome de fondation, c'est-à-dire qu'il existe un ensemble $y \in a$ tel que $y \cap x = \emptyset$. On définit pour cela l'ensemble b des rangs des éléments de a. C'est un ensemble d'ordinaux défini par le schéma de séparation :

$$b = \{\beta \mid \beta \in \alpha \wedge \exists y(y \in a \wedge \beta = rg(y))\} \tag{9}$$

Comme c'est un sous-ensemble de α, et que α est bien ordonné (c'est un ordinal), il existe un ordinal δ qui est le plus petit élément de b. Soit alors un ensemble $y_0 \in a$ tel que $rg(y_0) = \delta$, et supposons que $y_0 \cap a \neq \emptyset$. Soit alors $z \in y_0 \cap a$. Comme $z \in y_0$, on a que $rg(z) < rg(y_0)$. Comme $z \in a$, $rg(z) \geqslant rg(y_0)$ par définition de y_0. On a donc une contradiction, et donc $y_0 \cap a = \emptyset$.

□

§D.2 **Exercice.** Soit $\mathfrak{c}$ le cardinal de l'ensemble des réels. Montrer que le cardinal de l'ensemble des fonctions continues de $\mathbf{R}$ dans $\mathbf{R}$ est égal à $\mathfrak{c}^{\aleph_0}$.

Solution. Si f est une fonction continue de $\mathbf{R}$ dans $\mathbf{R}$, les valeurs prises par f sur $\mathbf{Q}$ la détermine uniquement. En effet, soit $y \in \mathbf{R}$, et soit (u_n) une suite de rationnels convergeant vers y. Alors par continuité de f, $f(y) = \lim_{n\to\infty} f(u_n)$. Si l'on écrit κ le cardinal de l'ensemble des fonctions continues, on a montré que $\kappa \leqslant \mathfrak{c}^{\aleph_0}$. Or, l'inégalité inverse est également vraie, puisque toute fonction ξ de ω dans $\mathbf{R}$ défini une fonction continue de $\mathbf{R}$ dans $\mathbf{R}$: il suffit de prendre la fonction définie par

$$f(x) = \begin{cases} \xi(0) & \text{si } x \leqslant 0 \\ \xi(i) + (\xi(i+1) - \xi(i))(x - i) & \text{si } i \leqslant x \leqslant i+1 \end{cases}$$

On a alors $\kappa \geqslant \mathfrak{c}^{\aleph_0}$, et on conclue par le théorème de Cantor-Bernstein. □

§D.3 *Remarque.* On peut de plus montrer que $\kappa = \mathfrak{c}$ en montrant que $\mathfrak{c} = \mathfrak{c}^{\aleph_0}$. Pour montrer cela, on remarque que $|[0,1]^2| = |[0,1]|$: l'inégalité $|[0,1]| \leqslant |[0,1]^2|$ est claire, et l'inégalité dans l'autre sens vient de l'injection de $[0,1]^2$ dans $[0,1]$ suivante : à (x,y), on associe le réel entre 0 et 1 dont l'écriture en binaire est obtenue en intercalant les écritures en binaire de x et de y. Cela permet de montrer que $|\mathbf{R}| = |\mathbf{R}^2|$ et par induction on obtient que $|\mathbf{R}^k| = |\mathbf{R}|$. Finalement, on a :

$$\mathfrak{c}^{\aleph_0} = |\mathbf{R}^\omega| = |\sup\{\mathbf{R}^k : k \in \omega\}| = \sup\{|\mathbf{R}^k| : k \in \omega\} = \mathfrak{c}$$