Introduction à la Théorie des Ensembles et nombres cardinaux.

Antoine Blanchon

Printemps 2009

Travail effectué dans le cadre optionnel des TIPE de l'université Lyon 1 et sous la direction de M.Altinel de l'Institut Camille Jordan.

Table des matières

Introduction

Lycéen je me posais déjà certains problèmes sur la densité des infinis, notamment le suivant : Soit un segment S dans l'espace et l'image I de sa projection sur un plan. Imaginons tout d'abord que le segment soit posé sur le plan. À chacun des points du segment S correspond un unique point du plan. On lève maintenant une extrémité du segment, l'autre restant confondue avec le plan. La projection de S sur le plan fait toujours correspondre à chacun des points de S un unique point de I sur le plan. Or ce segment image I est plus court que S ! Et ceci reste vrai quelle que soit l'inclinaison de S (tant qu'il n'est pas perpendiculaire au plan car alors la projection se fait sur un point unique), alors que la longueur du segment I devient minuscule pour une très forte inclinaison... Ce raisonnement montre qu'il y a le même nombre de points dans deux segments de tailles arbitraires, pour autant que cela ait un sens ! Pourtant cela peut paraître un peu contradictoire car on a envie de dire qu'il y a plus de points sur le segment le plus grand !

Cette contradiction provient du fait que l'on veut traiter le nombre de points des segments comme nous avons l'habitude de la faire avec des quantités finies alors que le nombre de points sur le segment est infini... Mais qu'est ce que l'infini ?

Avant la seconde moitié du $19^{\text{ème}}$ siècle et les travaux du mathématicien allemand Georg Ferdinand Ludwig Philipp Cantor, l'infini n'était pas considéré comme une quantité à proprement parler. L'approche de Cantor est révolutionnaire dans le sens où après avoir montré qu'il n'existe pas un mais une infinité d'infinis, il va manier ces grandeurs comme des quantités achevées. Sa théorie eut à se confronter à de nombreux détracteurs, dont quelques grands noms de son temps, avant d'être finalement unanimement acceptée. En effet, il s'avère qu'en formalisant de façon précise le cadre de la théorie de Cantor qui met au premier plan la notion d'ensemble, certains mathématiciens vont développer ce que l'on appelle la théorie des ensembles et qui permit de poser les bases de toutes les mathématiques modernes et apporte ainsi une avancée significative à la crise des fondements mathématiques au coeur de tous les débats de l'époque.

Parce que ce domaine des mathématiques me paraissait tout aussi intéressant que fondamental, le choix de faire un TIPE[1] sur ce sujet à fini par s'imposer de lui-même.

Ce mémoire présente un exposé complet sur la définition des nombres cardinaux, qui sont en quelque sorte une prolongation de ce que nous connaissons déjà avec les nombres finis, et décrit leur arithmétique.. Cette construction nécessite bien sur beaucoup de pré-requis, et ce mémoire est donc aussi l'occasion

[1] Travaux d'Initiative Personnelle Encadrés

de présenter une synthèse des connaissances que j'ai acquises durant l'étude de mon sujet de TIPE, la théorie des ensembles.

Le travail a été effectué en s'appuyant en grande partie sur la lecture active de l'excellent livre de Karel Hrbacek et Thomas Jech "Introduction to Set Theory, Third Edition, Revised and Expanded". Pour cette raison, ce mémoire propose un développement assez similaire à celui-ci et les démonstrations en sont de même souvent inspirées.

La plupart des résultats seront démontrés, sauf quelques uns dont la preuve, parfois fastidieuse, n'apporte pas grand intérêt, et pour des raisons de longueur de ce document. Seuls les théorèmes de récursion, finis et tranfinies seront à proprement parler admis.

Chapitre 1

Les fondements

Nul ne doit nous exclure du Paradis que Cantor a créé.
David Hilbert

1.1 Langage de la Théorie des ensembles et notion de propriétés

Tout le monde sait intuitivement ce qu'est un ensemble, un regroupement d'objets que nous pensons comme un tout. Pour quelles raison collectionnons nous ces objets ensemble ? Nous pouvons distinguer deux raisons à cela : car nous pouvons voir en ces objet une propriété commune (par exemple considérons l'ensemble des êtres vivant sur Terre), ou bien simplement car nous parvenons à regrouper ces objets dans notre esprit sans que ceux-ci n'aient à priori quelque chose en commun(prenons par exemple l'ensemble constitué de la chèvre de monsieur Seguin et de la première particule à être entrée en collision dans le LHC du CERN). Cette réflexion, loin d'être inutile nous permet de mieux appréhender ce qu'est un ensemble ce qui est primordial pour construire proprement notre théorie. Premièrement, notons que notre axiomatique devra rendre compte des deux façons qu'a notre esprit de construire un ensemble. Secondement, les ensembles sur lesquels nous travaillerons devront être parfaitement définis, et nous devons donc donner un moyen de savoir de façon univoque si tel ou tel objet est ou n'est pas dans l'ensemble. On se rend donc compte de la nécessité de clarifier la notion de propriété ; en effet, l'exemple donné concernant l'ensemble des êtres vivant sur Terre pourrait être interprété de différentes façons par une personne ou une autre en fonction de sa définition du vivant. On constate que le problème provient de ce que la notion de "vivant" est quelque peu subjective. Nous allons donc pour éviter ce genre de problèmes se fixer un langage formel, exempt de toute ambiguïté, pour décrire les propriétés.

Une formule fait référence à des objets d'une théorie, et s'écrit avec une suite de symboles qui appartiennent tous à ce qu'on appelle le langage de la théorie. Autrement dit un langage est une collection de symboles qui permettent d'écrire des formules pour parler des objets de la théorie. Un langage contient toujours les symboles logiques et des symboles de variables pour désigner les objet de la théorie ; on distingue en plus les symboles relationnels, fonctionnels, et de constantes. On appelle langage relationnel un langage qui ne contient que des

symboles relationnels.

Dans notre cas, le langage de la théorie des ensembles se réduit au symbole $\in$ d'appartenance, et bien sur au symbole $=$ d'égalité toujours présent, aux symboles logiques, et aux symboles de variables. Il ne comporte aucun symbole fonctionnel, ni de constante, mais seulement les symboles relationnels d'égalité et d'appartenance. On est donc dans le cadre particulier d'une structure relationnelle. Le symbole d'appartenance réfère à une relation binaire, c'est à dire à une relation entre deux objets, qui permet de dire que la première variable est un élément de la deuxième. Remarquons que tous les objets de notre univers sont des ensembles, ainsi les éléments d'un ensemble sont d'autres ensembles ! Pour tout ensemble a et b, on a $a \in b$ ou $b \in a$. $a \in b$ se lit "a appartient à b", ou "a est un élément de b", ou encore "b contient a".

Ce langage nous permet d'écrire de nombreuses formules, reste maintenant à nous limiter dans leurs constructions pour que celles ci aient un sens (ce qui est bien sur différent de dire qu'elles décriront quelque chose de vrai !). Ici nous nous permettrons uniquement d'écrire des formules du premier ordre, ce que nous définissons maintenant :

Définition 1 (Formule du premier ordre dans un langage relationnel)**.** *La définition est récursive.*

Premièrement on définit une formule atomique :

- *Si R est un symbole de relation n-aire, alors $R(x_1, x_2, ..., x_n)$ est une formule atomique.*
- *Toute formule atomique est de cette forme.*

Secondement, on donne les règles de construction suivante :

- *Si Φ et Ψ sont des formules du premier ordre, $\Phi \wedge \Psi$ et $\neg\Phi$ sont également des formules du premier ordre. (Suffisant pour justifier des autres compositions car par exemple $\Phi \vee \Psi = \neg(\neg\Phi \wedge \neg\Psi)$ et $\Phi \Rightarrow \Psi = \neg(\Phi \wedge \neg\Psi)$...).*
- *Si $\Phi(x_1, x_2, ..., x_n)$ est une formule du premier ordre, alors $\exists x_1, \Phi(x_1, x_2, ..., x_n)$ est aussi une formule du premier ordre.*

Troisièmement, on énonce que réciproquement toute formule du premier ordre s'obtient de la façon décrite précédemment.

Notons donc qu'une formule du premier ordre ne quantifie donc que les variables.

Nous nous permettrons uniquement d'écrire des formules du premier ordre pour exprimer une proposition ou une propriété. Mais heureusement, même en se donnant cette condition et un langage aussi restreint que le notre nous pourrons décrire tous les objets mathématiques dont nous pourrions avoir besoin et chaque formule ainsi construite avec un ensemble limité d'éléments dont l'agencement ne peut avoir qu'un unique sens, permet d'exprimer toute idée sans ambiguïté. Revenons maintenant munis de ce formalisme sur la notion de propriété.

Définition 2. *Une variable est dite libre dans une formule si elle n'est pas quantifiée. Dans le cas contraire elle est dite liée.*

Un énoncé qui ne comporte aucune variable libre est un énoncé, soit vrai soit faux, que l'on appelle *proposition.*

Définition 3. *Une propriété pour les variables $x_1, x_2, ..., x_n$ est une formule du premier ordre qui comporte $x_1, x_2, ..., x_n$ comme variables libres.*

1.2 Les Axiomes

Nous donnons comme telle la liste des axiomes classiques de la théorie des ensembles. Nous donnons pour chaque axiome son expression dans la langue naturelle puis dans notre langage formel. Remarquons dès à présent que l'unicité des ensembles construits dans cette section est garantie par l'axiome d'extensionnalité, et les notations introduites ont donc bien un sens.

Axiome d'existence Il existe un ensemble qui ne contient pas d'élément.

$$\exists X, \forall x, x \notin X$$

Cet axiome prouve que notre univers n'est pas vide, il existe au moins un ensemble : l'ensemble vide, noté $\emptyset$.

Axiome d'extensionnalité Si tout élément d'un premier ensemble appartient à un deuxième et inversement alors ces deux ensembles sont égaux.

$$\forall X, \forall Y, [(x \in X \Rightarrow x \in Y) \wedge (y \in Y \Rightarrow y \in X)] \Rightarrow (X = Y)$$

Cet axiome donne la condition d'égalité entre deux ensembles, on constate que seuls les éléments d'un ensemble le caractérisent au final, et non la façon dont il a été construit.

Schéma d'Axiomes de compréhension Soit $P(x)$ une propriété de x. Pour tout ensemble A, il existe un ensemble B tel que $x \in B$ si et seulement si $x \in A$ et $P(x)$.

$$\forall A, \exists B, (x \in B) \Leftrightarrow (x \in A \wedge P(x))$$

C'est un schéma d'axiomes, c'est à dire qu'il y a en fait un axiome pour chaque propriété P.

Notation 1. $\{x \in A | P(x)\}$ *est l'ensemble des éléments de* A *qui possède la propriété* P*.*

Axiome de la paire Pour chaque ensemble A et B, il existe un ensemble qui contient comme unique élément A et B.

$$\forall A, \forall B, \exists C, x \in C \Leftrightarrow (x = A \vee x = B)$$

Notation 2. $\{A, B\}$ *est l'ensemble qui contient* A *et* B *comme unique éléments.*

Cet axiome nous permet de commencer à construire des ensembles contenant de plus en plus d'éléments, on procède comme suit : D'après l'axiome de la paire il existe un ensemble $E = \{\emptyset, \emptyset\}$, qui est égal à l'ensemble qui ne contient que l'ensemble vide par l'axiome d'extentionnalité, on note donc $E = \{\emptyset\}$. Et donc toujours d'après l'axiome de la paire, $\{E, \emptyset\} = \{\{\emptyset\}, \emptyset\}$ est bien un ensemble...

Axiome de l'union Pour tout ensemble Z, il existe un ensemble X tel que x appartient à X si et seulement si il existe $Y \in Z$ tel que que $x \in Y$.

$$\forall Z, \exists X, x \in X \Leftrightarrow (\exists Y \in Z, x \in Y)$$

Notation 3. *L'union du système d'ensemble Z est noté $\bigcup Z$.*

Introduisont maintenant une définition pratique que nous utiliserons constamment par la suite.

Définition 4. *On dit que X est un sous ensemble de Y, ou que X est une partie de Y si tous les éléments de X sont aussi des éléments de Y. On dit que X est un sous ensemble strict (ou une partie stricte, ou un sous ensemble propre) de Y si X est un sous ensemble de Y, et que Y possède des éléments que X ne possède pas.*

Notation 4. *On note respectivement $X \subseteq Y$ ou $X \subset Y$ si X est un sous ensemble ou un sous ensemble strict de Y.*

On remarque que $X \subset Y$ si et seulement si $X \subseteq Y$ et $X \neq Y$.

Axiome de l'ensemble des parties Pour tout ensemble A, il existe un ensemble qui contient comme éléments toutes les parties de A.

$$\forall A, \exists B, (X \in B) \Leftrightarrow (X \subseteq A)$$

Notation 5. *On appelle ensemble des parties de A et on note $P(A)$ l'ensemble construit de cette façon.*

Axiome de l'infini Il existe un ensemble inductif.
Nous verrons dans le chapitre 2 ce qu'est un ensemble inductif.

Schéma d'Axiome de remplacement Soit $P(x, y)$ une propriété telle que pour chaque x, il existe un unique y pour lequel $P(x, y)$ est vérifiée. Pour tout ensemble A, il existe alors un ensemble B tel que pour chaque $x \in A$, il existe $y \in B$ pour lequel $P(x, y)$ est vérifiée.

$$\forall A, \exists B, (y \in B) \Leftrightarrow (x \in A \wedge P(x, y))$$

C'est aussi un schéma d'axiomes. Il justifie que la collection des objets qui sont liés un à un par une propriété à des éléments d'un ensemble, est également un ensemble.

Axiome du choix Il existe une fonction de choix pour chaque système d'ensembles.

Par ZF, on fait référence au système de ces axiomes sans l'axiome de choix, du nom des mathématiciens Zermelo et Fraenkel, premiers à proposer une véritable axiomatisation de la théorie des ensembles, et ZFC avec l'axiome de choix. L'axiome du choix est ainsi distingué des autres dans le sens où il postule de l'existence d'un ensemble d'une façon totalement non constructive par

rapport aux autres axiomes. Ces implications apportent une certaine cohérence pratique à la théorie comme nous aurons l'occasion de le mentionner, mais aussi quelques résultats contre-intuitifs. Pour ces raisons il rencontra et rencontre d'ailleurs toujours des opposants à son utilisation.

On peut rajouter à cette liste certains autres axiomes supplémentaires qui ne sont généralement pas admis comme étant part du système ZFC, sauf peut être l'axiome de fondation qui stipule que tout ensemble non vide contient un élément qui ne possède aucun élément en commun avec lui. Cet axiome permet d'éliminer de notre univers les ensembles qui sont éléments d'eux même ce qui permet d'éviter certains paradoxes.

Soulignons le fait que l'existence d'un ensemble ne peut être justifiée que par les axiomes donnés précédemment. Certains regroupements d'ensembles ne sont pas des ensembles au sens d'objets de notre univers ! C'est par exemple le cas de "l'ensemble de tous les ensembles" :

Démonstration. Soit V l'ensemble de tous les ensembles. Alors le Schéma de Compréhension permet d'affirmer que $A = \{x \in V | x \notin x\}$ est un ensemble, donc il appartient à V. On constate alors que si $A \in A$ alors $A \notin A$, et si $A \notin A$, alors $A \in A$; contradiction dans les deux cas. Or la seule hypothèse (tacite) que nous avions faite est que V est un ensemble. □

Les objets de notre théorie sont donc en fait regroupés dans ce qu'on appelle une classe.

Notons que l'axiome de la paire permet de justifier de l'existence d'ensembles même si les éléments n'ont à priori aucune propriété commune selon la remarque faite en introduction du chapitre.

Nous ne préciserons pas quand nous aurons recours à un axiome par la suite car cela est constamment le cas ! Néanmoins les trois derniers axiomes ne seront pas utilisés tout de suite et nous préciserons donc à quel moment nous en ferons un premier usage. Pour ce qui concerne l'axiome de choix, nous mentionnerons au fil de ce mémoire les implications qu'il pourrait avoir, mais nous effectuerons tout notre travail indépendamment de celui ci ne l'utiliserons donc à aucun moment.

1.3 Notions et définitions préliminaires

Opérations sur les ensembles

Nous sommes maintenant en mesure d'introduire quelques opérations élémentaires sur les ensembles.

L'axiome de compréhension permet de définir l'intersection de deux ensembles :

Définition 5. *On appelle intersection de A et B, et on note $A \cap B$ l'ensemble $\{x \in A | x \in B\}$ des éléments qui appartiennent à la fois à A et à B.*

L'axiome de la paire et de l'union permettent de définir l'union de deux ensembles :

Définition 6. *On appelle union de A et B, et on note $A \cup B$ l'ensemble des éléments qui appartiennent à A ou à B.*

L'axiome de compréhension nous permet également de définir la différence de deux ensembles :

Définition 7. *On note $A-B$ l'ensemble des éléments de A qui n'appartiennent pas à B.*

Relations

Un ensemble à deux éléments est une paire non-ordonnée (d'après l'axiome d'extensionnalité $\{A, B\} = \{B, A\}$). Pour définir une relation, notion fondamentale en mathématiques, dans le cadre de notre théorie il va falloir introduire la notion de couple, *ie* de paire ordonnée.

Définition 8. *On définit le couple d'éléments a et b par $(a, b) = \{a, \{b\}\}$.*

Définition 9. *Un ensemble R est une relation si R est un ensemble de couples. Si $(x, y) \in R$, on écrit xRy, et on dit que x et y sont en relation relativement à R.*

Cette définition très simple permet néanmoins de définir tout ce que nous savons sur les relations, fonctions, applications et leurs propriétés en imposant des conditions sur R. Nous ne détaillerons pas tout cela ici car ces constructions ne font pas parties des objectifs du mémoire et ne nous serviront pour la plupart pas pour la suite même si nous utiliserons bien sur constamment la notion de relation et de fonction.

Néanmoins redonnons ici la définition d'une relation d'ordre et d'ordre strict, puis la définition générale de ce qu'est un isomorphisme car ces notions vont être fondamentales pour la suite.

Définition 10. *Une relation d'ordre R sur un ensemble E est une relation qui possède les propriétés suivantes :*
- *Réflexivité : Si $x \in E$, alors $(x, x) \in R$.*
- *Transitivité : Si $(x, y) \in R$ et $(y, z) \in R$, alors $(x, z) \in R$.*
- *Antisymétrie : Si $(x, y) \in R$ et $(y, x) \in R$, alors $x = y$.*

Définition 11. *Une relation d'ordre stricte R' sur un ensemble E est une relation qui possède les propriétés suivantes :*
- *Transitivité : Si $(x, y) \in R'$ et $(y, z) \in R'$, alors $(x, z) \in R'$.*
- *Asymétrie : $(x, y) \in R'$ et $(y, x) \in R'$ ne peuvent pas être simultanément vraies.*

Un ensemble muni d'une relation d'ordre est dit ensemble ordonné.

Définition 12. *Soit un ensemble A muni d'une famille de relation R_i, et un ensemble B muni d'une famille de relation S_i où $i \in E$ un ensemble quelconque. Supposons de plus que si R_i est une relation n-aire sur A alors la relation S_i sur B est également une relation n-aire.*

Alors on dit qu'une bijection f de A dans B est un isomorphisme entre A et B si f préserve la structure de ces ensembles, ie :

$$\forall i \in E, \quad R_i(x_1, x_2, ..., x_n) \text{ si et seulement si } S_i(f(x_1), f(x_2), ..., f(x_n))$$

Par exemple si $<$ est l'ordre usuel de $\mathbb{Q}$, la fonction de $(\mathbb{Q}, <)$ dans $(\mathbb{Q}, <)$ qui à x associe $x + 1$ est un isomorphisme.

S'il existe un isomorphisme entre deux ensembles ordonnés, on dit qu'il sont isomorphes.

Chapitre 2

Nombres Naturels

Dieu fit le nombre entier, le reste est l'oeuvre de l'Homme...
Léopold Kronecker

2.1 Introduction aux nombres naturels

Qu'est ce qu'un nombre naturel ? Nous ne prétendons pas bien sur répondre à cette question philosophique, mais pour développer notre théorie nous allons devoir en donner une définition ensembliste. On voudrait par exemple que le nombre naturel 2 soit défini par un ensemble comportant "2" éléments conformément à notre intuition. Or si on peut facilement dire si un ensemble possède un, deux ou trois éléments, nous pouvons donner beaucoup d'exemples de tels ensembles. Nous allons voir qu'il existe une façon naturelle de faire un choix. La construction suivante est dûe à John von Neumann, un mathématicien et physicien américain d'origine hongroise.

Pour définir 0 nous nous tournons naturellement vers le seul ensemble qui ne possède aucun élément, et on pose donc

$$0 = \emptyset$$

Les ensembles contenant un seul élément sont les ensembles de la forme $\{x\}$ où x est un ensemble (les singletons). Comment choisir un représentant ? Le seul objet de notre théorie que nous avons défini pour l'instant étant l'ensemble $0 = \emptyset$ il semble naturel de poser

$$1 = \{\emptyset\}$$

Et dès lors que nous avons deux objets particuliers différents de défini (0 et 1), il semble encore une fois naturel de poser

$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$$

Nous allons continuer de cette façon ce qui nous donne

$$3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

$$4 = \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$$

...

L'idée est intéressante mais pas encore totalement satisfaisante. car nous pouvons avec cette méthode définir des nombres naturels aussi grands que nous le voulons, mais pas le concept de nombre naturel lui-même. En effet, nous ne pouvons pas définir un nombre naturel comme étant l'ensemble des nombres naturels plus petits car une telle définition fait appel au concept qu'elle essaie justement de définir !

Pour contourner cet obstacle nous allons en fait d'abord définir l'ensemble des entiers naturels, et donc en suite simplement dire que les nombres naturels sont les éléments de cet ensemble. Pour cela remarquons que chacun des nombres naturels que nous avons construit est égal à l'union de son prédécesseur et du singleton qui contient son prédécesseur, par exemple $2 = 1 \cup \{1\}$. On pose alors les définitions suivantes.

Définition 13. *On appelle successeur de x et on note $S(x)$ l'ensemble $x \cup \{x\}$.*

Si n est un entier naturel, $S(n)$ est l'entier qui le succède immédiatement, on utilise alors la notation suggestive $n + 1$ pour désigner $S(n)$. Notons bien qu'il ne s'agit pour l'instant que d'une notation, même si nous verrons qu'elle est compatible avec l'opération d'addition des nombres naturels qui sera définie à la fin du chapitre.

Définition 14. *Un ensemble I est dit inductif si il possède les deux propriétés suivantes :*

- $0 \in I$.
- *Si $n \in I$, alors $(n + 1) \in I$.*

Nous sommes proches de notre but maintenant que nous avons défini les ensembles inductifs. En effet nous savons que tout ensemble inductif doit contenir l'ensemble des nombres naturels. En fait l'ensemble des nombres naturels tel que nous voulons le construire est précisement le plus petit, au sens de l'inclusion, des ensembles inductifs, c'est à dire celui qui ne contient pas d'autre ensemble que 0 et ceux construit par l'opération successeur. On pose donc la définition suivante :

Définition 15. *On appelle ensemble des nombres naturels l'ensemble*

$$\mathbb{N} = \{n | n \in I, \text{ pour tout ensemble inductif } I\}$$

Les éléments de $\mathbb{N}$ sont appelés *nombres naturels*. Ainsi un ensemble est un nombre naturel si et seulement si il appartient à tout ensemble inductif. Remarquons que nous devons justifier l'existence de cet ensemble. Cela est facile avec le schéma d'axiome de compréhension.

Démonstration. Si on note $P(n)$ la propriété de n : "$n \in I$, pour tout ensemble inductif I." et si E est un ensemble inductif quelconque alors on a :

$$\mathbb{N} = \{n \in E | P(n)\}$$

□

Il reste néanmoins une question primordiale ! Existe-il un ensemble inductif ? Sans l'axiome de l'infini la réponse serait non dans le sens où on ne pourrait pas prouver l'existence d'un ensemble infini à l'aide des autres axiomes, qui à partir d'ensembles finis ne peuvent prouver que l'existence d'autres ensembles finis (voir chapitre suivant pour plus de détails sur ce point). Nous utilisons donc ici cet axiome comme une sorte de porte d'entrée pour l'infini, ce qui est la motivation première de la théorie des ensembles.

2.2 Propriétés des nombres naturels

Le théorème d'induction Le théorème d'induction est une conséquence immédiate de notre construction des nombres naturels, il en est donc l'outil fondamental pour leur étude.

Théorème 2.1 (Théorème d'Induction)**.** *Soit $P(x)$ une propriété de x qui peut éventuellement dépendre d'autres paramètres.*
(1) $P(0)$ est vraie. Si :
(2) Pour tout entier naturel n, $P(n) \Rightarrow P(n+1)$.
alors P est vraie pour tous les entiers naturels.

Démonstration. Soit l'ensemble $A = \{n \in \mathbb{N} | P(n)\}$. A est un ensemble inductif d'après les deux hypothèses. Donc $\mathbb{N} \subseteq A$. Et comme par construction $A \subseteq \mathbb{N}$ ces deux ensembles sont égaux, c'est à dire que P est vraie pour tout $n \in \mathbb{N}$. □

L'ordre dans $\mathbb{N}$

On remarque en observant la façon dont nous les avons construits que chaque entier naturel appartient à ceux qui lui sont plus grands, et aussi qu'un entier naturel contient tout ceux qui lui sont plus petits. En fait les entiers naturel sont ordonnés par l'appartenance.

Définition 16. *La relation d'ordre usuelle dans $\mathbb{N}$ est définie par : $m \prec n$ si et seulement si $m \in n$.*

Montrons d'abord ce petit lemme qui sera utile par la suite et qui fournit un bon exemple de démonstration à l'aide du principe d'induction.

Lemme 2.1. *$0 \leq n$, pour tout nombre naturel n.*

Démonstration. La preuve se fait avec l'aide du principe d'induction et en considérant la propriété $P(x)$: "$0 \leq x$". Nous allons montrer respectivement les deux conditions d'application du théorème ce qui prouvera la véracité de la proposition pour tout nombre naturel.

$0 = 0$ donc $0 \leq 0$. Ainsi $P(0)$ est vraie.

Supposons que $0 \leq n$, alors par définition soit $0 \prec n$ soit $0 = n$. Mais dans chaque cas $0 \in n \cup \{n\} = n + 1$, donc $0 \prec n + 1$. Ainsi $P(n) \Rightarrow P(n+1)$. □

Nous allons maintenant démontrer le résultat important de cette partie qui montre que l'ordre que nous avons défini dans $\mathbb{N}$ possède bien les propriétés que nous pouvons attendre de lui.

Théorème 2.2. *$(\mathbb{N}, \prec)$ est un ensemble totalement ordonné.*

Démonstration. Preuve de la transitivité : Soit m, n, p trois entiers naturels tels que $m \prec n$ et $n \prec p$. Nous devons montrer que $m \prec p$. Nous allons raisonner par induction sur p. Soit $[\forall m, n \in \mathbb{N}, (m \prec n \wedge n \prec x) \Rightarrow (m \prec x)]$ une propriété de x que nous nommerons $P(x)$.

$P(0)$: affirme que $\forall m, n \in \mathbb{N}$, $m \prec n$ et $n \prec 0$ implique que $m \prec 0$. Or d'après le lemme 2.1 il n'existe pas d'entier naturel n tel que $n \prec 0$ donc l'affirmation est trivialement vraie.

$P(p) \Rightarrow P(p+1)$: Nous devons montrer que $m \prec n$ et $n \prec p+1$ implique $m \prec p+1$. Or $n \prec p+1$ signifie par définition que $n \in p+1 = p \cup \{p\}$ donc que $n \in p$ ou que $n = p$. Si $n \in p$, ie $n \prec p$ alors $P(p)$ qui est notre hypothèse d'induction nous permet de dire que $m \prec p$, et donc que $m \in p \cup \{p\} = p+1$. Si $n = p$, alors comme $m \prec n$, $m \prec p$ et donc $m \in p+1$. Dans les deux cas on a bien $m \prec p+1$.

Donc $P(p)$ est vraie quel que soit $p \in \mathbb{N}$, ce qui est précisement l'énoncé de la transitivité.

Preuve de l'asymétrie : Nous devons montrer que pour tout $m, n \in \mathbb{N}$, $m \prec n$ et $n \prec m$ ne peuvent pas être vraies conjointement. Si c'était le cas, d'après la transitivité de $\prec$ on aurait $m \prec m$. Il nous faut maintenant montrer que cela ne peut jamais être vrai car comme nous raisonnons par l'absurde exhiber un contre exemple ne serait pas suffisant. Procédons par induction.

$0 \prec 0 \Leftrightarrow \emptyset \in \emptyset$ ce qui est faux.

Admettons que $m \prec m$ est faux pour un entier m. Montrons que $m+1 \prec m+1$ est également faux. Supposons $m+1 \prec m+1$, alors soit $m+1 \in m$, ie $m+1 \prec m$ soit $m+1 = m$. Si $m+1 = m$ on a $m \prec m$ ce qui est faux par hypothèse d'induction, donc on devrait avoir $m+1 \prec m$. Or comme on a toujours $m \prec m+1$ ceci conduit par transivité à $m \prec m$ ce qui est encore faux par hypothèse d'induction. Donc $m+1 \prec m+1$ ne peut pas être vraie, ce qui conclut la preuve par induction est donc la preuve de l'asymétrie de $\prec$.

Preuve que $\prec$ est un ordre total : Nous devons montrer que $\forall m, n \in \mathbb{N}$, ou bien $m \prec n$, ou bien $m = n$, ou bien $n \prec m$. Nous allons un fois de plus raisonner par induction, mais cette fois pour prouver le second point du principe d'induction nous aurons à effectuer une deuxième induction sur l'autre entier ! Commençons avec l'entier n.

On a bien d'après le lemme 2.1 $\forall m \in \mathbb{N}$, $m \geq 0$. Donc $m \prec 0$ ou $m = 0$ ou $0 \prec m$.

Supposons maintenant que la propriété est vraie pour un entier n. Montrons alors qu'elle est vraie pour son successeur, c'est à dire que $\forall m \in \mathbb{N}$, ou bien $m \prec n+1$, ou bien $m = n+1$, ou bien $n+1 \prec m$. Pour cela on utilise l'hypothèse d'induction et on fait une disjonction de cas : Si $m \prec n$, comme $n \prec n+1$, alors par transitivité $m \prec n+1$. Si $m = n$ alors comme $n \prec n+1$, $m \prec n+1$. Il reste le dernier cas où $n \prec m$, on va montrer que cela implique $n+1 \leq m$, c'est à dire que $n+1 \prec m$ ou bien $n+1 = m$ ce qui terminera la preuve.

On doit prouver ceci pour tout entier naturel m, on va donc de nouveau à ce stade procéder par induction sur m : Si $m = 0$, il n'y a rien à montrer car $0 = \emptyset$ ne contient aucun élément. Supposons enfin que cette propriété est vraie pour un entier m, nous allons montrer qu'elle doit l'être pour l'entier $m+1$. En effet, si $n \prec m+1$ alors $n \prec m$ ou bien $n = m$. Dans le premier cas par l'hypothèse d'induction alors $n+1 \leq m \prec m+1$, donc $n+1 \leq m+1$. Dans le deuxième cas alors bien sur $n+1 = m+1$ et donc $n+1 \leq m+1$.

Ainsi cette propriété est vraie pour tout entier m, ce qui termine également la preuve que $\prec$ est un ordre total dans $\mathbb{N}$, et donc notre démonstration.

□

L'ensemble des nombres naturels possède également muni de cet ordre une propriété primordiale pour la suite de notre étude. Nous la donnons dans le prochain théorème.

Définition 17. *Un ordre total $\prec$ dans un ensemble A est qualifié de bon-ordre si chaque sous ensemble non vide de A possède un plus petit élément. L'ensemble ordonné $(A, \prec)$ est alors dit bien-ordonné.*

Théorème 2.3. *L'ensemble $(\mathbb{N}, \prec)$ est bien-ordonné.*

Démonstration. Soit X un sous ensemble non vide de $\mathbb{N}$. Raisonnons par l'absurde. On suppose que X n'a pas de plus petit élément, et on considère alors $\mathbb{N} - X$. Remarquons que si pour tout $k \prec n$, $k \in \mathbb{N} - X$ alors n appartient aussi à $\mathbb{N} - X$ car sinon il serait le plus petit élément de X. Donc le théorème d'induction (ici utilisé sous une forme un peu différente mais équivalente) implique que tout nombre naturel appartient à $\mathbb{N} - X$, *ie* $X = \emptyset$ ce qui contredit notre hypothèse. □

2.3 Le théorème de récursion

Théorème 2.4 (Théorème de récursion)**.** *Soit A un ensemble, a un élément de A, et f une fonction de $A \times \mathbb{N}$ dans A. Il existe une unique suite infini $U : \mathbb{N} \to A$ telle que :*
(1) $U_0 = a$;
(2) $U_{n+1} = f(U_n, n)$ pour tout $n \in \mathbb{N}$.

Démonstration. Admis □

Le théorème de récursion est le deuxième outil fondamental introduit dans ce chapitre. La preuve de ce théorème nécessite à plusieurs reprises l'utilisation du théorème d'induction et découle donc d'une certaine façon de la nature intrinsèque des nombres naturels.

Il nous reste un point primordial à éclaircir avant que nous arrivions au terme de ce chapitre : remarquons que nous n'avons pas encore parlé des opérations arithmétiques sur les nombres naturels, l'addition et la multiplication. Ces opérations arithmétiques sont des opérateurs binaires sur $\mathbb{N}$, c'est à dire des fonctions de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$. Prouver leurs existences nécessite l'utilisation d'une version un peu différente du théorème de récursion pour les fonctions de deux variables que nous énonçons maintenant :

Théorème 2.5 (Version paramètrique du théorème de récursion)**.** *Soit $a : M \to A$ et $g : M \times A \times \mathbb{N} \to A$ des fonctions. Il existe une unique fonction $f : M \times \mathbb{N} \to A$ telle que :*
(1) $f(m, 0) = a(m)$, $\forall m \in M$;
(2) $f(m, n+1) = g(m, f(m, n), n)$, $\forall n \in \mathbb{N}, \forall m \in M$.

Démonstration. Admis □

Nous pouvons maintenant définir puis prouver l'existence des opérations $+$ et $\times$.

Théorème 2.6. *Il existe une unique fonction* $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *telle que :*
(1) $+(m, 0) = m$, $\forall m \in \mathbb{N}$ *;*
(2) $+(m, S(n)) = S(+(m, n))$, $\forall m, n \in \mathbb{N}$.

Démonstration. On applique simplement la version paramètrique du théorème de récursion avec $A = M = \mathbb{N}$, a l'identité sur $\mathbb{N}$ et g la fonction telle que $g(m, x, n) = S(x)$, $\forall m, x, n \in \mathbb{N}$. □

On constate que la notation que nous avions adopté pour l'opération successeur et bien compatible avec cette définition. (On prend $n = 0$)

Théorème 2.7. *Il existe une unique fonction* $\times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *telle que :*
(1) $\times(m, 0) = 0$, $\forall m \in \mathbb{N}$ *;*
(2) $\times(m, n + 1) = \times(m, n) + m$, $\forall m, n \in \mathbb{N}$.

Démonstration. On applique encore la version paramètrique du théorème de récursion avec $A = M = \mathbb{N}$, et cette fois a la fonction nul sur $\mathbb{N}$ et g la fonction telle que $g(m, x, n) = x + m$, $\forall m, x, n \in \mathbb{N}$. □

On défini enfin l'exponentiation des nombres naturels :

Théorème 2.8. *Il existe une unique fonction* $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *telle que :*
(1) $e(m, 0) = 1$, $\forall m \in \mathbb{N}$ *;*
(2) $e(m, n + 1) = e(m, n) \times m$, $\forall m, n \in \mathbb{N}$.

On note $e(a, b)$ de façon usuelle : a^b.

Démonstration. Cette fois la version paramètrique du théorème de récursion est appliquée avec $A = M = \mathbb{N}$, a la fonction constante de valeur 1 sur $\mathbb{N}$ et g la fonction telle que $g(m, x, n) = x \times m$, $\forall m, x, n \in \mathbb{N}$. □

Chapitre 3

Premières classifications des ensembles

Ce chapitre, et plus particulièrement la première section, introduit un concept qui me paraît être une des grandes idées de la théorie des ensembles. Aussi ai-je choisi de commencer cette section avec une petite discussion pour justifier l'introduction de ce concept.

"Combien d'éléments cet ensemble possède t'il ?"...N'est-ce pas une des premières questions qui nous vient à l'esprit à propos d'un ensemble ?
Nous pouvons répondre facilement à cette question de façon assez intuitive pour beaucoup d'ensembles comme par exemple $\{\emptyset\}$ ou $\{\{\emptyset, \{\emptyset\}\}, \emptyset\}$. Mais la question devient plus ardue lorsqu'il s'agit de le faire pour certains ensembles comportant "beaucoup plus" d'éléments comme par exemple $\mathbb{N}$.

Néanmoins, dans le cas de tels ensembles si nous ne pouvons immédiatement quantifier leurs tailles, nous pouvons les comparer. On pourrait par exemple se demander s'il y a plus d'entiers pairs ou d'entiers impairs ? Intuitivement nous avons envie de dire qu'il y en a autant car à chaque entier pair on peut associer l'entier impair qui le suit immédiatement. Et on peut faire de même dans le cas de "petit" ensemble : Remarquons en effet que pour dire que les ensembles $\{\emptyset, \{\emptyset\}\}$ et $\{\{\emptyset\}, \{\{\emptyset\}\}\}$ ont la même taille on peut, plus simplement que de compter le nombre d'éléments de chacun, constater qu'à l'élément $\emptyset$ du premier ensemble on peut associer l'élément $\{\emptyset\}$ du second ensemble et qu'à l'élément $\{\{\emptyset\}\}$ du premier ensemble on peut associer l'élément $\{\{\{\emptyset\}\}\}$ du second.

3.1 Cardinalité des ensembles

La réflexion menée en introduction du chapitre amène à poser la définition suivante :

Définition 18. *On dit que deux ensembles A et B sont équipotents (ou ont le même cardinal), et on note $|A| = |B|$, si les ensembles A et B sont en bijection.*

Intuitivement, A et B ont la même "taille", ou même "puissance" ; ce qui signifie pour les ensembles finis, nous le verrons, que "A et B possèdent le même nombre d'éléments".

Et il est facile de vérifier que la notion d'équipotence possède les propriétés d'une relation d'équivalence.

Définition 19. *On dit que A est subpotent (a un cardinal inférieur ou égal) à B si il existe une injection de A dans B. On note ceci $|A| \leq |B|$.*

On écrit aussi $|A| < |B|$ si $|A| \leq |B|$ et $|A| \neq |B|$.

Lemme 3.1.

- *Si $|A| \leq |B|$ et $|A| = |C|$, alors $|C| \leq |B|$.*
- *Si $|A| \leq |B|$ et $|B| = |C|$, alors $|A| \leq |C|$.*
- $|A| \leq |A|$.
- *Si $|A| \leq |B|$ et $|B| \leq |C|$, alors $|A| \leq |C|$.*

Ce lemme prouve la réflexivité et la transitivité de $\leq$. Nous allons maintenant voir avec le prochain théorème que l'antisymétrie est également satifaite. Ce théorème est tout à fait non trivial, nous aurons besoin du lemme suivant :

Lemme 3.2. *Si $A_1 \subseteq B \subseteq A$ et $|A_1| = |A|$, alors $|B| = |A|$.*

Démonstration. Soit f une bijection de A dans A_1. On définit par récursion deux suites d'ensembles $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ de la façon suivante :

$$A_0 = A, \quad B_0 = B,$$

et pour tout nombre naturel n,

$$A_{n+1} = f[A_n], \quad B_{n+1} = f[B_n].$$

Comme par hypothèse $A_1 \subseteq B \subseteq A$, c'est à dire $A_1 \subseteq B_0 \subseteq A_0$, on a par construction des suites $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$: $A_{n+1} \subseteq A_n$, pour tout $n \in \mathbb{N}$ (cela nécessite en toute rigueur une induction).

On pose alors

$$C_n = A_n - B_n,$$

et

$$C = \bigcup_{n\in\mathbb{N}} C_n, \quad D = A - C.$$

Toujours par construction, on a $f[C_n] = C_{n+1}$, donc

$$f[C] = \bigcup_{n\in\mathbb{N}} C_n.$$

On peut alors définir la fonction de A dans B suivante :

$$g(x) = \begin{cases} f(x) & si\ x \in C; \\ (x) & si\ x \in D. \end{cases}$$

Les restrictions de g à C et D sont des injections, et leurs ensembles images sont disjoints, donc g est une bijection de A dans $f[C] \cup D = B$.

□

Théorème 3.1 (Théorème de Cantor-Bernstein)**.** *Si $|X| \leq |Y|$ et $|Y| \geq |X|$, alors $|X| = |Y|$*

Démonstration. Par hypothèse nous avons une injection f de X dans Y et une injection g de Y dans X. Montrons que $|X| = |Y|$: $f \circ g$ et une injection de X dans X et $g[f[X]] \subseteq g[Y] \subseteq X$. Or comme f et g sont injective, $|g[f[X]]| = |X|$. Donc d'après le lemme 3.2, $|g[Y]| = |X|$. Et comme $|g[Y]| = |Y|$ (g est injective) on a bien $|Y| = |X|$. □

Étant réflexive, transitive et antisymétrique, $\leq$ se comporte ainsi comme une relation d'ordre sur les classes d'équivalences d'ensembles équipotents ! Une question naturel est alors de savoir si cet ordre est total, c'est à dire si pour tout ensemble A et B, on a $|A| \leq |B|$ ou $|B| \leq |A|$. La réponse à cette question sera apporté dans le Chapitre 6 sur l'Axiome du choix ; nous ne l'utiliserons donc pas d'ici là.

Nous allons terminer cette section en démontrant un résultat fondamental dû à Cantor dont nous aurons l'occasion de reparler.

Théorème 3.2 (Théorème de Cantor)**.** *Pour tout ensemble X, $|P(X)| > |X|$.*

Démonstration. Nous devons prouver que pour tout ensemble X, $|X| \leq |P(X)|$ et $|X| \neq |P(X)|$. Comme il existe clairement une injection de X dans $P(X)$ (prenez par exemple l'application qui à $x \in X$ associe $\{x\} \in P(X)$), il suffit de monter qu'il n'existe pas de surjection de X dans $P(X)$, car ainsi il n'existe pas de bijection entre X et $P(X)$, ie $|X| \neq |P(X)|$.

Soit f une quelconque fonction de X dans $P(X)$. On introduit l'ensemble $A = \{x \in X | x \notin f(x)\}$. $A \subseteq X$ et donc $A \in P(x)$. Si f est surjective alors il existe $a \in X$ tel que $f(a) = A$. Deux cas possibles : Soit $a \in A$, alors on doit avoir $a \notin f(a) = A$; impossible. Soit $a \notin A$, on a $a \notin f(a) = A$, donc $a \in A$; impossible également. Donc f n'est pas surjective. □

Certains auront remarqué que nous venons de mettre en évidence les premières propriétés de la cardinalité sans pour autant définir ce qu'est le cardinal d'un ensemble. Il est possible de continuer à étudier les propriétés de l'équipotence et de la subpotence en considérant simplement ce qui a été défini (les deux ensembles sont en bijection ; il existe une injection de l'un dans l'autre). Néanmoins l'objet de ce mémoire, la construction des nombres cardinaux, exige que l'on définisse $|E|$, le cardinal de l'ensemble E, comme un objet de notre théorie, *ie* un ensemble, pour chaque ensemble E. Nous aimerions donc bien trouver une famille d'ensembles qui fournirait de tels représentants, c'est à dire qui vérifie les propriétés suivantes :

- À chaque ensemble E on peut associer un unique représentant, appelé son nombre cardinal, noté $|E|$
- E et F sont équipotents si et seulement si $|E| = |F|$.

Des représentants pour certains types d'ensembles pourons déjà être exhibé dans la suite de ce chapitre.

3.2 Ensembles finis

Définition 20. *Un ensemble E est dit fini s'il est équipotent avec un nombre naturel $n \in \mathbb{N}$. On définit alors également $|E| = n$, et on dit que E possède n éléments.*

Définition 21. *Un ensemble est dit infini s'il n'est pas fini.*

Lemme 3.3. *Il n'existe pas de bijection d'un entier naturel n dans un de ses sous-ensembles propre.*

Démonstration. La preuve se fait par induction sur n.
Pour $n = 0$ c'est trivialement vrai. Supposons que c'est vrai pour un entier n. Si ce n'est pas vrai pour l'entier $n+1$, il existe une bijection f de $n+1$ dans $X \subset n+1$. Il y a deux cas possibles : Soit $n \in X$, soit $n \notin X$.

Si $n \notin X$, alors $X \subseteq n$ (linéarité de l'ordre dans N) et la restriction de f à n et une bijection de n dans un sous-ensemble propre de n $(X - \{f(n)\})$. Contradiction avec l'hypothèse d'induction.

Si $n \in X$, alors il existe $k \leq n$ tel que $n = f(k)$. On considère la fonction g sur n définie comme suit :

$$g(i) = \begin{cases} f(i) & \text{pour tout } i \neq k,\ i \prec n \\ f(n) & \text{si } i = k \prec n \end{cases}$$

Alors g est une bijection de n dans $X - \{n\}$ qui est un sous-ensembe propre de n, ce qui contredit également notre hypothèse d'induction. Donc c'est vrai pour l'entier $n+1$.

□

Corollaire 3.4. $\mathbb{N}$ *est infini.*

Démonstration. L'opération successeur définit une bijection de $\mathbb{N}$ dans un de ses sous-ensembles propre $(\mathbb{N} - \{0\})$. □

La définition 20 conformément à notre intuition définit les nombres cardinaux des ensembles qui ne comportent qu'un nombre fini d'éléments comme le nombre de ses éléments. Montrons donc que les nombres naturels forment une famille apte à représenter les nombres cardinaux des ensembles finis :

Démonstration. Soit un ensemble fini X.

Existence et unicité du nombre cardinal de X :
L'existence est une conséquence immédiate de la définition. L'unicité : Supposons que $|X| = m$ et que $|X| = n$ avec m et n deux entiers naturels différents. Alors X est en bijection avec m et n, et il existe ainsi une bijection entre m et n. Comme ces deux entiers sont différent, on sais également que l'un est un sous-ensemble propre de l'autre (voir Chapitre sur les nombres naturels), ce qui est impossible à cause du lemme précédent.

Reste à voir que si X et Y deux ensembles finis, X et Y sont équipotent ssi $|X| = |Y|$: Si X et Y sont équipotent, alors X et Y sont forcément en bijection avec le même entier naturel n (facile). Alors $|X| = n = |Y|$.
Si $|X| = |Y|$ alors X et Y sont tout deux équipotent à un même entier naturel par définition, et sont donc équipotent entre eux. □

Vient ensuite toute une série de théorèmes prouvant que l'union, l'image par une fonction, etc... d'ensembles finis restent finis. Nous nous contenterons de donner ici quelques-uns de ces résultats importants qui pourront nous servir par la suite sans apporter la démonstration de chacun.

Théorème 3.3. *Si X est fini et admet Y comme sous-ensemble, alors Y est fini. De plus, $|Y| \leq |X|$.*

Démonstration. Si X est fini, il est en bijection avec un nombre naturel n ; on peut supposer que $X = \{x_0, x_1, ..., x_{n-1}\}$, où les x_i sont deux à deux distincts, et que Y est non vide sinon le théorème est trivial. Pour montrer que Y est fini il suffit de construire une suite finie qui a pour ensemble image Y. On procède par récursion. Soit la suite définie par :

$$k_0 = \text{le plus petit } k \text{ tel que } x_k \in Y;$$

$$k_{i+1} = \text{le plus petit } k \text{ tel que } k \succ k_i, \text{ et } k \prec n, \text{ et } x_k \in Y. \text{ (S'il existe !)}$$

Cette suite est évidemment finie puisque tous ses éléments sont des éléments de X qui est fini, et son ensemble image est exactement Y. De plus cet ensemble image peut s'écrire, quitte à réorganiser la numérotation, $Y = \{x_0, x_1, ..., x_{m-1}\}$ avec $m \preceq n$ comme $Y \subseteq X$. Donc $|Y| \leq |X|$. □

Théorème 3.4. *Si X est fini et f est une fonction, alors $f[X]$ est fini. De plus $|f[X]| \leq |X|$.*

Théorème 3.5. *Soit S un système d'ensembles. Si S est fini et que tout ensemble $X \in S$ est fini, alors $\bigcup S$ est fini.*

Démonstration. On procède par induction sur le nombre d'ensembles dans S.

S'il n'y a qu'un ensemble X dans S alors $\bigcup S = X$ qui est fini par hypothèse.

Supposons maintenant que la propriété soit vraie si S contient n ensembles. On doit montrer que cela implique que la propriété est vraie lorsque S contient $n+1$ ensembles. On a :

$$\bigcup_{i=0}^{n+1} S = \bigcup_{i=0}^{n} X_i \cup X_{n+1}$$

Or par hypothèse d'induction, $\bigcup_{i=0}^{n} S$ est fini, et par hypothèse du théorème X_{n+1} est fini, donc on a ramené le problème à montrer que l'union de deux ensembles finis est fini.

Soient donc X et Y deux ensembles finis. On peut supposer $X = \{x_0, x_1, ..., x_{n-1}\}$ et $Y = \{y_0, y_1, ..., y_{n-1}\}$. On procède comme dans la preuve précédente en construisant une suite finie qui a pour ensemble image $X \cup Y$:

C'est le cas de la suite z telle que

$$z_i = x_i \text{ pour } 0 \preceq i \prec n, \qquad z_i = y_{i-n} \text{ pour } n \preceq i \prec n+m.$$

Ce qui termine la preuve. □

Théorème 3.6. *Si X et Y sont des ensembles finis, alors $X \times Y$ est fini, et $|X \times Y| = |X| \times |Y|$.*

3.3 Ensembles dénombrables

Définition 22. *Un ensemble D est dit dénombrable s'il est en bijection avec $\mathbb{N}$ l'ensemble des entiers naturels, c'est à dire si $|D| = |\mathbb{N}|$. Un ensemble D est au plus dénombrable si $|D| \leq |\mathbb{N}|$.*

Notons qu'un ensemble est dénombrable si et seulement si il existe une bijection de $\mathbb{N}$ dans celui ci, c'est à dire si et seulement si il est l'ensemble image d'une suite infinie et injective.

Les résultats de cette section seront pour la plupart exposés sans être démontrés.

Théorème 3.7. *Un sous ensemble infini d'un ensemble dénombrable est dénombrable.*

Démonstration. Soit A un ensemble dénombrable et B un sous ensemble infini de A. Il existe une suite infinie et injective $(a_n)_{n\in\mathbb{N}}$ qui a pour ensemble image A. On définit grâce au théorème de récursion la suite $(b_n)_{n\in\mathbb{N}}$ de la façon suivante :

$b_0 = a_{k_0}$ où k_0 est le plus petit k tel que $a_k \in B$. Et $b_{n+1} = a_{k_{n+1}}$, où k_{n+1} est le plus petit k tel que $a_k \in B$ et $a_k \neq b_i$, pour tout $i \preceq n$; ce nombre naturel k existe toujours comme B est infini par hypothèse.

On a bien construit une suite infinie injective, et qui a pour ensemble image B, donc B est dénombrable d'après la remarque qui suit la définition 22. □

Corollaire 3.5. *Un ensemble est au plus dénombrable si et seulement si il est fini ou dénombrable.*

Théorème 3.8. *L'ensemble image d'une suite $(a_n)_{n\in\mathbb{N}}$ est au plus dénombrable, c'est à dire d'après le corollaire fini ou dénombrable.*

Théorème 3.9. *L'union de deux ensembles dénombrables est dénombrable.*

On en déduit par induction le corollaire suivant :

Corollaire 3.6. *L'union d'un système fini d'ensembles dénombrables est dénombrable.*

Théorème 3.10. *Le produit cartésien de deux ensembles dénombrables est dénombrable.*

Et de la même façon que ce qui a été fait pour les ensembles finis, on en déduit facilement par induction le corollaire suivant :

Corollaire 3.7. *pour tout nombre naturel n, $\mathbb{N}^n$ est dénombrable.*

On ne peut pas généraliser les deux théorèmes précédents pour des systèmes dénombrables sans l'aide l'axiome du choix, tout le problème consiste en effet à pouvoir choisir une numérotation des éléments de chacun des ensembles dénombrables du système dénombrable. Si un tel choix est possible les résultats sont vrais, ce que montre par exemple le théorème suivant pour l'union :

Théorème 3.11. *Soit $\{A_n | n \in \mathbb{N}\}$ un système dénombrable d'ensembles au plus dénombrables tel qu'il existe un système d'énumérotation des A_n. Alors $\bigcup_{n\in\mathbb{N}} A_n$ est au plus dénombrable.*

Théorème 3.12. *Si A est un ensemble dénombrable alors l'ensemble de toutes les suites finis d'éléments de A est dénombrable.*

Corollaire 3.8. *L'ensemble de tous les sous ensembles finis d'un ensemble dénombrable est dénombrable.*

Comme pour le cas particulier des ensembles finis, on peut définir le cardinal des ensembles dénombrables. Nous avons défini les ensembles dénombrables comme étant ceux en bijection avec $\mathbb{N}$; c'est à dire qu'un ensemble est dénombrable s'il a le "même nombre d'éléments" que $\mathbb{N}$. On définit alors simplement le cardinal des ensembles dénombrables comme l'ensemble $\mathbb{N}$ muni de la relation " $\prec$ " d'ordre habituelle (nous verrons ultérieurement pourquoi l'ordre est important).

Définition 23. *Si A est un ensemble dénombrable, $|A| = (\mathbb{N}, \prec)$.*

Avec cette définition $(\mathbb{N}, \prec)$ est donc un nombre cardinal, on utilise la notation $\aleph_0$ pour le désigner. Nous pouvons ici encore prouver que cet ensemble est un bon représentant pour le cardinal des ensembles dénombrables :

Démonstration.
- Pour chaque ensemble dénombrable un unique nombre cardinal lui est associé : $\aleph_0$.
- Deux ensembles dénombrables X et Y sont toujours équipotents (on compose les bijections qui les relient à $\mathbb{N}$) et $|X| = \aleph_0 = |Y|$. □

3.4 Ensembles indénombrables

Nous avons vu lors de la section précédente que beaucoup d'ensembles sont au plus dénombrables. On peut facilement prouver que c'est aussi le cas d'ensembles comme $\mathbb{Z}$ et $\mathbb{Q}$. On se pose alors la question de savoir si tout les ensembles infinis sont dénombrables ? Si c'était le cas le mémoire s'arrêterait ici et je n'aurais donc pas choisi ce sujet ! C'est Cantor qui répondit en premier à cette question en prouvant la non-dénombrabilité de $\mathbb{R}$. Il mit plus tard en évidence l'existence d'infinis toujours "plus grands" avec le théorème qui porte son nom et que nous avons vu en première section de ce chapitre. En effet, on doit avoir $|P(X)| \succ |X|$ pour tout ensemble X. Et c'est justement cette richesse des infinis qui est au coeur de la théorie des ensembles.

Théorème 3.13. $\mathbb{R}$ *est indénombrable.*

Démonstration (Argument diagonal de Cantor) : Il suffit de montrer que l'ensemble E des réels entre 0 et 1 compris est indénombrable. Supposons que E soit dénombrable. On écrit chaque réel sous sa forme décimale, de tel façon à ce qu'aucune écriture ne présente que le chiffre 9 à partir d'un certain rang pour assurer l'unicité de cette écriture décimale. Comme E est dénombrable on peut le mettre en bijection avec $\mathbb{N} - 0$, *ie* on peut associer à chacun de ces réels un nombre naturel strictement positif et réciproquement de façon unique. Chaque élément de E est alors de la forme $0, a_1^n a_2^n a_3^n a_4^n a_5^n ...$ pour un entier $n \geq 1$. Considérons alors le réel $0, b_1 b_2 b_3 b_4 b_5 ...$ tel que $\forall i \geq 1,\ b_i \neq a_i^i$ (par exemple $b_i = 0$ si $a_i^i \neq 0$ et $b_i = 1$ si $a_i^i = 0$). Alors $0, b_1 b_2 b_3 b_4 b_5 ... \notin E$. Contradiction. □

On a donc $|\mathbb{R}| \succ |\mathbb{N}|$, or d'après le théorème de Cantor, $|P(\mathbb{N})| \succ |\mathbb{N}|$ (donc $P(\mathbb{N})$ n'est pas dénombrable !). Nous donnons sans le prouver le théorème suivant qui va quantifier plus précisement les choses :

Théorème 3.14. $|P(\mathbb{N})| = \left|2^{\mathbb{N}}\right| = |\mathbb{R}|$

Ce théorème permet de poser la notation de $2^{\aleph_0}$ pour le cardinal de $\mathbb{R}$. On l'appel le cardinal du continu.

3.5 Définitions alternatives à la finitude, Dedekind infini

Nous terminerons ce chapitre par l'étude de quelques approches alternatives pour définir la notion d'ensemble fini et infini. Nous considérerons leurs pertinences et regarderons si elles sont équivalentes à celle que l'on vient de développer. Nous nous arrêterons particulièrement sur la notion d'ensemble Dedekind infini.

Remarquons qu'aucune des approches suivantes n'engage le concept de nombres naturels.

Définition 24 (première alternative)**.** *Un ensemble A est dit fini si et seulement si il existe une relation d'ordre $\prec$ telle que :*
(a) $\prec$ est un ordre total de A.
(b) Tout sous ensemble non vide de A possède un plus petit et un plus grand élément vis à vis de $\prec$.

Cette définition est assez intuitive, en effet A est un sous ensemble de A. Donc si A est infini on aimerait bien qu'il n'existe pas d'ordre qui puisse donner un plus grand élément, et au contaire si A est fini on veut pouvoir trouver un ordre dans lequel tout sous ensemble admet des "bornes".

Proposition 3.9. *La définition 24 est équivalente à la définition 20 donnée en section 2 de ce chapitre.*

Démonstration. Si X est équipotent à un nombre naturel n, on peut poser $X = \{x_0, x_1, ..., x_{n-1}\}$. On définit alors l'ordre $\prec$ par : $x_0 \prec x_1 \prec ... \prec x_{n-1}$. C'est un ordre linéaire de X, et si Y est un sous ensemble non vide de X, $Y = \{x_i | i \in I\}$ où I est un sous ensemble non vide de n. I possède un $\in$-plus petit élément a et un $\in$-plus grand élément b comme n est $\in$-bien ordonné. Alors x_a est le plus petit élément de Y. En effet supposons qu'il existe $x_{a'} \in Y$ tel que $x_{a'} \prec x_a$; alors a' appartient à I et a' est plus petit (au sens de l'appartenance) que a, ce qui contredit le fait que a est le $\in$-plus petit élément de I. On justifie de même que x_b est le plus grand élément de Y.

Supposons maintenant que $(X, \prec)$ est un ensemble ordonné qui vérifie (a) et (b). Soit a le plus petit élément de X, et soit f la fonction de $X \times \mathbb{N} \to X$ telle que $f(x, n)$ soit le plus petit élément de X plus grand que x (pour tout n). Cette fonction est bien définie à cause des hypothèses sur $(X, \prec)$. Le théorème de récursion prouve alors l'existence d'une suite U d'éléments de X telle que : U_0 soit le plus petit élément de X, et U_{n+1} soit le plus petit élément plus grand que U_n. La suite U parcourt tous les éléments de X et cette suite est nécessairement finie sans quoi l'ensemble $\{U_0, U_1, U_2, ...\}$ serait un sous ensemble de X qui n'admet pas de plus grand élément. Donc $X = \{U_0, U_1, ..., U_m\}$ pour un $m \in \mathbb{N}$ et X est en bijection avec m. □

Définition 25 (deuxième alternative)**.** *Un ensemble A est dit fini si toute famille non vide de parties de A a un élément $\subseteq$-maximal.*

Proposition 3.10. *La définition 25 est équivalente à la définition 20 donnée en section 2 de ce chapitre.*

Démonstration. Soit X un ensemble. Supposons premièrement que $|X| = n$ où $n \in \mathbb{N}$. Si F est une famille de sous ensemble de X ($F \subseteq P(X)$), on considère l'ensemble $E = \{|Y| \mid Y \in F\}$. C'est un sous ensemble de $\mathbb{N}$, il possède un plus grand élément m. L'élément Y_0 de F tel que $|Y_0| = m$ est $\subseteq$-maximal sinon il existerait $Y' \in F$ tel que $Y_0 \subseteq Y'$, et donc $|Y'| \succ |Y_0|$ ce qui contredit le fait que m soit le plus grand élément de E.

Pour prouver la réciproque nous raisonnons par contraposée. Supposons alors que X est infini au sens de notre première définition. On considère l'ensemble $F = \{Y \subseteq X | Y \text{ est fini}\}$. F est une famille de sous ensemble de X, et F ne possède pas d'élément $\subseteq$-maximal : En effet, si Y_0 est un tel élément, soit l'ensemble $Y_1 = Y_0 \cup \{x\}$ où $x \notin Y_0$ (x existe comme X est supposé infini). On a alors $Y_0 \subseteq Y_1$. Contradiction car Y_1 est fini en tant qu'union de deux ensembles finis et appartient donc à F. □

Rappelons nous que $\mathbb{N}$ qui est un ensemble infini est en bijection avec un de ses sous ensembles propre. Et d'un autre côté, il suit du Lemme 3.3 qu'aucun ensemble fini n'est en bijection avec une de ses parties stricte. Ceci suggère une dernière approche que nous allons détailler.

Dedekind infini

Définition 26 (troisième alternative)**.** *Un ensemble est dit Dedekind infini s'il est en bijection avec un de ses sous ensembles propres. Un ensemble est dit Dedekind fini s'il n'est pas Dedekind infini.*

Lemme 3.11. *Tout ensemble dénombrable est Dedekind infini.*

Démonstration. Soit E un ensemble dénombrable. Alors E est équipotent à $\mathbb{N}$, *ie* il existe une bijection f de E dans $\mathbb{N}$. Nous savons également que f^{-1} est une bijection de $\mathbb{N}$ dans E. On se souvient aussi de l'opération successeur qui est une bijection :

$$S : \begin{cases} \mathbb{N} \longrightarrow \mathbb{N} - \{0\} \\ n \longmapsto S(n) \end{cases}$$

Considérons alors la fonction $b = f^{-1} \circ S \circ f$. C'est une bijection (en tant que composée de bijections) qui va de E dans $E - \left\{f^{-1}(0)\right\}$, un sous espace propre de E. Donc E est Dedekind infini. □

Nous allons maintenant démontrer la proposition suivante qui donne une caractérisation importante des ensembles Dedekind infinis.

Théorème 3.15. *Un ensemble est Dedekind infini si et seulement si il admet un sous-ensemble dénombrable.*

Démonstration. Soit X un ensemble.

*) Supposons dans un premier temps que X contient un ensemble dénombrable D. D'après le lemme précédent, il existe une bijection b de D dans une de ses partie strictes. Soit alors l'application suivante :

$$F : \begin{cases} X \longrightarrow F(X) \\ x \longmapsto \begin{cases} x \ si \ x \in X - D \\ b(x) \ si \ x \in D \end{cases} \end{cases}$$

F est une bijection (car b en est une) de X dans un de ses sous ensembles propres. Donc X est Dedekind infini.

**) Supposons maintenant que X est Dedekind infini. Alors il existe une bijection f de X dans $f(X) \subset X$. Soit $D = \{x_n | n \in \mathbb{N}\}$ où $\forall n \in \mathbb{N}$, $x_{n+1} = f(x_n)$, et $x_0 \in X - f(X)$.

$$Soit \ \varphi : \begin{cases} D \longrightarrow \mathbb{N} \\ x_n \longmapsto n \end{cases}$$

D est un ensemble au plus dénombrable, la preuve sera terminée quand nous aurons montré que φ est une bijection, c'est à dire que D est bien dénombrable. Il suffit pour cela de montrer que tous les $x_i \in D$ sont différents deux à deux.

Montrons donc par induction sur le nombre naturel i que $\{x_0, x_1, ..., x_i\}$ est un ensemble d'éléments deux à deux distincts, pour tout $i \geq 1$.

(1)L'ensemble $\{x_0, x_1\}$ est bien un ensemble d'éléments deux à deux distincts car $x_0 \in X - f(X) \neq x_1 \in f(X)$.

(2) Supposons que $\{x_0, x_1, ..., x_i\}$ est un ensemble d'éléments deux à deux distincts, montrons alors que $\{x_0, x_1, ..., x_i, x_{i+1}\}$ est un ensemble d'éléments deux à deux distincts. Ceci équivaut à montrer que $x_{i+1} \neq x_k, \forall k = 0, ..., i$ d'après notre hypothèse d'induction.

Si $k = 0$ on a bien $x_{i+1} \neq x_k$ car $x_0 \notin f(X)$. Si $k = 1, ..., i$ alors supposons par l'absurde que $x_{i+1} = x_k$, c'est à dire que $f(x_i) = f(x_{k-1})$. Or comme f est une bijection, elle est en particulière injective et on a donc $x_i = x_{k-1}$. Impossible car d'après l'hypothèse d'induction $\{x_0, x_1, ..., x_i\}$ est un ensemble d'éléments deux à deux distincts.

Donc finalement $\{x_0, x_1, ..., x_i, x_{i+1}\}$ est aussi un ensemble d'éléments deux à deux distincts, ce qui termine la preuve. (Remarque : on aurait aussi pu arriver à une contradiction sans utiliser l'hypothèse d'induction une seconde fois en "redescendant" avec l'injectivité de f jusqu'à x_0.)

□

Nous allons prouver deux derniers résultats.

Proposition 3.12. *Soit A et B deux ensembles Dedekind finis. Alors $A \cup B$ et $A \times B$ sont Dedekind finis.*

Démonstration.
- Par l'absurde supposons que $A \cup B$ est Dedekind infini. Alors d'après le théorème que nous venons de démontrer, il existe $D \subseteq A \cup B$ un sous ensemble dénombrable. D possède à priori des éléments dans A, notons D_1 l'ensemble de ces éléments, et dans B, notons D_2 l'ensemble de ces éléments. Si D_1 et D_2 étaient des ensembles finis, alors $D_1 \cup D_2$ serait fini ce qui n'est pas le cas. Ainsi l'un au moins de D_1 ou D_2 est dénombrable, et donc l'un au mois des ensembles A ou B est Dedekind infini. Contradiction.

- Idem pour le produit cartésien car on a vu au début de ce chapitre que si X et Y sont des ensembles finis alors $X \times Y$ est aussi un ensemble fini. □

Proposition 3.13. *Si A est un ensemble infini, alors $P(P(A))$ est Dedekind infini.*

Démonstration. Montrons que $\{S_n \in P(P(A))|n \in \mathbb{N}\}$ où $S_n = \{X \subset A| \, |X| = n\}$ est un sous ensemble dénombrable de $P(P(A))$.

Comme par hypothèse A est infini on peut toujours trouver des sous ensembles de A de cardinal fini n. Les S_n existe donc pour tout $n \in \mathbb{N}$ et sont tous distinct deux à deux.

Ainsi $\varphi : \begin{cases} \{S_n \in P(P(A))|n \in \mathbb{N}\} \longrightarrow \mathbb{N} \\ S_n \longmapsto n \end{cases}$ est une bijection. □

Pour cette dernière approche nous pouvons encore démontrer dans ZFC l'équivalence de la définition avec celle donnée par la définition 20, mais la preuve fait obligatoirement appelle à l'axiome de choix, sans celui-ci on ne peut pas prouver la coïncidence des deux notions.

Chapitre 4

Nombres Ordinaux

Vers l'infini, et au delà !
Buzz l'éclair

On se souvient de l'opération successeur qui nous a permis de contruire les nombres naturels, un à un, puis finalement avec l'aide de l'axiome de l'infini l'ensemble $\mathbb{N}$ lui même. L'opération successeur étant applicable à tout ensemble, une remarque pertinente serait de se demander si on peut continuer le proccessus en prenant les successeurs de $\mathbb{N}$! La poursuite de cette construction va nous permettre d'étendre la notion de nombres naturels au cas infini. Ces nouveaux ensembles seront des outils fondamentaux dans l'objectif qui est le notre.

La première section est consacrée à l'étude des ensembles bien ordonnés qui est un pré-requis indispensable.

4.1 Ensembles bien-ordonnés

Revenons tout d'abord sur la notion d'ensembles bien ordonnés. On se rappelle qu'un ensemble est bien ordonné par une relation d'ordre si celle-ci est totale et si chacun de ses sous ensembles non vides possède un plus petit élément vis a vis de celle-ci. Les ensembles bien ordonnés possèdent cette propriété d'être comparables par leurs "longueurs". Nous préciserons ce que nous entendons par là dans la suite.

Définition 27. *Soit $(E, \prec)$ un ensemble totalement ordonné.*
On dit que $S \subset E$ est un segment initial de E si $\forall s \in S$, $x \prec s \Rightarrow x \in S$.

Lemme 4.1. *Si $(O, \prec)$ est un ensemble bien ordonné et S un segment initial de celui-ci il existe $a \in O$ tel que $S = \{x \in O | x \prec a\} =: O[a]$.*

Démonstration. Soit $C = O - S$ le complémentaire de S dans O. Cet ensemble est non vide (S est un sous ensemble propre de O) et possède donc un plus petit élément que nous nommons a. Si $x \prec a$ alors x ne peut pas appartenir à C car a est le plus petit élément de cet ensemble, donc $x \in S$. Si $x \succeq a$ alors x ne peut pas appartenir à S car sinon a appartiendrait aussi à S comme S est un segment initial. Finalement $S = \{x \in O | w \prec a\}$. □

Lemme 4.2. *Si f est une fonction strictement croissante d'un ensemble bien ordonné $(O, \prec)$ dans lui-même, alors pour tout $x \in O$, $f(x) \succeq x$.*

Démonstration. Supposons que l'ensemble $X = \{x \in O | f(x) \prec x\}$ ne soit pas vide. Alors il a un plus petit élément a, et a vérifie $f(a) \prec a$. Et comme f est strictement croissante, $f(f(a)) \prec f(a)$, et donc $f(a) \in X$. Absurde car a est le plus petit élément de X. □

Proposition 4.3.
(a) Aucun ensemble bien ordonné n'est isomorphe à un de ses segments initiaux.
(b) Tout ensemble bien ordonné admet un unique automorphisme, l'identité.
(c) Si deux ensembles bien ordonnés sont isomorphes alors l'isomorphisme est unique.

Démonstration. Remarquons tout d'abord qu'un isomorphisme f d'un ensemble bien ordonnée $(O, \prec)$ dans un de ses sous ensembles est une fonction strictement croissante : si o_1 et o_2 des éléments de O, $o_1 \prec o_2 \Rightarrow f(o_1) \prec f(o_2)$ car f est un isomorphisme.
(a) Supposons qu'il existe un isomorphisme f de O dans $O\,[a]$ pour un $a \in O$. Comme $f(a) \in O\,[a]\,,\ f(a) \prec a$. Or ceci est impossible d'après le lemme 4.2 car f est strictement croissante.
(b) Soit f un automorphisme de O. f et f^{-1} sont des fonctions strictements croissantes dons pour tout $o \in O$, $f(o) \succeq o$ et $f^{-1}(o) \succeq o \Rightarrow o \succeq f(o)$. Ainsi $\forall o \in O,\ f(o) = o$, *ie* f est l'identité.
(c) Soit f et g deux isomorphismes entre W_1 et W_2. Alors $f \circ g^{-1}$ est un automorphisme de W_2 et c'est donc l'identité, *ie* $f = g$. □

Nous pouvons à présent donner le résultat important de cette section.

Théorème 4.1. *Soit $(W_1, \prec_1)$ et $(W_2, \prec_2)$ deux ensembles bien ordonnés. Exactement une des propositions suivante est vraie :*
- *W_1 et W_2 sont isomorphe.*
- *W_1 et isomorphe à un segment initial de W_2.*
- *W_2 et isomorphe à un segment initial de W_1.*

D'après la proposition 4.3 l'isomorphisme est à chaque fois unique. Nous ne détaillerons pas la preuve de ce théorème.

4.2 Nombres ordinaux

Comme évoqué dans l'introduction du chapitre, les nombres ordinaux pourrons être vu comme une généralisation des nombres naturels. Nous en donnons ici la définition, toujours dûe à John von Neumann, puis investigons leurs propriétés.

Définition 28. *Un ensemble T est dit transitif si tout élément de T est un sous ensemble de T.*

Définition 29. *Un nombre ordinal est un ensemble α tel que :*
(a) α soit transitif.
(b) α soit strictement bien ordonné par $\in_\alpha$.

On dit souvent ordinal au lieu de nombre ordinal. Il est clair que les nombres naturels sont des nombres ordinaux, et il en est de même pour l'ensemble $\mathbb{N}$ des nombres naturels. On prendra plutôt par convention des lettres grèques minuscules pour désigner des nombres ordinaux, on pose donc la définition suivante :

Définition 30. $\omega = (\mathbb{N}, \in)$

Proposition 4.4. *Le successeur d'un nombre ordinal α est aussi un nombre ordinal.*

Démonstration. $S(\alpha) = \alpha \cup \{\alpha\}$ est un ensemble transitif puisque α en est un. De plus $\alpha \cup \{\alpha\}$ est ordonné par l'appartenance, α étant le plus grand élément et également le segment initial engendré par lui même. □

On note une fois de plus $\alpha + 1$ le successeur de α. On constate que certains ordinaux ne peuvent pas être construits par l'opération successeur, comme par exemple ω, on est dons amené à poser la définition suivante :

Définition 31. *On dit que α est un ordinal successeur si il existe β tel que $\alpha = \beta + 1$. On dit que α est un ordinal limite dans le cas contraire.*

Définition 32. *Pour tout ordinal α et β, $\alpha \prec \beta$ si et seulement si $\alpha \in \beta$.*

On étend ainsi l'ordre des nombres naturels défini au chapitre 2. Nous allons maintenant introduire le théorème fondamental qui montre que cet ordre possède toute les propriétés d'un bon ordre.

Lemme 4.5. *Tout élément d'un nombre ordinal est un nombre ordinal.*

Démonstration. Soit $x \in \alpha$ un ordinal. (a) Montrons que x est transitif : Soit u et v tels que $u \in v \in x$. Nous devons montrer que $u \in x$. Comme α est transitif, et $x \in \alpha$, on a $v \in \alpha$, et donc $u \in \alpha$ également. Ainsi u, v, x sont tous des éléments de α qui est bien ordonné par l'appartenance, donc $u \in x$. (b) Montrons que x est bien ordonné par $\in_x$: Comme $x \in \alpha$, $x \subseteq \alpha$. Ainsi la relation $\in_x$ n'est qu'une restriction du bon ordre $\in_\alpha$ de α, donc est un bon ordre. □

Ce lemme prouve que chaque ordinal est égal à l'ensemble des ordinaux qui lui sont inférieurs. Et ainsi qu'un ordinal est un segment initial de tout autre ordinal qui le contient.

Lemme 4.6. *Soient α et β des ordinaux, alors $\alpha \subset \beta$ si et seulement si $\alpha \in \beta$.*

Démonstration. Soit $\alpha \subset \beta$. Alors $\beta - \alpha$ est un sous ensemble non vide de β et possède un plus petit élément γ vis à vis de $\in_\beta$. On a forcément $\gamma \subseteq \alpha$ car sinon par transitivité de β, tout $\delta \in \gamma - \alpha$ serait un élément de $\beta - \alpha$ plus petit que γ. Il suffit maintenant de montrer que $\alpha \subseteq \gamma$ car alors $\alpha = \gamma \in \beta$.

Soit alors $\delta \in \alpha$, montrons que $\delta \in \gamma$: Si ce n'est pas le cas alors soit $\gamma \in \delta$ soit $\gamma = \delta$ (δ et γ appartiennent tout deux à l'ensemble bien ordonné $(\beta, \in)$). Mais ceci implique $\gamma \in \alpha$ comme α est transitif, et contredit le fait que $\gamma \in \beta - \alpha$. □

Théorème 4.2. *Soient α, β, et γ trois ordinaux.*
(a) Si $\alpha \prec \beta$ et $\beta \prec \gamma$ alors $\alpha \prec \gamma$.
(b) $\alpha \prec \beta$ and $\beta \prec \alpha$ ne peuvent être simultanément vraies.
(c) On a soit $\alpha \prec \beta$, soit $\alpha = \beta$, soit $\beta \prec \alpha$.
(d) Tout ensemble non vide de nombres ordinaux possède un plus petit élément vis à vis de $\prec$.

Démonstration.
(a) Immédiat d'après la transitivité de γ.
(b) En effet car sinon par transitivité $\alpha \prec \alpha$, c'est à dire $\alpha \in \beta$ ce que nous avons exclu par définition d'un ordinal (α est strictement bien ordonné).
(c) Si α et β sont des ordinaux on peut vérifier que $\alpha \cap \beta$ est aussi un ordinal (tout élément de $\alpha \cap \beta$ et un élément de α et β, donc est un sous ensemble de α et β, donc est un sous ensemble de $\alpha \cap \beta$, et la restriction d'un bon ordre strict et toujours un bon ordre strict). Or on ne peut pas avoir $\alpha \cap \beta \subset \alpha$ ni $\alpha \cap \beta \subset \beta$ car cela implique respectivement d'après le lemme 4.6 $\alpha \cap \beta \in \alpha$ et $\alpha \cap \beta \in \beta$ et donc $\alpha \cap \beta \in \alpha \cap \beta$ ce qui contredit encore la définition d'un ordinal. Reste alors deux cas possibles : Soit $\alpha \cap \beta = \alpha$, alors $\alpha \subseteq \beta$ et donc d'après le lemme 4.6 on a $\alpha \in \beta$ ou bien $\alpha = \beta$, soit $\alpha \cap \beta = \beta$, et alors de la même façon on a $\beta \in \alpha$ ou bien $\alpha = \beta$.
(d) Soit A un ensemble non vide d'ordinaux et $\alpha \in A$. L'ensemble $A \cap \alpha$ est soit l'ensemble vide, auquel cas α est le plus petit élément de A, soit un sous ensemble non vide de α et alors possède un plus petit élément β dans l'ordre $\in_\alpha$ qui est le plus petit élément de A dans l'ordre $\prec$. □

Proposition 4.7. *Les nombres naturels sont exactement les nombres ordinaux finis.*

Démonstration. Comme nous savons que tout nombre naturel est un ordinal, et qu'il est bien sur fini, il suffira de prouver que tous les nombre ordinaux qui ne sont pas des nombres naturels sont infinis. Si α est un ordinal et $\alpha \notin \mathbb{N}$, alors comme l'appartenance est asymétrique, nécessairement $\alpha \geq \omega$. Donc $\omega \subseteq \alpha$ comme α est transitif. Donc α est infini. □

Pour les nombres naturels nous avons bien les propriétés vues au chapitre 2, ω étant un ordinal, donc un ensemble strictement bien ordonné. Plus généralement nous avons introduit un ordre qui nous permet de comparer les ordinaux relativement les uns aux autres, mais sans définir une relation d'ordre dans un hypothétique ensemble des nombres ordinaux. La raison est donné par la proposition suivante :

Proposition 4.8. *La collection de tous les ordinaux n'est pas un ensemble.*

Démonstration. Supposons que X soit l'ensemble de tous les ordinaux. On vérifie que $\bigcup X$ est aussi un nombre ordinal : (a) Soit $x \in \bigcup X$, alors $x \in \alpha$ pour un ordinal $\alpha \in X$, donc x est un sous ensemble de α car α est transitif, donc x est un sous ensemble de $\bigcup X$. (b) X est un ensemble (strictement) bien ordonné d'après le point (d) du théorème 4.2. Alors d'après la proposition 4.4 le successeur σ de $\bigcup X$ est aussi un ordinal, et il n'appartient pas à X car sinon $\sigma \subseteq \bigcup X$ et d'après le lemme 4.6 soit $\sigma = \bigcup X$ soit $\sigma \in \bigcup X$ ce qui conduit dans chaque cas à $\sigma \in S(\bigcup X) = \sigma$ et contredit la définition du nombre ordinal σ. Ceci est absurde d'après la définition de X. □

Retournons nous maintenant vers les ensembles bien ordonnés en générals. Nous savons que si deux ordinaux sont distincts, ils ne sont pas isomorphes en tant qu'ensembles bien ordonnés car l'un est un segment initial de l'autre. En fait chaque nombre ordinal caractérise une catégorie de bon ordre et les ordinaux sont donc des représentants des ensembles bien ordonnés. Le grand résultat qui suit précise ce que nous entendons par là, cela sera fondamental pour la suite de notre étude.

Théorème 4.3. *Tout ensemble bien ordonné est isomorphe à un unique nombre ordinal.*

La preuve de ce théorème nécessite pour la première fois l'utilisation de l'axiome de remplacement.

Démonstration. Soit $(O, \prec)$ un ensemble bien ordonné. Soit A l'ensemble de tous les éléments de O pour lesquels $O[a]$ est isomorphe à un nombre ordinal. Cet ordinal est déterminé de façon unique comme deux ordinaux distincts ne peuvent pas être isomorphes (l'un est un segment initial de l'autre) ; on le note alors α_a. Le schéma d'axiome de remplacement prouve que $S = \{\alpha_a | a \in A\}$ est un ensemble. S est un ensemble d'ordinaux donc il est ordonné par $\in$. S est également transitif, car si $\gamma \in \alpha_a \in S$, soit φ l'isomorphisme entre $O[a]$ et α_a et soit $c = \varphi^{-1}(\gamma)$, on a alors $\varphi|_c$ qui est un isomorphisme entre $O[c]$ et γ et donc $\gamma \in S$. Donc S est un nombre ordinal, on pose $S = \alpha$.

Un argument similaire montre que $\forall a \in A$, $b \prec a$ implique $b \in A$: soit φ l'isomorphisme de $O[a]$ et α_a. Alors $\varphi|_{O[b]}$ est un isomorphisme de $O[b]$ et un segment initial I de α_a. Donc il existe $\beta \prec \alpha_a$ tel que $I = \{\gamma \in \alpha_a | \gamma \prec \beta\} = \beta$; *ie*, $\beta = \alpha_b$. Ceci montre que $b \in A$ et $\alpha_b \prec \alpha_a$. On en conclut que soit $A = O$, soit $A = O[c]$ pour un $c \in O$.

On définit maintenant la fonction $f : A \to S = \alpha$ par $f(a) = \alpha_a$. Comme $b \prec a$ implique $\alpha_b \prec \alpha_a$ et d'après la définition de S, il est évident que f est un isomorphisme de $(A, \prec)$ dans α. Si $A = O[c]$, nous devrions avoir $c \in A$, une contradiction. Par conséquent $A = O$ et f est un isomorphisme de $(A, \prec)$ dans α.

□

4.3 Induction et récursion transfinie

Les deux outils fondamentaux que sont le théorème d'induction et de récursion pour les nombres naturels sont également généralisables au cas des nombres ordinaux, c'est ce que nous faisont dans cette section.

Théorème 4.4 (Théorème d'Induction Transfinie)**.** *Soit P une propriété. Si pour tout nombre ordinal α :*

$$P(\beta) \text{ est vrai pour tout } \beta \prec \alpha, \text{ implique } P(\alpha). \tag{4.1}$$

Alors $P(\alpha)$ est vraie pour tout ordinal α.

Démonstration. Supposons que γ ne possède pas la propriété P. Soit alors S l'ensemble de tous les ordinaux $\beta \prec \gamma$ qui n'ont également pas cette propriété. S a un plus petit élément α. Comme chaque $\beta \prec \alpha$ possède la propriété P, alors d'après (4.1) $P(\alpha)$ est vraie ; contradiction. □

Et on peut également en formuler une version plus proche de ce que nous avions pour les nombres naturels.

Théorème 4.5 (Théorème d'Induction Transfinie, seconde version)**.** *Soit P une propriété. Si,*
(1) $P(0)$ est vraie.
(2) $P(\alpha)$ implique $P(\alpha + 1)$ pour tout ordinal α.

(3) Pour tout ordinal limite $\alpha \neq 0$, si $P(\beta)$ est vraie pour tout $\beta \prec \alpha$, alors $P(\alpha)$ est vraie.
Alors $P(\alpha)$ est vraie pour tout ordinal α.

Démonstration. Il suffit de montrer que les hypothèses (1), (2) et (3) impliquent (4.1). Soit alors un ordinal α tel que $P(\beta)$ soit vraie pour tout $\beta \prec \alpha$. Si $\alpha = 0$ alors $P(\alpha)$ est vraie d'après (1). Si α est un successeur, $\alpha = \beta + 1$ pour un $\beta \prec \alpha$; or nous savons que $P(\beta)$ est vraie, donc $P(\alpha)$ est vraie d'après (2). Si $\alpha \neq 0$ est un ordinal limite, nous avons $P(\alpha)$ par (3). □

Nous donnons maintenant le théorème de récursion dans sa version transfinie :

Théorème 4.6 (Théorème de récursion Transfinie)**.** *Soit G une opération. Soit la propriété $P(x, y)$*

$$\begin{cases} x \text{ est un ordinal et } y = t(x) \text{ pour un calcul } t \text{ de longueur } x \text{ basé sur } G, \\ ou \\ x \text{ n'est pas un ordinal et } y = \emptyset. \end{cases}$$

Alors la propriété P définit une nouvelle opération F telle que $F(\alpha) = G(F|_\alpha)$ pour tout ordinal α.

Démonstration. Admis. □

Puis dans sa version paramétrique :

Théorème 4.7 (Théorème de récursion Transfinie, version paramétrique)**.** *Soit G une opération. Soit la propriété $Q(x, y, z)$*

$$\begin{cases} x \text{ est un ordinal et } y = t(x) \text{ pour un calcul } t \text{ de longueur } x \text{ basé sur } G \text{ et } z, \\ ou \\ x \text{ n'est pas un ordinal et } y = \emptyset. \end{cases}$$

Alors la propriété Q définit une nouvelle opération F telle que $F(z, \alpha) = G(z, F_z|_\alpha)$ pour tout ordinal α et pour tout ensemble z.

Démonstration. Admis. □

4.4 Arithmétique des ordinaux

La version paramétrique du théorème de récursion transfinie permet de définir l'addition, la multiplication et l'exponentiation des nombres ordinaux de façon à prolonger directement ce qui a été établit pour les nombres naturels. Nous définirons ces trois opérateurs binaires sans justification particulière de leur existence.

Définition 33 (Addition des nombres ordinaux)**.** *Pour tout ordinal β :*
(1) $\beta + 0 = \beta$.
(2) $\beta + (\alpha + 1) = (\beta + \alpha) + 1, \ \forall \alpha$.
(3) $\beta + \alpha = Sup\{\beta + \gamma | \gamma \prec \alpha\}$ pour tout ordinal limite $\alpha \neq 0$.

On note encore une fois que si on prend $\alpha = 0$, on retrouve avec (2) une équation qui justifie la notation que nous avions adoptée pour le successeur.

L'addition des ordinaux peut différer de celle plus particulière des nombres naturels, le lemme suivant prouve par exemple que l'addition n'est pas toujours commutative :

Lemme 4.9. *Si α est un ordinal limite et si $\beta \prec \alpha$, alors $\beta + \alpha = \alpha$.*

Démonstration. Par définition $\beta + \alpha = Sup\{\beta + \gamma | \gamma \prec \alpha\}$, montrons donc que cet ensemble est égal à α.

Si $\delta \in Sup\{\beta + \gamma | \gamma \prec \alpha\}$, alors $\delta = \beta + \gamma_0$ avec $\gamma_0 \prec \alpha$. Or $\beta \prec \alpha$, donc $\beta + \gamma_0 \in \alpha$ (alpha est limite). Et comme $\delta = \beta + \gamma_0$, $\delta \in \alpha$.

Si $\delta \in \alpha$, on peut comparer δ et β : Soit $\delta \prec \beta$, c'est à dire $\delta \in \beta$ et comme $\beta \in Sup\{\beta + \gamma | \gamma \prec \alpha\}$, alors $\delta \in Sup\{\beta + \gamma | \gamma \prec \alpha\}$. Soit $\delta = \beta$, et alors bien sur $\delta \in Sup\{\beta + \gamma | \gamma \prec \alpha\}$. Soit $\delta \succ \beta$, et alors il existe $\gamma \prec \alpha$ tel que $\delta = \beta + \gamma \in Sup\{\beta + \gamma | \gamma \prec \alpha\}$. □

Ainsi par exemple, $1 + \omega = \omega \neq \omega + 1 = S(\omega)$.

Définition 34 (Multiplication des nombres ordinaux)**.** *Pour tout ordinal β :*
(1) $\beta \times 0 = 0$.
(2) $\beta \times (\alpha + 1) = (\beta \times \alpha) + \beta, \ \forall \alpha$.
(3) $\beta \times \alpha = Sup\{\beta \times \gamma | \gamma \prec \alpha\}$ *pour tout ordinal limite* $\alpha \neq 0$.

Définition 35 (Exponentiation des nombres ordinaux)**.** *Pour tout ordinal β :*
(1) $\beta^0 = 1$.
(2) $\beta^{\alpha+1} = \beta^\alpha \times \beta, \ \forall \alpha$.
(3) $\beta^\alpha = Sup\{\beta^\gamma | \gamma \prec \alpha\}$ *pour tout ordinal limite* $\alpha \neq 0$.

La multiplication et bien sur l'exponentiation ne sont également pas toujours commutative mais on peut vérifier d'autres règles de l'arithmétique des nombres naturels. Nous n'irons pas plus loin dans cette brève introduction.

Il existe une très belle interprétation de cette arithmétique si on considère la façon dont les ordinaux représentent les bons ordres car on peut observer un lien entre les opérations arithmétiques et la façon de construire des ensembles bien ordonnés à partir d'autres.

Chapitre 5

Nombres Cardinaux

Nous sommes parvenus au point clé de ce mémoire. Nous avons maintenant tous les outils nécessaires à la définition des nombres cardinaux pour les ensembles bien ordonnés. Nous avons bien sûr envie plus généralement de définir le nombre cardinal d'un ensemble quelconque, mais la question de savoir si tout ensemble est ordonnable sera abordée dans le prochain et dernier chapitre et est donc laissée de côté ici.

Faisons un petit résumé utile de ce que nous avons appris dans les chapitres précédents. Nous avons vu que dans le cas très particulier des ensembles finis, le cardinal d'un ensemble a été défini conformément à notre intuition à son nombre d'éléments, c'est à dire à l'unique nombre naturel avec lequel il est en bijection. Nous savons également que ce nombre naturel n'est rien d'autre qu'un nombre ordinal fini. De même, on a défini le cardinal des ensembles dénombrables, c'est à dire en bijection avec $\mathbb{N}$, comme l'ensemble $\mathbb{N}$ ordonné par l'appartenance. Et $\mathbb{N} = \omega$ est également un nombre ordinal. Il est donc tout à fait naturel d'étendre ce concept au cas infini et d'utiliser de façon systématique les ordinaux pour définir les cardinaux.

Il existe néanmoins une subtilité. En effet nous avons vu que certains ordinaux étaient équipotents entre eux, par exemple ω est en bijection avec $\omega + 1$, mais aussi avec 2ω, et $\omega^\omega \ldots$ Tous les nombres ordinaux ne définiront donc pas des nombres cardinaux.

5.1 Alephs

Définition 36. *Un nombre ordinal α est dit ordinal initial s'il n'est équipotent à aucun $\beta \prec \alpha$.*

Lemme 5.1. *Deux ordinaux initiaux sont équipotents si et seulement s'ils sont égaux.*

Démonstration. Soit α et β deux ordinaux initiaux. Si ils sont égaux alors évidemment ils sont équipotents. Réciproquement prenons α et β équipotents. Supposons qu'ils ne soient pas égaux. Ils sont comparables d'après le théorème 4.2, par exemple $\beta \prec \alpha$. Or ceci contredit le fait que α soit un ordinal initial comme α et β sont équipotents. □

Théorème 5.1. *Tout ensemble bien ordonnable est équipotent à un unique ordinal initial.*

Démonstration. Soit E un ensemble bien ordonné.
Existence : D'après le théorème 4.3 du chapitre 4, E est isomorphe à un unique nombre ordinal α. Donc E est équipotent à α. Soit α_0 le plus petit ordinal équipotent à α. E équipotent à α_0 par transitivité de la relation d'équipotence. Or α_0 est un ordinal initial car s'il existe $\beta \prec \alpha_0$ équipotent à α_0 alors β est aussi équipotent à α par transitivité, ce qui est impossible comme α_0 est le plus petit ordinal équipotent à α. Unicité : découle du lemme précédent. □

On a maintenant tout en main pour prouver que la famille des ordinaux initiaux est une famille de bons représentants pour définir les nombres cardinaux des ensembles bien ordonnables. C'est ce que nous faisons dans le corollaire qui suit.

Corollaire 5.2. *Les ordinaux initiaux sont des représentants adéquats pour la cardinalité des ensembles bien ordonnables.*

Démonstration. Premièrement, à tout ensemble bien ordonnable on peut associer un unique représentant qui est l'unique ordinal initial auquel il est équipotent d'après le théorème 5.1. Secondement, on doit montrer que si X et Y des ensembles bien ordonnables, X est équipotent à Y si et seulement si X et Y sont équipotent au même ordinal initial. En effet, supposons X et Y équipotents. Alors X équipotent à un ordinal initial α_X et Y équipotent à un ordinal initial α_Y implique α_X équipotent à α_Y et donc $\alpha_X = \alpha_Y$ d'après le lemme 5.1. Et la réciproque est immédiate par transitivité de l'équipotence. □

On peut alors poser la définition suivante pour les nombres cardinaux des ensembles bien ordonnables :

Définition 37 (Nombres Cardinaux)**.** *Si X est un ensemble ordonnable, on appelle nombre cardinal de X et on note $|X|$ l'unique ordinal initial équipotent à X.*

Remarques : Les nombres cardinaux sont donc précisément les ordinaux initiaux. Cette définition est compatible avec ce que nous avions vu précédement concernant les cardinaux des ensembles finis et le cardinal des ensembles dénombrables.

Bien sur une question supplémentaire fait surface : existe-il des ordinaux initiaux plus grand que ω ? En effet, rien ne le garantit pour l'instant, même si nous avons vu, avec par exemple le théorème de Cantor, qu'il existe des ensembles qui ont une cardinalité plus grande que celle de l'ensemble des nombres naturels, peut être que ceux ci ne sont pas bien ordonnables.

Nous allons montrer qu'il existe en fait des ordinaux initiaux arbitrairement grands.

Définition 38. *On définit pour tout ensemble A son nombre de Hartogs, noté $h(A)$, qui est le plus petit ordinal qui n'est équipotent à aucun sous ensemble de A.*

Par définition, $h(A)$ est le plus petit ordinal qui ne s'injecte pas dans A. En particulier, A n'est pas équipotent à $h(A)$ (il est subpotent). Comme on

a vu qu'un nombre ordinal est l'ensemble des nombres ordinaux qui lui sont inférieurs, le nombre de Hartogs d'un ensemble A est encore l'ensemble de tous les ordinaux subpotents à A.

Lemme 5.3. *Pour tout ensemble A, $h(A)$ est un ordinal initial.*

Démonstration. En effet, supposons qu'il existe β équipotent à $h(A)$ tel que $\beta \prec h(A)$, alors β est équipotent à un sous ensemble de A et donc $h(A)$ est équipotent à un sous ensemble de A, ce qui contredit la définition de $h(A)$. □

Lemme 5.4. *Le nombre de Hartogs de A existe pour tout ensemble A.*

Démonstration. Soit un ensemble A quelconque. On définit T l'ensemble des parties de $A \times A$ qui sont des graphes de relations de bon ordre sur un sous-ensemble de A :

$$T = \{R \in P(A \times A) | \exists B \subseteq A, (B, R) \text{ est bien ordonné}\}$$

Soit maintenant la propriété $P(R, \alpha)$ de la relation R est du nombre ordinal α suivante : "$\exists B \subseteq A$, tel que (B, R) soit isomorphe à $(\alpha, \prec)$". D'après le théorème 4.3, il existe pour chacun des ensembles bien ordonnés (B, R) un unique ordinal α tel que $(\alpha, \prec)$ lui soit isomorphe. Donc pour chaque R, il existe un unique α tel que $P(R, \alpha)$ soit vraie. Le schéma d'axiomes de remplacement appliqué à la propriété P justifie ainsi l'existence d'un ensemble H qui contient tous les ordinaux α tel que $P(R, \alpha)$ soit vraie pour un élément R de T.

Montrons que tous les ordinaux équipotents à un sous ensemble de A appartiennent à H. Soit donc α_0 un nombre ordinal équipotent à un sous ensemble B_0 de A. Il suffit de trouver un ordre $R \in T$ tel que $P(R, \alpha_0)$ soit vraie. Si f est une bijection de α_0 dans B_0, l'ordre $R = \{(f(\beta), f(\gamma)) | \beta \prec \gamma \prec \alpha_0\}$ convient.

$h(A)$ est par définition l'ensemble de tous les ordinaux équipotent à un sous ensemble de A. On peut donc écrire :

$$h(A) = \{\alpha \in H | \alpha \text{ est un ordinal équipotent à un sous ensemble de A}\}$$

et l'existence de $h(A)$ est alors justifié par le schéma d'axiome de compréhension. □

On peut ainsi définir par une récursion transfinie une échelle d'ordinaux initiaux, c'est à dire de nombres cardinaux de plus en plus large :

Définition 39.

$$\aleph_0 = \omega;$$

$$\aleph_{\alpha+1} = h(\aleph_\alpha) \textit{ pour tout } \alpha;$$

$$\aleph_\alpha = Sup\,\{\omega_\beta | \beta \prec \alpha\} \textit{ si } \alpha \textit{ et un ordinal limite non nul.}$$

Théorème 5.2.
(a) $\aleph_\alpha$ est un ordinal initial infini pour tout α.
(b) Si ζ est un ordinal initial infini, alors il existe un α tel que $\zeta = \aleph_\alpha$.

Démonstration.
(a) La preuve se fait par induction sur α. Le seul cas non trivial est lorsque α est un ordinal limite. Supposons que $|\aleph_\alpha| = |\gamma|$ pour un $\gamma \prec \aleph_\alpha$. Alors il existe un ordinal $\beta \prec \alpha$ tel que $\gamma \leq \aleph_\beta$ (par définition du Sup). Mais ceci est impossible car cela implique $|\aleph_\alpha| = |\gamma| \leq |\aleph_\beta| \leq |\aleph_\alpha|$.
(b)Premièrement, on peut montrer par induction que $\alpha \leq \aleph_\alpha$ pour tout α. Par conséquent, pour tout ordinal initial infini ζ, il y a un ordinal α tel que $\zeta \prec \aleph_\alpha$ (par exemple le successeur de ζ). Ainsi, il suffit de prouver la proposition suivante : Pour tout ordinal initial infini $\zeta \prec \aleph_\alpha$, il existe un ordinal $\gamma \prec \alpha$ tel que $\zeta = \aleph_\gamma$, ce que l'on fait par induction sur α. La proposition est trivialement vraie pour $\alpha = 0$. Si $\alpha = \beta + 1$, $\zeta \prec \aleph_\alpha = h(\aleph_\beta)$ implique que $|\zeta| \leq |\aleph_\beta|$, donc soit $\zeta = \aleph_\beta$ et nous pouvons poser $\gamma = \beta$, ou bien $\zeta \prec \aleph_\beta$ et l'existence de $\gamma \prec \beta \prec \alpha$ découle de l'hypothèse d'induction. Si α est un ordinal limite, $\zeta \prec \aleph_\alpha = Sup\{\aleph_\beta | \beta \prec \alpha\}$ implique que $\zeta \prec \aleph_\beta$ pour un ordinal $\beta \prec \alpha$. Et l'hypothèse d'induction permet encore d'affirmer l'existence d'un ordinal $\gamma \prec \beta$ tel que $\zeta = \aleph_\gamma$. □

On a ainsi montré que les ordinaux initiaux infinis forment une suite transfinie d'ordinaux initiaux $(\aleph_\alpha)_\alpha$ est un ordinal·

Dans le chapitre 3 nous avions défini une relation d'ordre $\leq$ sur l'ensemble des classes d'équivalences d'ensembles équipotents avant même de définir les nombres cardinaux comme des nombres ordinaux particuliers. Cet ordre est compatible avec l'ordre des nombres ordinaux, c'est à dire que si $|X| = \aleph_\alpha$ et si $|Y| = \aleph_\beta$, alors $|X| \leq |Y|$ si et seulement si $\aleph_\alpha \in \aleph_\beta$.

Finalement tous les ensembles bien ordonnables sont équipotents soit à un entier naturel (ensembles finis), soit à un ordinal initial infini (ensembles infinis), et les nombres cardinaux de tous ces ensembles sont définis comme étant respectivement les nombres naturels et les alephs.

5.2 Arithmétique des cardinaux

On propose ici des définitions à la somme, le produit et l'exponentiation de deux cardinaux, puis nous étudions les propriété de cette arithmétique. Dans toute cette section on considère que κ, μ et ν sont des nombres cardinaux, et X et Y des ensembles disjoints tels que $|X| = \kappa$ et $|Y| = \mu$.

Définition 40. $\kappa + \mu = |X \cup Y|$

Définition 41. $\kappa\mu = |X \times Y|$

Définition 42. $\kappa^\mu = \left|X^Y\right|$

On peut bien sur montrer que ces définitions ne dépendent pas du choix des ensembles X et Y.

Du fait de ces définitions, beaucoup de propriétés arithmétiques des cardinaux découlent soit des propriétés d'union, de produit et de puissance de deux ensembles (par exemple on sait que l'union est associative, donc la loi + est également commutative), soit des propriétés de l'équipotence, (par exemple comme $|X \times Y| = |Y \times X|$, la loi $\times$ est commutative)...

Donnons une liste de ces premières propriétés arithmétiques des cardinaux : Propriétés additives :

(a) Commutativité
(b) Associativité
(c)$\kappa \leq \kappa + \mu$
(d)$\kappa_1 \leq \kappa_2$ et $\mu_1 \leq \mu_2$ implique $\kappa_1 + \mu_1 \leq \kappa_2 + \mu_2$
Propriétés multiplicatives :
(e) Commutativité
(f) Associativité
(g)$\kappa \leq \kappa \times \mu$ si $\mu \succ 0$
(h)$\kappa_1 \leq \kappa_2$ et $\mu_1 \leq \mu_2$ implique $\kappa_1 \times \mu_1 \leq \kappa_2 \times \mu_2$
Propriété de distribution :
(i)$\kappa \times (\mu + \nu) = \kappa \times \mu + \kappa \times \nu$
Propriétés d'exponentiation :
(j)$\kappa \leq \kappa^\mu$ si $\mu \succ 0$
(k)$\mu \leq \kappa^\mu$ si $\kappa \succ 1$
(l)$\kappa_1 \leq \kappa_2$ et $\mu_1 \leq \mu_2$ implique $\kappa_1^{\mu_1} \leq \kappa_2^{\mu_2}$

Pour pousser encore plus loin l'analogie avec l'arithmétique des nombres naturels, remarquons que :
(m)$\kappa + \kappa = 2 \times \kappa$
(n)$\kappa \times \kappa = \kappa^2$

Démonstration de (m).
$2 \times \kappa$ est le cardinal de $\{0,1\} \times X$. Remarquons que $\{0,1\} \times X = (\{0\} \times X) \cup (\{1\} \times X)$, que $|\{0\} \times X| = |\{1\} \times X|$, et que ces deux ensembles sont disjoints. Donc $2 \times \kappa = \kappa + \kappa$.

□

Donnons enfin trois derniers résultats :

Proposition 5.5.
(a)$\kappa^{\mu+\nu} = \kappa^\mu \times \kappa^\nu$
(b)$(\kappa^\mu)^\nu = \kappa^{\mu \times \nu}$
(c)$(\kappa \times \mu)^\nu = \kappa^\nu \times \mu^\nu$

Donnons quelques exemples plus concrets qui mettent en évidence que cette arithmétique diffère totalement de ce que nous avons l'habitude de voir avec les nombres naturels. Les cardinaux finis étant justement exactement les nombres naturels il va falloir regarder avec au moins un nombre cardinal infini, par exemple $\aleph_0$, on a :

$$\aleph_0 + n = \aleph_0$$

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\aleph_0 \times \aleph_0 = \aleph_0$$

Ces résultats sont justifiés par ce qui a été vu dans le chapitre 3 sur les ensembles dénombrables. On pourrait se demander si on peut retrouver des résultas semblables pour d'autres alephs ? La réponse est oui est sera une conséquence du théorème que nous énonçons maintenant.

Théorème 5.3. $\aleph_\alpha \times \aleph_\alpha = \aleph_\alpha$, *pour tout* α.

idée de la démonstration. On prouve par induction transfinie sur l'ordinal α que $\aleph_\alpha \times \aleph_\alpha \leq \aleph_\alpha$. Il faut pour cela construire un bon ordre sur l'ensemble $\aleph_\alpha \times \aleph_\alpha$, et donc vérifier que l'ordre que l'on introduit possède toute les propriétés d'un bon ordre ce qui est assez long... Finalement, comme on a aussi $\aleph_\alpha \times \aleph_\alpha \geq \aleph_\alpha$, on en déduit que $\aleph_\alpha \times \aleph_\alpha = \aleph_\alpha$ □

Corollaire 5.6. *Pour tout α et β tel que $\alpha \leq \beta$, et pour tout nombre naturel non nul n on a :*

$$\aleph_\alpha \times \aleph_\beta = \aleph_\beta$$
$$n \times \aleph_\alpha = \aleph_\alpha$$

Démonstration. Si $\alpha \leq \beta$, alors d'une part nous avons $\aleph_\beta = 1 \times \aleph_\beta \leq \aleph_\alpha \times \aleph_\beta$, et d'autre part le théorème 5.3 nous donne $\aleph_\alpha \times \aleph_\beta \leq \aleph_\beta \times \aleph_\beta = \aleph_\beta$. Donc d'après le théorème de Cantor-Bernstein, $\aleph_\alpha \times \aleph_\beta = \aleph_\beta$.

La seconde égalité est prouvée avec les mêmes arguments. □

Corollaire 5.7. *Pour tout α et β tel que $\alpha \leq \beta$, et pour tout nombre naturel n on a :*

$$\aleph_\alpha + \aleph_\beta = \aleph_\beta$$
$$n + \aleph_\alpha = \aleph_\alpha$$

Démonstration. Si $\alpha \leq \beta$, alors $\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \times \aleph_\beta = \aleph_\beta$. D'où l'égalité. Si n est un nombre naturel, alors $\aleph_\alpha \leq n + \aleph_\alpha \leq \aleph_\alpha + \aleph_\alpha = 2 \times \aleph_\alpha = \aleph_\alpha$. D'où l'égalité. □

Rappelons nous du petit problème des segments posés en introduction du mémoire. Nous savons maintenant qu'un segment quelconque, possède $2^{\aleph_0}$ éléments car est en bijection avec une partie de $\mathbb{R}$. De plus si on juxtapose deux segments, on obtient un segment qui comporte $2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0}$ éléments (car comme $2^{\aleph_0}$ est un cardinal infini, d'après le théorème 5.2 il existe α tel que $2^{\aleph_0} = \aleph_\alpha$, et $\aleph_\alpha + \aleph_\alpha = \aleph_\alpha$ d'après le corollaire 5.7).

Pour conclure... Nous avons dans ce chapitre enfin pu définir les nombres cardinaux d'un à priori très large panel d'ensemble, ceux qui sont bien ordonnables, et introduire une arithmétique efficace. Mais avons nous pour autant répondu à notre problématique ? C'est à dire tous les ensembles sont ils bien ordonnables ? Il existe beaucoup de façon de bien ordonner des ensembles donnés, ce qui nous inciterai à répondre oui à cette question, mais le prouver n'est pas possible avec uniquement les axiomes que nous avons utilisés jusqu'à présent ; cela nécessite l'axiome de choix. Nous avions déjà pu évoquer dans ce mémoire d'autres implications importantes de l'axiome de choix, comme par exemple la concordance entre les notions d'infini et de Dedekind infini, ou autres. On se rend compte ici que cet axiome est la pièce indispensable pour mener à bout à notre édifice : Dans ZFC le travail que nous avons accompli est complétement abouti car la famille des ordinaux limites fournie des représentants des nombres cardinaux de tous les objets de la théorie.

De plus, en ce qui concerne l'arithmétique des nombres cardinaux, nous aimerions bien étendre les opérations à des sommes et produits infinis, mais de telles définitions ne pourraient être justifiées sans l'aide de l'axiome de choix.

Nous sommes belle et bien à la limite de ce qui est constructible dans le cadre de ZF ; là également où s'arrête notre travail.

Bibliographie et remerciements

Comme dit en introduction, à part quelques lectures complémentaires, le seul livre qui m'ait servi de support pédagogique est : "Introduction to Set Theory, Third Edition, Revised and Expanded" de Karel Hrbacek et Thomas Jech ; collection "Pure and applied mathematics, a series of monographs and textbooks" et publié en 1999 par le groupe CRC Press.

Je remercie chaleureusement pour son grand investissement Tuna Altinel, mon enseignant référent, qui a toujours été là pour me guider, du choix du sujet au questions les plus précises, et ceci malgré un semestre boulversé mais très chargé en travail et en événements.

Je remercie également les autres personnes qui ont pu me soutenir et m'encourager dans le choix et la réalisation d'un TIPE. Choix que je ne regrette évidement pas étant donné l'importance des connaissances acquises, et l'ouverture qu'a suscité pour moi ce travail d'introduction à la théorie des ensembles.