

Faculté des sciences

La théorie des topos et les liens avec les ensembles

Liens entre théories, ensembles et catégories.

Auteur·es : Sébastien Mattenet

Promoteur·rices : Tim Van der Linden

Lecteur·rices : Marino Gran, Peter Verdée

Année académique 2019-2020

Master[120] en sciences mathématiques, finalité approfondie

Remerciements

Merci à mon promoteur professeur Tim Van der Linden pour son soutien lors du développement de ce mémoire. Sa disponibilité et ses conseils ont été d'une grande aide dans la réalisation de cet ouvrage.

Merci à M.M. Clementino, professeur de l'Université de Coimbra, pour m'avoir introduit à la théorie des topos.

Merci à Marine et à ma famille pour le soutien et l'aide à l'écriture.

Enfin un tout grand merci à mon entourage et tous ceux qui m'ont aidé et soutenu pendant les 5 années d'études pour aboutir à ce mémoire.

Table des matières

Introduction	1
1 La théorie derrière la théorie des ensembles	2
1.1 Définitions formelles de théorie	2
1.1.1 Le langage propositionnel	2
1.1.2 La logique classique CL, et intuitionniste IL	3
1.2 Langage du premier ordre	3
1.2.1 Exemples	4
1.3 Théorie des types	6
1.3.1 La théorie des types intuitionniste	6
1.3.2 La théorie des types basée sur l'égalité	8
1.3.3 Les τ -théories	9
1.3.4 Remarque	9
1.3.5 τ -théorie vs théorie des types	10
2 Les ensembles et fonctions comme notions de base	11
2.1 Introduction	11
2.2 Retour sur la logique classique	11
2.2.1 Interprétation bivaluée	12
2.3 Algèbre de Boole et de Heyting	13
2.3.1 Exemples	14
2.4 Interprétation dans une algèbre	14
3 Le point de vue catégorique	17
3.1 Les catégories comme ensembles	17
3.2 La catégorie \mathbb{N}	19
3.3 La catégorie <i>Ens</i>	19
3.4 Définition de topos	20
3.4.1 Catégorie cartésienne fermée	21
3.4.2 Classificateur de sous-objet	21
3.5 Exemples	23
4 Les topos comme ensembles	24
4.1 Les morphismes sont des fonctions	24
4.2 Topos et power-objet	25
4.2.3 Remarque sur les sous-objets	28
4.3 Le foncteur \mathcal{P}	33
5 La logique interne	36
5.1 Logique intuitionniste	36
5.2 Logique intuitionniste de premier ordre	38
5.3 Théorie des types	41
5.4 Quelques résultats notables	44

6 Compléter l'équivalence	45
6.1 Équivalence topos-ensemble	45
6.1.1 La théorie des ensembles engendre un topos	45
6.1.2 Un topos engendre une théorie des ensembles	45
6.1.7 Les deux constructions sont inverses	50
6.2 Équivalence topos-logique	51
6.2.1 Une théorie des types engendre un topos	52
6.2.2 Les deux constructions sont inverses	52
Conclusion	56

Introduction

Il est parfois dit que les topos constituent le cadre dans lequel se déroulent les mathématiques, que pour tout sujet mathématique il existe un topos approprié pour traiter le sujet. L'objectif de ce mémoire est de comprendre cette affirmation, en particulier ce que signifie : les topos *sont* un cadre mathématique.

Le sujet étant vaste, il a été restreint et concentré sur le lien entre la théorie des ensembles et les topos. Cela a mené à quatre grands résultats qui seront exposés dans ce mémoire :

- Le topos est une structure d'ensembles ;
- Le topos contient une structure logique ;
- Le topos contient une structure d'ensembles ;
- Le topos est une structure logique.

Les liens entre la théorie des ensembles et la logique sont eux-mêmes plus anciens que la découverte des topos comme base de la mathématique. Il m'a semblé nécessaire de redéfinir et redémontrer certains des liens déjà existants entre les deux.

Dans ce mémoire, j'ai fait le choix de parcourir les pré-requis dans un ordre philosophique, c'est-à-dire dans un premier temps voir les mathématiques d'un point de vue Logiciste et ses différentes formalisations de la théorie des ensembles. Ensuite je parlerai de la vision classique/Bourbakiste, c'est-à-dire voir les outils mathématiques comme étant des ensembles avec des propriétés supplémentaires. Finalement, j'adopterai le point de vue catégorique et j'introduirai les topos en termes de relations internes et externes.

La quantité de matière étant conséquente, de nombreuses preuves ont dû être omises. J'ai fait le choix de garder principalement les preuves d'ordre catégorique, mais de laisser des références précises pour celui qui souhaiterait lire la preuve. Ma contribution se situe principalement dans la compréhension, reformulation et harmonisation des résultats qui se trouvent dans les livres de référence. En particulier chaque auteur a sa conception ontologique des mathématiques, qui se traduit par un cadre métamathématique, et certaines incompatibilités émergent lorsque l'on rassemble les résultats.

1 La théorie derrière la théorie des ensembles

Introduction

Une des manières de voir les mathématiques est comme une partie de la logique : une collection d'axiomes et de règles de déductions logiques. Dans cette perspective, on ne parle pas, par exemple d'un groupe abélien en particulier mais du concept de groupe abélien et on développe la théorie des groupes abéliens. C'est-à-dire qu'on ne manipule pas les éléments d'un groupe particulier (appelé modèle de la théorie) mais directement les axiomes des groupes abéliens et les règles de logique.

Une distinction importante est que les objets en eux-mêmes n'existent pas forcément. Ainsi la théorie des groupes parle de lettres a_i et de relations R qui respectent certaines propriétés. Un groupe est un modèle de la théorie et ses éléments et relations existent et peuvent être manipulés, mais dans la théorie en elle-même, les lettres a_i et R ne sont pas des éléments et ne peuvent pas être manipulés. En particulier, l'ensemble de toutes les phrases démontrables dans une certaine théorie, s'il existe, n'existe que dans une métathéorie des mathématiques, mais pas dans le cadre formaliste.

Nous allons définir le langage propositionnel, la logique classique et intuitionniste, pour ensuite étendre à la logique de premier ordre, donner quelques exemples utiles et enfin parler de la théorie des types intuitionnistes basée sur l'égalité.

1.1 Définitions formelles de théorie

- Un système axiomatique, aussi appelé théorie, est composé de :
- Un alphabet et des règles de construction de phrases ;
 - Une collection de phrases distinguées, appelées axiomes ;
 - Des règles d'inférence qui déterminent comment trouver de nouvelles phrases à partir des autres.

On définit formellement une démonstration comme étant une liste de phrases propositionnelles qui sont soit des axiomes, soit dérivables à partir des phrases précédentes de la liste (via les règles d'inférence). On définit la dernière phrase d'une preuve comme étant un théorème. On dit d'un système qu'il axiomatise tout les théorèmes.

1.1.1 Le langage propositionnel

Soit un langage composé d'une infinité de variables a_i et des lettres $\wedge, \vee, \sim, \supset,), ($.

On peut former des phrases par induction sur les règles suivantes :

- Les variables a_i sont des phrases ;
- Si α est une phrase alors $(\sim \alpha)$ est une phrase ;
- Si α, β sont des phrases alors $(\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \supset \beta)$ sont des phrases.

Les parenthèses seront omises quand la lisibilité ne sera pas remise en question. Parfois elles seront remplacées par des crochets, $[\dots]$, à nouveau dans un souci de lisibilité.

On note Φ_0 l'ensemble des lettres et Φ celui des phrases constructibles avec cette méthode.

En fonction de la formalisation que l'on fait, on aura un groupe distingué de phrases, qui seront les phrases intéressantes de notre théorie. Elles seront appelées tautologies, phrases valides, phrases démontrables, ou encore phrases vraies selon le contexte.

Ces premiers exemples viennent de [2].

1.1.2 La logique classique CL, et intuitionniste IL

Comme premier exemple on a l'axiomatisation de la logique classique. On reprend le langage propositionnel et distingue certains axiomes. Les axiomes sont toutes les phrases de la forme :

1. $\alpha \supset (\alpha \wedge \alpha)$;
2. $(\alpha \wedge \beta) \supset (\beta \wedge \alpha)$;
3. $(\alpha \supset \beta) \supset ((\alpha \wedge \gamma) \supset (\beta \wedge \gamma))$;
4. $((\alpha \supset \beta) \wedge (\beta \supset \gamma)) \supset (\alpha \supset \gamma)$;
5. $\beta \supset (\alpha \supset \beta)$;
6. $(\alpha \wedge (\alpha \supset \beta)) \supset \beta$;
7. $\alpha \supset (\alpha \vee \beta)$;
8. $(\alpha \vee \beta) \supset (\beta \vee \alpha)$;
9. $((\alpha \supset \gamma) \wedge (\beta \supset \gamma)) \supset ((\alpha \vee \beta) \supset \gamma)$;
10. $\sim \alpha \supset (\alpha \supset \beta)$;
11. $((\alpha \supset \beta) \wedge (\alpha \supset \sim \beta)) \supset \sim \alpha$;
12. $\alpha \vee \sim \alpha$.

On indique également une règle d'inférence, qui permet à partir de phrases distinguées (les axiomes dans ce cas-ci) de déduire une nouvelle phrase distinguée :

1. à partir des phrases α et $\alpha \supset \beta$ on peut déduire β

avec α, β des phrases propositionnelles.

On définit également le système axiomatique intuitionniste IL, qui est défini de la même manière mais sans les axiomes générés par le tiers exclu (règle 12). Ce système axiomatise la logique intuitionniste inspirée par Brouwer. Brièvement c'est une théorie ontologique des mathématiques qui pose que les mathématiques sont inventées et non découvertes. En conséquence, le tiers exclu n'a pas de sens car un énoncé mathématique ne devient vrai (ou faux) qu'à partir du moment où il est démontré.

1.2 Langage du premier ordre

La théorie de logique classique ou intuitionniste n'est pas suffisamment puissante pour faire des mathématiques. Il manque notamment le concept de variable et de relation. Nous allons donc créer un modèle plus puissant, appelé un langage élémentaire du premier ordre (1^{er} ordre car \forall est défini seulement sur les éléments et pas sur les relations). Il est possible de définir un modèle général, mais nous nous restreindrons au cas le plus simple, une seule constante et une ou deux relations binaires. Dans un cas général R peut être une relation entre n élément, on appelle cela l'arité de R .

Soit un modèle avec les symboles suivants :

- Une constante c ;
- Des variables v ;
- Des relations R ;
- Le symbole \forall ;
- Le symbole \exists .

La construction de phrases se fait selon les règles suivantes :

- Les formules se construisent de manière identique ;
- Si t, u sont des termes (variable ou constante) et R une relation alors tRu est une formule ;
- Si ϕ est une formule et v une variable alors $(\forall v)\phi$ et $(\exists v)\phi$ sont des formules ;
- Dans le cadre précédent on dit que la variable v n'est pas libre ou occupée. Si une variable apparaît sans être occupée par un quantificateur (\forall, \exists) alors on dit qu'elle est libre. Une formule est bornée quand toutes les variables sont occupées. Si une formule a encore des variables libres, alors on dit que c'est une formule ouverte.

Comme nous avons des variables et des termes distingués, il va être utile de noter le remplacement d'une variable par un terme. Si $\phi(v)$ est une formule ouverte, libre en v , on note $\phi(v/t)$ pour la formule avec t à la place de v . Bien que les termes et les formules sont tous les deux des phrases, il paraît logique de dire d'une formule qu'elle est vraie ou fausse, mais pas pour un terme. Cette disparité sera adressée quand nous allons interpréter les phrases logiques.

Les théories classiques (respectivement intuitionnistes) de premier ordre ont comme axiomes tous les axiomes de la forme admise en logique classique (resp. intuitionniste).

On rajoute en plus comme axiomes toutes les phrases de formes suivantes :

- $\forall v\phi(v) \supset \phi(v/t)$ pour t un terme et $\phi(v)$ libre en v ;
- $\phi(v/t) \supset \exists v\phi(v)$ pour t un terme et $\phi(v)$ libre en v .

On rajoute les règles d'inférences suivantes :

- À partir de $\phi \supset \psi$ on peut déduire $\phi \supset (\forall v)\psi(v)$ si v n'est pas libre dans ϕ ;
- À partir de $\phi \supset \psi$ on peut déduire $(\exists v)\phi(v) \supset \psi$ si v n'est pas libre dans ψ .

Bien souvent, notre modèle va avoir une relation d'égalité distinguée qui respecte les axiomes suivants : pour tout terme t, u et formule $\phi(v)$ libre en v

- tRt ;
- $(tRu) \wedge \phi(v/t) \supset \phi(v/u)$.

Cette relation distinguée sera notée $=$.

Nous laissons en exercice au lecteur le soin de démontrer que ces deux axiomes impliquent les propriétés usuelles de réflexivité, symétrie et transitivité.

1.2.1 Exemples

Nous pouvons formaliser la théorie des ensembles Z_0 et ensuite ZFC , qui servira de cadre pour le reste des mathématiques lors de la conception suivante.

Une théorie des ensembles Z_0 est un modèle avec les relations $=, \in$ qui respectent les axiomes suivant.

Définition 1.2.2. On note $a \equiv b$ pour $(a \supset b) \wedge (b \supset a)$
 $v \subseteq u$ pour $\forall w(w \in v \supset w \in u)$
 $\exists! v \phi(v)$ pour $\exists v[\phi(v) \wedge \forall w(\phi(w) \supset v = w)]$

Soit une théorie Z_0 avec les axiomes suivants :

1. Le symbole $=$ respecte les axiomes d'égalité ;
2. *Extensionnalité* : $(\forall t)(t \in u \equiv t \in v) \supset u = v$;
3. *Ensemble vide* : $(\exists t)(\forall v)(\sim (u \in t))$;
4. *Paire* : $\forall u \forall v \exists t (\forall w (w \in t \equiv w = u \vee w = v))$;
5. *Powerset* : $\forall u \exists t (\forall v (v \in t \equiv v \subseteq u))$;
6. *Union* : $\forall u \exists t (\forall v (v \in t \equiv \exists w (w \in u \wedge v \in w)))$;
7. *Séparation bornée* : $\forall u \exists t (\forall v (v \in t \equiv v \in u \wedge \phi(v)))$ avec ϕ borné.

En fait l'axiome de séparation encode le lien entre une phrase propositionnelle, une fonction et les ensembles. Une phrase logique peut être vue comme une fonction qui prend des valeurs de vérité et renvoie une valeur de vérité. Mais il est également possible de voir cette phrase logique comme étant une fonction caractéristique qui, pour chaque élément d'un ensemble de départ, nous indique s'il fait partie d'un sous-ensemble distingué.

En particulier, l'axiome de séparation nous permet de séparer le sous-ensemble qui a la propriété ϕ .

En combinant l'axiome de séparation avec l'axiome d'extensionnalité, on obtient que le sous-ensemble est unique (car défini en terme de ses éléments).

Cela nous permet d'introduire la notation suivante $\{u : \phi\}$ qui est la collection de tous les ensembles u pour lesquels $\phi(u)$ est vrai ou démontrable.

Il faut faire attention que la notation $\{u : \phi\}$, n'est pas toujours un ensemble qui existe dans la théorie. Par exemple si $\phi = \sim (u = u)$ alors $\{u : \phi\}$ ne sera bien défini que si la théorie admet un ensemble vide. La raison est que même si l'axiome de séparation nous garantit que l'on peut prendre le sous-ensemble de u avec la propriété ϕ , il n'existe pas d'ensemble de tous les ensembles.

On note également (u, v) pour l'ensemble $\{\{u\}, \{u, v\}\}$. L'intuition est qu'on met u en premier et ensuite v , mais le principal est que cette notation nous permet de déduire l'ordre, en particulier on peut déduire la phrase suivante :

$$[(u, v) = (t, w)] \equiv [u = t \wedge v = w]$$

On définit maintenant les notations

- $\{(u, v) : \phi\}$ pour $\{t : \exists u \exists v [t = (u, v) \wedge \phi]\}$;
- \emptyset pour l'ensemble vide ;
- $\mathbf{OP}(u)$ pour $\exists t, \exists v [u = (t, v)]$;
- $\mathbf{Rel}(u)$ pour $\forall v [v \in u \supset \mathbf{OP}(v)]$;
- $\mathbf{Fonct}(u)$ pour $\mathbf{Rel}(u) \wedge \forall v \forall t \forall w [(v, t) \in u \wedge (v, w) \in u \supset t = w]$;
- $\mathbf{Dom}(u)$ pour $\{t : \exists v [(t, v) \in u]\}$;
- $\mathbf{Im}(u)$ pour $\{t : \exists v [(v, t) \in u]\}$;
- $g \circ f$ pour $\{(t, w) : \exists s [(t, s) \in f \wedge (s, w) \in g]\}$.

Ceci permet de définir une fonction par son graphe, c'est-à-dire une fonction est une relation entre deux ensembles A, B qui associe à chaque élément de A un seul de B .

Z_0 est une théorie des ensembles, mais il lui manque certains axiomes pour pouvoir rendre compte de l'usage moderne des mathématiques. ZFC est la théorie munie des axiomes de Z_0 et des axiomes suivants :

- *Infini*, \aleph : $\exists u[0 \in u \wedge \forall v(v \in u \supset v \cup \{v\} \in u)]$;
- *Choix* "si u est un ensemble d'ensembles non vides, alors il existe une fonction de choix" $\forall u \forall v[(\mathbf{Fonct}(u) \wedge \sim (\mathbf{Dom}(u) = \emptyset) \wedge \mathbf{Im}(u) \subseteq v) \supset \exists t(\mathbf{fonct}(t) \wedge \mathbf{Dom}(t) = v \wedge \mathbf{Im}(t) \subseteq \mathbf{Dom}(u) \wedge u \circ t \circ u = u)]$;
- *Régularité* : $\forall u(\sim (u = \emptyset) \supset \exists v(v \in u \wedge v \cap u = \emptyset))$;
- *Remplacement* : "si la phrase $\phi(u, v)$ se comporte comme une fonction alors l'image d'un ensemble est un ensemble"

$$\forall u \forall v \forall w[\phi(u, v) \wedge \phi(u, w) \supset v = w] \supset \forall t \exists s(s = \{v : \exists u(u \in t \wedge \phi(u, v))\}).$$

Le C de *ZFC* fait référence à l'axiome du choix, un peu plus controversé et il est parfois fait mention de *ZF* pour parler du système sans l'axiome du choix.

Il est possible de démontrer que l'axiome du choix implique le tiers exclu et donc cette théorie des ensembles n'est pas intuitionniste. Il existe plusieurs axiomatisations des ensembles qui permettent de rester dans le cadre intuitionniste, comme par exemple *CZF* et *IZF*.

On remarquera également la relation entre une formule ϕ et l'ensemble $\{u : \phi\}$. Ainsi que la relation qui est faite entre les fonctions et les formules, en particulier le remplacement dit que si ϕ se comporte comme une fonction, alors il existe une fonction appropriée. Il a parfois été considéré que la fonction est un outil de base et qu'il est possible de définir les ensembles en termes d'images de fonctions. Cela se fait encore parfois en fondement catégorique.

1.3 Théorie des types

La théorie des types ajoute la notion que les constantes et variables ont certains types qui ne peuvent pas se mélanger. Par exemple, un ensemble, un nombre et une fonction auront des types différents. Dans ce contexte-là, les symboles \forall, \exists devront indiquer sur quels types ils quantifient. Toutes les théories précédentes peuvent se traduire en théorie des types, un type pour les objets et un pour les quantificateurs.

Nous allons maintenant donner la définition d'une famille de théories de deux manières équivalentes. Ces formulations viennent de [6, II.1-2]. Toutes les théories qui ont au moins les axiomes de la théorie des types et les règles de dérivation de la théorie des types seront appelé des théories des types intuitionniste.

1.3.1 La théorie des types intuitionniste

Elle est composée de :

- Une collection de types, y compris un type distingué Ω de vérité et un type 1 ;
- Pour chaque type, des éléments, en particulier une infinité de variables de ce type. On note $x : X$ pour dire que x est de type X ;
- Pour chaque ensemble fini X de variables, une relation binaire d'implication \vdash_X entre des termes des formules de Ω tels que toutes les variables libres sont de type de X . Cela s'interprète comme "dans le contexte X , la formule à gauche implique celle de droite".

On demande en plus les règles suivantes :

- * La classe de types est fermée sous les opérations suivantes :
 - 1 et Ω sont des types ;
 - si X, Y sont des types alors $X \times Y$ est un type et $P(X)$ est un type ;

- On autorise qu'il y ait des types en plus et des identifications entre types. Ainsi, on pourrait demander $\mathcal{P}(1) = \Omega$, $(A \times B) \times C = A \times (B \times C)$ ou $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$.
- * Les éléments sont générés à partir des règles suivantes :
 - Il existe une infinité de variables x_1^A, x_2^A, \dots de type A ;
 - $\blacksquare : 1$;
 - si $a : A, b : B$ alors $(a, b) : A \times B$;
 - si $a : A, \theta : \mathcal{P}(A)$ alors $(a \in \theta)$ est de type Ω ;
 - si $\phi(x) : \Omega$ qui peut éventuellement avoir une variable libre $x : A$, alors $\{x : A \mid \phi(x)\}$ est un terme de type $\mathcal{P}(A)$ ou x n'est plus libre;
 - $\top : \Omega$ et $\perp : \Omega$;
 - si $p, q : \Omega$ alors $p \vee q, p \wedge q, p \supset q$ sont de type Ω ;
 - si $\phi(x) : \Omega$ alors $\forall_{x \in A} \phi(x)$ et $\exists_{x \in A} \phi(x)$ sont des termes de Ω et x n'est plus libre.

On définit comme raccourci de notation :

- Les mêmes notation que 1.2.2;
- $\neg \alpha$ pour $\alpha \supset \perp$;
- $a = a'$ pour $\forall_{u : \mathcal{P}(A)} [a \in u \equiv a' \in u]$;
- $\vdash_X \alpha$ pour $\top \vdash_X \alpha$;
- \vdash pour \vdash_\emptyset .

[6] crédite Leibniz pour la définition d'égalité.

On donne maintenant les règles de construction de phrases.

* Règles structurelles :

- $\alpha \vdash_X \alpha$;
- $\alpha \vdash_X \beta, \beta \vdash_X \gamma$ implique $\alpha \vdash_X \gamma$;
- $\alpha \vdash_X \beta$ implique $\alpha \vdash_{X \cup \{y\}} \beta$;
- $\phi(y) \vdash_{X \cup \{y\}} \psi(y)$ implique $\phi(b) \vdash_X \psi(b)$ si y est une variable de type B et b un terme de type B . On demande cependant que B soit non vide et qu'aucune variable libre de B ne soit utilisée par ϕ ou ψ .

* Règles logiques :

- $\alpha \vdash_X \top$;
- $\perp \vdash_X \alpha$;
- $\gamma \vdash_X \alpha \wedge \beta$ si et seulement si $\gamma \vdash_X \alpha$ et $\gamma \vdash_X \beta$;
- $\gamma \vee \alpha \vdash_X \beta$ si et seulement si $\gamma \vdash_X \beta$ et $\alpha \vdash_X \beta$;
- $\gamma \vdash_X \alpha \supset \beta$ si et seulement si $\gamma \wedge \alpha \vdash_X \beta$;
- $\alpha \vdash_X \forall_{y : Y} \phi(y)$ ssi $\alpha \vdash_{X \cup \{y\}} \phi(y)$;
- $\exists_{y : Y} \phi(y) \vdash_X \alpha$ ssi $\phi(y) \vdash_{X \cup \{y\}} \alpha$.

* Règles supplémentaires :

- Compréhension :
 - $\vdash_X \forall_{x : A} [x \in \{x' : A \mid \phi(x')\} \equiv \phi(x)]$;
- Extensionnalité :
 - $\vdash \forall_{u : \mathcal{P}A} \forall_{v : \mathcal{P}A} [\forall_{x : A} (x \in u \equiv x \in v) \supset u = v]$;
 - $\vdash \forall_{s : \Omega} \forall_{t : \Omega} [(s \equiv t) \supset s = t]$;
- Produit :
 - $\vdash \forall_{z : 1} z = \blacksquare$;
 - $\vdash \forall_{z : A \times B} \exists_{x : A} \exists_{y : B} z = (x, y)$;
 - $\vdash \forall_{x : A} \forall_{x' : A} \forall_{y : B} \forall_{y' : B} [(x, y) = (x', y') \supset (x = x' \wedge y = y')]$.

On peut également rajouter un type distingué \mathbb{N} des nombres naturels, qui satisfait les axiomes suivants :

- $0 : \mathbb{N}$;
- $x : \mathbb{N}$ implique $Sx : \mathbb{N}$;
- Axiomes de Peano :
- $\vdash \forall_{x:\mathbb{N}}(Sx = 0 \supset \perp)$;
- $\vdash \forall_{x:\mathbb{N}}\forall_{y:\mathbb{N}}(Sx = Sy \supset x = y)$;
- $\vdash \forall_{u:\mathcal{P}\mathbb{N}}[(0 \in u \wedge \forall_{x:\mathbb{N}}(x \in u \supset Sx \in u)) \supset \forall_{y:\mathbb{N}}y \in u]$.

De plus cette théorie intuitionniste peut être rendue classique en rajoutant l'axiome $\forall_{t:\Omega}(t \vee \neg t)$ ou bien $\forall_{t:\Omega}(\neg\neg t \supset t)$. Ces deux axiomes sont équivalent en ce sens qu'avoir l'un des deux implique l'autre.

Il est en réalité possible de réduire cette théorie, en définissant les termes \perp, \wedge, \exists en terme de \forall, \vee, \supset . Dans ce cas tous les axiomes contenant ces termes deviennent des théorèmes démontrables dans la théorie. On procède comme suit :

- \perp est défini par $\forall_{t:\Omega}t$;
- $\alpha \vee \beta$ par $\forall_{t:\Omega}([\alpha \supset t] \wedge [\beta \supset t]) \supset t$;
- $\exists_{x:A}\phi(x)$ par $\forall_{t:\Omega}(\forall_{x:A}[\phi(x) \supset t] \supset t)$.

Il est même possible d'aller plus loin et de définir tous les termes logiques en fonction de l'égalité et l'inclusion.

1.3.2 La théorie des types basée sur l'égalité

La construction est fort similaire, on mentionne uniquement les règles qui changent. Toutes les règles avec les symboles $\wedge, \vee, \supset, \exists, \forall$ sont enlevées et on rajoute à la place :

- si $a : A$ et $a' : A$ alors $a = a'$ est un terme de Ω .

Le symbole \vdash_X quant à lui n'est plus vu comme une relation binaire, mais comme une relation entre un ensemble Γ de formules (appelés hypothèses) et une formule (thèse). On écrit donc $\Gamma \vdash_X \alpha$ pour dire que α est induit par $\{\phi_1, \dots, \phi_n\}$. On suppose que toutes les variables libres de Γ sont des éléments de X . Par souci de lisibilité on notera parfois $\phi_1, \dots, \phi_n \vdash_X \alpha$.

Si $n = 0$, c'est-à-dire $\Gamma = \emptyset$ alors on note $\vdash_X \alpha$. De même, si $X = \emptyset$ on notera \vdash .

Les axiomes à rajouter sont :

- * Règles structurelles :
 - $\Gamma \vdash_X \alpha$ et $\Gamma \cup \{\alpha\} \vdash_X \beta$ implique $\Gamma \vdash_X \beta$;
 - $\Gamma \vdash_X \alpha$ implique $\Gamma \cup \{\beta\} \vdash_X \alpha$;
- * Règles d'égalité :
 - $\vdash_X a = a$;
 - $a = b$ implique $\phi(a) \vdash_X \phi(b)$ en supposant que a et b peuvent être substitués à x dans $\phi(x)$;
 - $\Gamma, \alpha \vdash_X \beta, \Gamma, \beta \vdash_X \alpha$ implique $\Gamma \vdash_X \alpha = \beta$;
- * Autres règles :
 - $(a, b) = (c, d) \vdash_X a = c$;
 - $(a, b) = (c, d) \vdash_X b = d$;
 - $\vdash_X (x \in \{x' : A \mid \phi(x')\}) = \phi(x)$ avec x un élément de X et de type A ;
 - $\vdash_z z = \blacksquare$ si $z : 1$;
 - $\Gamma \vdash_{X \cup \{x\}} \phi(x) = x \in \theta$ implique $\Gamma \vdash_X \{x : A \mid \phi(x)\} = \theta$;
 - $\Gamma, z = (x, y) \vdash_{X \cup \{x, y, z\}} \phi(z)$ implique $\Gamma \vdash_{X \cup \{z\}} \phi(z)$.

On définit les expressions $\top, \wedge, \supset, \forall$ comme suit

- \top est le terme $\blacksquare = \blacksquare$;
- $\alpha \wedge \beta$ est l'abréviation de $(\alpha, \beta) = (\top, \top)$;
- $\alpha \supset \beta$ remplace $\alpha \wedge \beta = \beta$;
- $\forall_{x:A} \phi(x)$ est défini par $\{x : A \mid \phi(x)\} = \{x : A \mid \top\}$.

En remplaçant $\Gamma = \{\alpha, \beta, \dots\}$ par $\alpha \wedge \beta \wedge \dots$, on trouve que les deux définitions sont équivalentes. Les détails sont dans [6, II.2.2-4].

Il est remarquable qu'à partir d'une théorie avec la notion d'égalité et d'appartenance, on puisse déduire tous les axiomes logiques. Cela laisse penser que la théorie des ensembles contient tous les outils pour former la logique à partir des intersections et unions et à l'inverse, que les connecteurs logiques sont suffisants pour définir les opérations d'ensembles. Ce parallélisme trouve sa place dans les topos qui pourront être interprétés comme une théorie logique ou comme une catégorie des ensembles généralisée.

On appelle une théorie des types, toute théorie qui a les axiomes et règles de dérivations précédents. On appelle la théorie des types, la théorie minimale, c'est-à-dire celle qui a uniquement les axiomes requis pour être une théorie des types.

1.3.3 Les τ -théories

Cette famille de théories des types de [5] est fort semblable à la précédente, mais avec un peu plus de redondance.

Une τ -théorie a des types générés par les produits et power-types. À nouveau, 1 et Ω sont des types de base. Elle admet les symboles $\wedge, \vee, \supset, \neg, \in_A, =_A$, avec les mêmes règles que les deux théories précédentes.

Un contexte est une liste $\vec{x} = x_1, \dots, x_n$ de variables distinctes. Le cas $n = 0$ est autorisé et dans ce cas $\vec{x} = \emptyset$. Si y est une variable qui n'est pas dans \vec{x} alors \vec{x}, y est le contexte auquel on a rajouté y à la fin de la liste. On écrit $\vec{x}.t$ (resp. $\vec{x}.\phi$) pour le terme t (formule ϕ) dans le contexte \vec{x} . On considère uniquement des contextes acceptables, c'est-à-dire où toutes les variables libres de t (de ϕ) sont incluses dans le contexte \vec{x} . Dans ce cas, on peut interpréter $\alpha \vdash_{\vec{x}} \beta$ comme "dans le contexte \vec{x} , α implique β ".

Si $t : A \times B$ alors il existe une fonction $\text{fst}(t) : A$ et $\text{sec}(t) : B$, ce qui revient en pratique à demander que les termes de $A \times B$ soient de la forme $t = (x : A, y : B)$, de manière similaire avec la théorie précédente.

Les règles de power-types sont changées par les suivantes :

- Extensionnalité : $\top \vdash_w (w = \{x : A \mid x \in_A w\})$ pour $w : \mathcal{P}(A)$;
- Collection : $(z \in \{y : A \mid \phi\}) \vdash_{\vec{x}, z} \phi(z/y)$ et son inverse, avec ϕ qui a toutes ses variables libres dans \vec{x}, y .

On définit la théorie comme étant l'ensemble des séquents de la forme $\alpha \vdash_{\vec{x}} \beta$ qui sont dérivables dans la théorie.

1.3.4 Remarque

Remarquons que il est équivalent de demander un séquent $\alpha \vdash_{\vec{x}} \beta$ et la phrase $\vdash \forall_{\vec{x}}(\alpha \supset \beta)$. Ici $\forall_{\vec{x}}$ est la concaténation de $\forall_{y:ix_i}$ pour toutes les variables du contexte \vec{x} . On dira que la phrase ϕ est dérivable dans τ pour dire que le séquent $\vdash \phi$ est dérivable.

Avec cette équivalence, on remarque que les règles logiques correspondent aux axiomes de la logique intuitionniste de premier ordre, que les règles struc-

turelles sont les règles de dérivation et les autres règles sont des axiomes de théories des ensembles.

1.3.5 τ -théorie vs théorie des types

Johnstone affirme dans [5, D4.1] que son approche (τ -théories) est équivalente à celle de Lambek et Scott (théorie des types intuitionniste) et les deux auteurs arrivent à une équivalence de catégories avec les topos, mais il y a des différences que je ne suis pas parvenu à réconcilier. En premier lieu Johnstone demande que les types soient librement générés à partir d'un ensemble donné, ce qui exclut les identifications entre types possibles dans la théorie de Lambek.

Ensuite Johnstone garde la différence \in_A , avec en théorie un symbole pour chaque type. Toutefois comme ce symbole ne peut être utilisé qu'avec un seul type qui le précède, il n'y a pas d'ambiguïté à retirer l'indice A .

Une autre différence est l'utilisation de termes en contexte. De plus Johnstone demande que le compte des variables libres soit fait dans la théorie en elle-même avec une fonction de variable libre FV , tandis que ce compte se fait de manière externe à la théorie par Lambek.

Enfin Johnstone demande l'existence externe d'éléments a, b tel que $t = (a, b)$ tandis que Lambek demande la version interne $\forall_{t:A \times B} \exists_{a:A} \exists_{b:B} (a, b) = t$. En pratique cela a peu d'importance car 5.4 montre que dans un topos l'existence interne implique l'existence externe dans un topos.

Mentionnons finalement que ces théories sont introduites dans un cadre Logicien, c'est-à-dire que les types ne sont pas des objets qui existent, on demande seulement s'ils existent, quelles propriétés seraient démontrables. Osius prend ce point de vue dans [10], mais Lambek et Scott, et Johnstone sont dans un autre cadre métathéorique et considèrent que les types et les phrases sont des objets qui existent et peuvent être manipulés.

2 Les ensembles et fonctions comme notions de base

2.1 Introduction

Dans la conception courante des mathématiques, on ne s'intéresse pas à la théorie pure, mais plutôt aux ensembles qui vérifient les axiomes. On appelle un ensemble et relations qui satisfont les axiomes d'une certaine théorie, un modèle de cette théorie. Par exemple, un ensemble et une opération qui satisfont les axiomes de groupe sera un modèle de la théorie des groupes, ou encore un groupe. La conception Bourbakiste considère les outils mathématiques comme rien de plus qu'un ensemble d'éléments muni de structures supplémentaires. Dans ce cadre, la théorie des ensembles est considérée comme donnée et le reste se construit dessus. Notre métathéorie est la théorie des ensembles (et des mathématiques) dans laquelle on évolue pour construire le reste. Sans précisions, la métathéorie est ZFC.

Dans ce cadre, tous les ensembles de la métathéorie existent et peuvent être manipulés. En particulier une théorie logique est confondue avec le modèle de sa représentation, c'est-à-dire que l'on considère que les lettres a_i et les relations R existent et respectent les axiomes de la théorie.

La notion d'ensemble comme fondation des mathématiques, bien que dominante aujourd'hui n'est pas garantie. On pourrait argumenter que la notion de fonction est tout aussi basique et dans la pratique les deux ne se dissocient pas tellement. NBG a ainsi oscillé entre une axiomatisation d'ensembles et une axiomatisation en terme de fonctions [3].

2.2 Retour sur la logique classique

Pour cet exemple, nous allons combiner l'approche logique, l'approche en termes d'ensembles et en termes de fonctions pour illustrer les différents points de vue sur les mêmes objets mathématiques. Cette approche nous vient directement de [2, Ch6.2-4].

Reprenons les phrases propositionnelles, définies en 1.1. Supposons que les variables a_i aient une certaine valeur de vérité (que l'on considérera juste vrai ou faux pour commencer). On veut maintenant interpréter ces phrases. L'idée est d'associer à une variable a_i une valeur de vérité comme par exemple vrai ou faux, et ensuite étendre cette valeur de vérité à d'autres phrases par les relations suivantes :

- $\alpha \vee \beta$ est vrai si α ou β sont vrais ;
- $\alpha \wedge \beta$ est vrai si α et β sont vrais ;
- $\sim \alpha$ est vrai si α est faux ;
- $\alpha \supset \beta$ est vrai si " α implique β ".

On peut associer à chaque connecteur logique une table de vérité. On désigne par 1 (resp. 0) le fait qu'une proposition soit vraie (resp. fausse).

Le connecteur \sim est défini par la table suivante

α	$\sim \alpha$
1	0
0	1

On obtient donc une fonction $\neg : \{0, 1\} \rightarrow \{0, 1\}$.
 Comme cette fonction a valeur dans $\{0, 1\}$ on peut la voir comme une fonction caractéristique d'un sous-ensemble (en l'occurrence $\{0\}$).
 Un raisonnement similaire est fait pour les autres connecteurs logiques

α	β	$\alpha \vee \beta$
1	1	1
1	0	1
0	1	1
0	0	0

En notant $2 = \{0, 1\}$, ce connecteur définit (ou est défini par) une fonction $\cup : 2 \times 2 \rightarrow 2$ et (de manière équivalente) un sous-ensemble $\{(1, 1), (1, 0), (0, 1)\}$

α	β	$\alpha \wedge \beta$
1	1	1
1	0	0
0	1	0
0	0	0

Pareil pour $\cap : 2 \times 2 \rightarrow 2$ et le sous-ensemble $\{(1, 1)\}$.

α	β	$\alpha \supset \beta$
1	1	1
1	0	0
0	1	1
0	0	1

Enfin, on a $\Rightarrow : 2 \times 2 \rightarrow 2$ et le sous-ensemble $\{(1, 1), (0, 1), (0, 0)\}$.

Remarque

Concernant l'implication, ce que signifie précisément " a implique b " n'est pas toujours clair dans le langage familier et les logiciens ont plusieurs définitions. La table de vérité ici provient de l'argument que nous souhaitons éviter de déduire quelque chose de faux à partir de prémisses vraies. Cependant le sous-ensemble désigné peut également être retrouvé à partir de $\lesseqgtr = \{(a, b) \mid a \leq b\}$, ce qui suggère la définition suivante : $\alpha \supset \beta$ si β est au moins aussi vrai que α . Ce sera notre intuition pour \supset dans la suite.

2.2.1 Interprétation bivaluée

Nous pouvons maintenant écrire formellement une interprétation de notre langage propositionnel.

Une interprétation est une fonction $V : \Phi_0 \rightarrow \{0, 1\} \simeq \{Vrai, Faux\}$ étendu à Φ par les règles suivantes :

- $V(\sim \alpha) = \neg V(\alpha)$;
- $V(\alpha \vee \beta) = V(\alpha) \cup V(\beta)$;
- $V(\alpha \wedge \beta) = V(\alpha) \cap V(\beta)$;
- $V(\alpha \supset \beta) = V(\alpha) \Rightarrow V(\beta)$.

Les ensembles Φ_0 et Φ sont ceux définis en 1.1.1.

Il y a un ensemble de phrases propositionnelles qui se distingue par la propriété d'être vrai pour toutes les interprétations. On appelle ces phrases des tautologies. Il est possible de démontrer que ce sont exactement les phrases démontrables dans le système de logique classique CL. La démonstration se fait en démontrant que les axiomes de bases sont des tautologies et ensuite que l'ensemble des tautologies est fermé par les règles de dérivations.

En prenant la convention qu'un énoncé est vrai s'il n'a aucun contre-exemple, alors on peut voir les tautologies comme des phrases caractérisées par la propriété d'être toujours vraies. On peut également voir les phrases valides comme l'image inverse du maximum par la fonction évaluation, c'est-à-dire que l'évaluation est la fonction qui caractérise la notion de vérité. Dans ce contexte, la fonction d'évaluation est une fonction qui indique à quel point un énoncé est vrai, et les tautologies sont les phrases les plus vraies possible, les phrases qui ne peuvent pas être fausses.

2.3 Algèbre de Boole et de Heyting

Les algèbres de Boole et de Heyting sont reliées à la logique classique et intuitionniste respectivement. Leur définitions et les preuves suivantes proviennent de [2].

Soit P un ensemble partiellement ordonné (P, \leq) . On définit les propriétés suivantes :

- P est **borné** : il y a un élément maximum 1 et un élément minimum 0 ;
- P est un **treillis** : toute paire d'éléments de P admet une borne supérieure $x \cup y$ et une borne inférieure $x \cap y$. Ces bornes sont définies comme étant le maximum des minorants, et le minimum des majorants pour l'ordre donné ;
- P est un **treillis distributif** : pour tout triplet, on a les égalités suivantes :
 1. $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$;
 2. $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$;
- P a des **compléments** : pour tout $x \in P$ le complément est l'unique y tel que :
 1. $x \cap y = 0$;
 2. $x \cup y = 1$;
- P a des **pseudo-compléments** : pour tout $x \in P$ le pseudo-complément est l'unique y tel que $\forall a \in P, a \leq y \Leftrightarrow x \cap a = 0$;
- P a des **pseudo-compléments relatifs** : pour tout $x \in P$ le pseudo-complément relatif à z est l'unique y tel que $\forall a \in P, a \leq y \Leftrightarrow x \cap a \leq z$.

Il est possible de démontrer que tout complément est un pseudo-complément, mais l'inverse n'est pas vrai en général.

Une algèbre de Boole (resp. de Heyting) est un treillis, borné, distributif, complémenté (resp. relativement pseudo-complémenté).

Dans une algèbre Booleene, on note $\neg x$ pour le complément de x et on définit $x \Rightarrow z = \neg x \sqcup z$.

Dans une algèbre de Heyting, on note $x \Rightarrow z$ pour le pseudo-complément de x relativement à z et on note $\neg x$ comme étant le pseudo-complément de x , c'est-à-dire $x \Rightarrow 0$.

Il est à noter qu'une algèbre de Boole est un cas particulier d'algèbre de Heyting. De plus, la condition $a \Rightarrow b = \neg a \cup b$ est nécessaire et suffisante pour qu'une algèbre de Heyting soit une algèbre de Boole. Dans ce cas, les définitions de \neg, \Rightarrow en tant qu'algèbre de Boole ou de Heyting coïncident.

2.3.1 Exemples

Un exemple d'algèbre de Boole est celle induite par les sous-ensembles d'un ensemble A .

Soit A un ensemble, $\mathcal{P}(A)$ muni de la structure d'inclusion est une algèbre de Boole.

- Le maximum et le minimum sont $1 = A$ et $0 = \emptyset$ respectivement ;
- Les bornes supérieures et inférieures correspondent respectivement à $S \cup T$ et $S \cap T$ pour $S, T \subseteq A$;
- Les égalités sont respectées $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$;
- Le complément correspond au complément usuel $\neg S = S' = A \setminus S$.

En particulier si $A = \{1\}$ on a $\mathcal{P}(A) = \{\emptyset, \{1\}\} = \Omega$. Le maximum est $1 = \{1\}$, le minimum est $0 = \emptyset$, la relation d'ordre est $0 \leq 1$, c'est-à-dire $\emptyset \subseteq \{1\}$ et les opérateurs $\wedge, \vee, \neg, \Rightarrow$, correspondent au opérateurs $\wedge, \vee, \sim, \supset$ définis en 2.2.

Pour un exemple d'algèbre de Heyting, on va s'intéresser aux ouverts d'un espace topologique.

Soit A un espace topologique, $\mathcal{O}(A)$ muni de la structure d'inclusion est une algèbre de Heyting.

- Le maximum et le minimum sont $1 = A$ et $0 = \emptyset$ respectivement ;
- Les bornes supérieures et inférieures correspondent respectivement à $S \cup T$ et $S \cap T$ pour $S, T \in \mathcal{O}(A)$;
- Les égalités sont respectées $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$;
- Le pseudo-complément relatif est $S \Rightarrow T = A \setminus (\overline{S \setminus T})$;
- Le pseudo-complément correspond au complément de la fermeture de l'élément, c'est-à-dire au plus grand ouvert qui ne contient pas l'élément. La différence avec l'exemple précédent se fait sur le bord de S qui n'est pas inclus dans le pseudo-complément $\neg S = A \setminus \overline{S}$.

Il est important de remarquer que dans ces deux cas, l'ensemble $A \cap B$ est le plus grand ensemble qui contient tout les éléments qui sont dans A et dans B , cet ensemble est donc la manifestation de la phrase "être dans A et B ". Il en est de même pour $A \cup B$ et " être dans A ou B ", pour $\neg A$ et "ne pas être dans A " et pour $A \Rightarrow B$ et " être dans B au moins autant que dans A ".

Ceci motive donc à interpréter ces connecteurs comme étant des connecteurs propositionnels et interpréter des phrases propositionnelles dans une algèbre.

2.4 Interprétation dans une algèbre

Soit P une algèbre de Boole ou de Heyting.

Une interprétation dans P est une fonction $V : \Phi_0 \rightarrow P$ étendu à Φ par les règles suivantes :

- $V(\sim \alpha) = \neg V(\alpha)$;
- $V(\alpha \vee \beta) = V(\alpha) \cup V(\beta)$;
- $V(\alpha \wedge \beta) = V(\alpha) \cap V(\beta)$;
- $V(\alpha \supset \beta) = V(\alpha) \Rightarrow V(\beta)$.

Une phrase est dite valide dans P si toutes ses interprétation dans P donnent le maximum (c'est-à-dire 1).

Il est possible de montrer qu'avec cette représentation, les algèbres de Boole caractérisent les phrases de logique classique, en ce sens qu'une phrase démontrable de CL est valide dans toute algèbre de Boole et, inversement, qu'une phrase valide dans toute algèbre de Boole est une tautologie de CL.

Démontrer que toutes les tautologies de CL sont valides dans une algèbre de Boole se fait par construction. On démontre que les axiomes de CL sont valides, et que la règle de dérivation préserve la validité.

Exemple 2.4.1. Le Modus Ponens préserve la validité dans les algèbre de Heyting.

Soit \mathcal{O} une algèbre de Heyting et soit $V : \Phi \rightarrow \mathcal{O}$ une interprétation qui rend $\alpha, \alpha \supset \beta$ valide. Comme α est valide dans \mathcal{O} on sait $V(\alpha) = 1$. De même, $V(\alpha \supset \beta) = 1$

$$\begin{aligned} 1 &= V(\alpha \supset \beta) \\ &= V(\alpha) \Rightarrow V(\beta) \\ &= 1 \Rightarrow V(\beta) \end{aligned}$$

Cela signifie que 1 est le pseudo-complément de 1 relativement a $V(\beta)$. C'est-à-dire que pour tout $x \in \mathcal{O}$, on a $x \leq 1$ ssi $1 \sqcap x \leq V(\beta)$. Comme 1 est le maximum, la condition $x \leq 1$ est toujours vraie et $1 \sqcap x = x$.

On peut réécrire $x \leq V(\beta), \forall x \in \mathcal{O}$, c'est-à-dire que $V(\beta)$ est le maximum, donc β est une phrase valide.

Il est généralement plus compliqué de démontrer l'autre sens, qu'une phrase vraie dans toutes les algèbres de Boole est forcément démontrable à partir des axiomes.

Théorème 2.4.2. *Il existe une algèbre de Boole qui caractérise exactement les phrases démontrables de CL.*

Démonstration. L'idée est de munir l'ensemble Φ de tous les énoncés possibles d'un ordre, qui sera donné par les implications logiques.

Soit \sim_c la relation d'équivalence sur Φ donnée par $\alpha \sim_c \beta$ si les phrases $\alpha \supset \beta$ et $\beta \supset \alpha$ sont des théorèmes de la logique classique. Cette définition est équivalente à demander $\alpha \sim_c \beta$ ssi $\alpha \equiv \beta$ est un théorème de la logique classique.

Cette relation d'équivalence est bien définie :

- Réflexive $\alpha \supset \alpha$ par axiomes de CL ;
- Symétrique par définition ;
- Transitive : si $\alpha \sim_c \beta, \beta \sim_c \gamma$, on a comme tautologie de CL $\alpha \supset \beta, \beta \supset \gamma$.

Par l'axiome 4, on en déduit que $\alpha \supset \gamma$. L'autre implication se fait exactement de la même manière, on en conclut que $\alpha \sim_c \gamma$.

On est maintenant en mesure de munir l'ensemble $B = \frac{\Phi}{\sim_c}$ d'une relation d'ordre en posant $[\alpha] \leq [\beta]$ si $\alpha \supset \beta$ est une tautologie de CL. Cette relation est bien définie, car si on a une démonstration de $\alpha \sim_c \alpha', \beta \sim_c \beta', \alpha \supset \beta$, alors on peut démontrer $\alpha' \supset \beta'$ en combinant les trois démonstrations.

B muni de cette relation d'ordre est une algèbre de Boole, dans laquelle on peut vérifier que :

- $[\alpha] \sqcap [\beta] = [\alpha \wedge \beta]$;
- $[\alpha] \sqcup [\beta] = [\alpha \vee \beta]$;
- $\neg[\alpha] = [\sim \alpha]$;
- $[\alpha] = 1$ si et seulement si α est une tautologie de la logique classique.

Ceci rend la fonction d'évaluation considérablement plus simple, car on a $V(\alpha) = [\alpha]$. On en conclut que α est valide dans B si et seulement si α est une tautologie de CL. \square

L'algèbre ainsi obtenue s'appelle **l'algèbre de Lindenbaum**. En changeant \sim_c par \sim_i , l'équivalence des phrases démontrablement équivalentes sous la logique intuitionniste, le résultat est une algèbre de Heyting qui caractérise les phrases démontrables de IL.

Il est important de noter que cette preuve utilise une conception ensembliste de la théorie logique. C'est-à-dire qu'on confond la théorie logique (qui n'a pas de nécessité ontologique d'exister) avec sa représentation canonique dans ZFC (qui est réelle en un certain sens). Ainsi la logique dit "si on a des variables et des connecteurs, voici ce qu'il se passerait", tandis que la conception classique dit, "voici l'ensemble de variables et les connecteurs". En particulier Brouwer serait contre l'existence même de l'ensemble des phrases démontrables.

3 Le point de vue catégorique

Introduction

La théorie des catégories, développée par Saunders MacLane étend ce que les Bourbakistes ont tenté de faire, c'est-à-dire une étude des structures mathématiques, indépendamment des objets sous-jacents. Il est possible de considérer les catégories comme la notion de base des mathématiques et redéfinir les ensembles, algèbres de Heyting, théories logiques et autres outils mathématiques uniquement en termes catégoriques.

Ce mémoire a essayé d'utiliser le cadre adapté à chaque outil plutôt qu'un grand cadre unifiant.

3.1 Les catégories comme ensembles

On définit une catégorie \mathbb{C} comme étant la donnée d'un ensemble d'**objets** et d'un ensemble de **morphismes** (aussi appelés **fonctions** ou **flèches**) entre deux objets, qui satisfont les propriétés de composition suivantes :

- Pour tout morphisme $f : A \rightarrow B$ et $g : B \rightarrow C$ il existe un morphisme de composition $g \circ f = A \rightarrow C$;
- Pour tout objet $A, B, C, D \in \mathbb{C}$, pour tout morphisme $f : A \rightarrow B$, $g : B \rightarrow C$ et $h : C \rightarrow D$ on a $(h \circ g) \circ f = h \circ (g \circ f)$;
- Pour tout objet $x \in \mathbb{C}$ il existe un morphisme distingué $id_x : X \rightarrow X$;
- Pour tout $x \in \mathbb{C}$ et pour tout $f = A \rightarrow X, g = X \rightarrow B$, on a $f \circ id_x = f$ et $id_x \circ g = g$.

Les ensembles d'objets et de morphismes sont à comprendre au sens intuitif (parfois appelé naïf) comme une collection d'objets. Si les ensembles sont également des ensembles au sens de ZFC (ou votre métathéorie favorite), on dit que la catégorie est **petite**.

On introduit quelques notions de théorie des catégories :

- f est un **monomorphisme** si $gf = hf \Rightarrow h = g$. L'idée est celle d'une fonction injective. Cette définition ne colle pas trop à l'intuition dans un cas général, mais fonctionne dans le cas des topos pour des raisons qui deviendront plus claires par la suite. On raccourcit souvent " f est mono" ;
- f est **épimorphisme** si $fg = fh \Rightarrow h = g$. L'idée est celle d'une fonction surjective (même remarque) ;
- $f : A \rightarrow B$ est **isomorphisme** s'il existe un morphisme f^{-1} tel que $ff^{-1} = id_A$ et $f^{-1}f = id_B$. Les deux conditions sont indépendantes et l'idée est que ces deux objets sont semblables. En composant avec f et f^{-1} , on a une équivalence entre les morphismes partant et venant de A et ceux de B . Ces deux objets interagissent de la même manière avec les autres objets de la catégorie et toutes leurs propriétés seront les mêmes, c'est pourquoi les propriétés catégoriques sont toujours définies à isomorphisme près ;
- Un **diagramme** est un ensemble de flèches et d'objets de départ et d'arrivée (appelé domaine et codomaine, en analogie au cas des fonctions). On dit qu'il commute si tous les chemins entre deux objets sont égaux.

Un exemple de diagramme qui commute :

$$\begin{array}{ccc} A & \xrightarrow{id_A} & A \\ \downarrow f & & \downarrow f \\ B & \xrightarrow{id_B} & B \end{array}$$

- Si \mathcal{D} est un diagramme ou une catégorie, son **dual** \mathcal{D}^{op} est celui obtenu en changeant le sens des flèches. Comme les définitions en catégories se définissent souvent en termes de diagrammes, l'objet qui respecte la définition duale est appelé **le dual** ou le **co-**.

Par exemple un épimorphisme est le dual d'un monomorphisme, et le coproduit est le dual du produit ;

- Un **foncteur** est une paire de fonctions (au sens large) entre catégories qui préserve la structure de catégorie, c'est-à-dire un foncteur F envoie les objets sur les objets, les flèches sur les flèches tout en respectant

- $F(id_A) = id_{F(A)}$

- si $f : A \rightarrow B$ alors $F(f) : F(A) \rightarrow F(B)$

- $F(f \circ g) = F(f) \circ F(g)$

Il peut arriver que $F(f) : F(B) \rightarrow F(A)$ et $F(f \circ g) = F(g) \circ F(f)$. Dans ce cas, on dit que F est un foncteur contravariant, noté de manière covariante $F : \mathcal{C}^{op} \rightarrow \mathcal{D}$;

- Une limite d'un foncteur $F : \mathcal{D} \rightarrow \mathcal{C}$ est un objet $L \in \mathcal{C}$ et un morphisme $L \rightarrow F(D)$ pour tout objet $D \in \mathcal{D}$. Cela fait une sorte de cône au dessus du diagramme $F\mathcal{D}$.

On demande en plus que :

- Le diagramme de l'image de F et du cône limite est un diagramme qui commute ;

- Pour tout autre cône $(L', \{g_D\})$ au dessus de $F(\mathcal{D})$, il existe un unique morphisme $L \rightarrow L'$ qui fait commuter le diagramme total.

Par exemple, soit $\mathcal{D} =$

$$A \rightrightarrows B$$

Un foncteur F choisit deux morphismes de \mathcal{C} avec le même domaine et codomaine. La limite de F est alors un objet L avec une flèche f tel que le diagramme suivant commute.

$$\begin{array}{ccc} L & & \\ \downarrow f & \searrow fu=fv & \\ A & \xrightarrow{u} & B \\ & \xrightarrow{v} & \end{array}$$

On demande donc f tel que $fu = fv$. La seconde condition dit que f doit être minimal, en ce sens que tout autre candidat (L', g) doit pouvoir se factoriser, représenté par ce diagramme

$$\begin{array}{ccc} L & \xrightarrow{f} & A \xrightarrow{u} B \\ \uparrow \exists! \downarrow g & \nearrow & \xrightarrow{v} \\ L' & & \end{array}$$

Cette limite est la définition d'**égalisateur** de (u, v) et on dit que f est un **mono-régulier**. Les monos réguliers sont une meilleure définition des fonctions injectives. Heureusement dans les topos, la distinction est superflue.

Cette introduction bien que très rapide couvre les notions de base de la théorie des catégories. Dans la suite nous supposons que le lecteur est familier avec certains outils qui n'ont pas été définis ici comme les foncteurs représentables et les adjonctions. Nous invitons le lecteur peu familier avec ces points à lire la référence [7].

Nous prendrons les conventions suivantes de notation :

- id_A est le morphisme d'identité $id_A : A \rightarrow A$;
- Les objets sont notés en majuscule, les morphismes en minuscule et les catégories avec des lettres particulières, par exemple \mathbb{C}, ξ ;
- $X \in \mathbb{C}$ signifie un objet X de la catégorie \mathbb{C} ;
- Pour $f : A \rightarrow B$ et $g : B \rightarrow C$, la composition se note $g \circ f = fg$. L'intuition est que, si f, g sont des fonctions alors $f(g) = f \circ g$, et que la lecture de flèches dans un diagrammes se fasse dans l'ordre. \circ se lit donc "après" et le diagramme suivant se lit $fg = h$.

$$\begin{array}{ccc} B & \xrightarrow{g} & C \\ f \uparrow & \nearrow h & \\ A & & \end{array}$$

- Les monos sont notés $A \rightarrowtail B$ ou encore $A \hookrightarrow B$;
- Les épis sont notés $A \twoheadrightarrow B$.

Quelques exemples

3.2 La catégorie \mathbb{N}

Soit la catégorie dont les objets sont les nombres naturels. Il existe un morphisme $\blacksquare : N \rightarrow M$ si $N \leq M$. Cette catégorie est une catégorie petite, dont les morphismes sont donnés par une structure d'ordre.

3.3 La catégorie Ens

Soit la catégorie qui contient comme objets les ensembles au sens de ZFC. Cette catégorie n'est pas petite, car il n'existe pas d'ensemble qui contient tous les ensembles. Les morphismes de Ens sont toutes les fonctions entre deux ensembles. L'identité et la composition sont données par la fonction identité et la composition de fonctions.

Cette catégorie va jouer un rôle spécial par la suite, c'est pourquoi on va lister quelques caractéristiques :

1. Il y a un objet **initial** $1 = \{\cdot\}$. Un objet initial est la limite du foncteur vide, c'est-à-dire un objet tel que pour tout autre objet $A \in Ens$, il existe une unique fonction $! : A \rightarrow \{\cdot\}$;
2. Il y a un objet **terminal** $0 = \emptyset$. Il s'agit de la propriété duale de l'initial, donc pour tout $A \in Ens$ il existe un unique $! : \emptyset \rightarrow A$;
3. Si $A, B \in Ens$ il y a un **produit** $A \times B = \{(a, b) \mid a \in A, b \in B\}$, et des fonctions (π_A, π_B) de projection sur A et B , qui forment la limite d'un foncteur défini sur une catégorie avec deux objets et pas de flèches.

4. Le coproduit est l'union disjointe $A \dot{\cup} B$ avec les inclusions canoniques ;
5. Si $u, v : A \rightarrow B$ sont deux fonctions, leur égalisateur est donné par $\{a \in A \mid u(a) = v(a)\}$ et la fonction d'inclusion ;
6. 1 est un **générateur**, en ce sens que si $f \neq g$ alors il existe un élément $x : 1 \rightarrow \text{dom}(f)$ tel que $f(x) \neq g(x)$;
7. Les monos sont les fonctions injectives, les épis sont les fonctions surjectives et les isos sont les fonctions bijectives ;
8. Par l'axiome du choix, pour tout épi $f : A \rightarrow B$ il existe un inverse à gauche $s : B \rightarrow A$ tel que $sf = id_B$;
9. Pour tout ensemble $A \in \text{Ens}$, l'objet $\mathcal{P}(A) = \{x \subseteq A\}$ est un objet de Ens ;
10. Chaque objet de Ens est un ensemble et peut donc être muni d'une structure d'algèbre de Boole comme au point 2.3.1 ;
11. Pour tout sous-ensemble $S \subseteq A$, il existe une fonction caractéristique $\chi_S : A \rightarrow \{1, 0\} = \Omega$ qui vaut 1 si $x \in S$ et 0 sinon ;
12. Si A, B sont des ensembles alors la collection de toutes les fonctions de A vers B est également un ensemble (par les axiomes de ZFC). On note cet ensemble B^A ;
13. Il existe une fonction $0 : 1 \rightarrow \mathbb{N}$ et une fonction $S : \mathbb{N} \rightarrow \mathbb{N}$ qui caractérisent les nombres naturels ;
14. Toute fonction est décomposable en epi-mono.

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 & \searrow e & \nearrow i \\
 & & \text{im}(f)
 \end{array}$$

Certaines de ces propriétés sont uniques à Ens et certaines vont revenir par la suite.

Les propriétés 1 – 5, 9, 11, 12, 14 sont des propriétés qui seront vraies dans tous les topos.

La propriété 11 est plus spécifique aux ensembles. Un topos qui respecte cette propriété est appelé **Booléen**, mais en général il existe seulement une structure d'algèbre de Heyting.

La propriété 6 s'appelle être **bien pointé**, et la propriété 8 est appelé **axiome du choix**. Finalement la propriété 13 définit un **objet de nombre naturels** dans une catégorie générale.

3.4 Définition de topos

Il y a plusieurs manières différentes de définir un topos, [5] a une liste de définitions différentes. Nous allons prendre la définition la plus courante, et travailler comme un catégoricien. Le lecteur est prévenu que la suite est dense en définitions et est encouragé à lire la suite plusieurs fois.

On définit un topos comme une catégorie qui :

1. est finiment complète et finiment cocomplète ;
2. est cartésienne fermée ;

3. à un classificateur de sous-objets.

La définition précédente est légèrement redondante. En effet, la cocomplétude est dérivable à partir des 3 autres conditions, mais cette affirmation restera sans démonstration.

On va maintenant définir tous les termes :

3.4.1 Catégorie cartésienne fermée

Une catégorie est cartésienne fermée si elle a des produits finis (inclus le produit vide) et que pour tout objet X le foncteur $Y \mapsto X \times Y$ a un adjoint à droite.

Cet adjoint à droite est l'exponentielle, noté $(-)^X : Y \mapsto Y^X$. Cet exponentielle se caractérise par un morphisme particulier, appelé **évaluation**, avec la propriété universelle suivante : pour tout $g : C \times A \rightarrow B$, il existe un unique \hat{g} tel que le diagramme suivant commute.

$$\begin{array}{ccc} B^A \times A & \xrightarrow{ev} & B \\ \hat{g} \times id_A \uparrow & \nearrow g & \\ C \times A & & \end{array}$$

Dans la catégorie Ens , Y^X est l'ensemble des fonctions de X à Y et le diagramme correspond à associer à $f(c, x)$ la fonction $f_c(\cdot)$ et puis évaluer en x . Cette opération est appelé Curryfication et représente une certaine notion de fonction interne.

En particulier, on a $A \simeq 1 \times A$ et donc pour tout morphisme $f : A \rightarrow B$, on définit le nom de f par $[f] : 1 \rightarrow B^A$ qui fait commuter le diagramme.

$$\begin{array}{ccc} B^A \times A & \xrightarrow{ev} & B \\ [f] \times id_A \uparrow & \nearrow f \circ pr_A & \\ 1 \times A & & \end{array}$$

Avec ce diagramme, chaque morphisme $f : A \rightarrow B$ est associé à un élément global de l'ensemble B^A . C'est la notion interne d'ensemble des fonction de A vers B .

3.4.2 Classificateur de sous-objet

Dans Ens , on a pour $C \subseteq B \subseteq A$ que B factorise C

$$\begin{array}{ccc} B & \xrightarrow{b} & A \\ i \uparrow & \nearrow c & \\ C & & \end{array}$$

Cela nous donne l'idée de définir un sous-ensemble de X comme étant un monomorphisme vers X . Cependant plusieurs monos peuvent définir le même sous-objet.

On définit pour m, n mono vers X que $n \leq m$ si m factorise n , c'est-à-dire s'il

existe un t tel que :

$$\begin{array}{ccc} M & \xrightarrow{m} & X \\ \uparrow \scriptstyle t & \nearrow \scriptstyle n & \\ N & & \end{array}$$

Cela force la relation suivante :

$$n \cong m \Leftrightarrow n \leq m \text{ et } m \leq n \Leftrightarrow \exists t \text{ isomorphisme tel que } tm = n$$

On définit l'ensemble (au sens large) des sous-objets $Sub(X)$ comme les monomorphismes vers X quotienté par cette relation d'équivalence. Il est facile de voir que cet ensemble préordonné est borné (par id_X et $0 : 0 \rightarrow X$ respectivement). Nous montrerons dans la suite qu'il s'agit en fait d'une algèbre de Heyting.

Un classificateur de sous-objets est un objet Ω et un morphisme $\top : 1 \rightarrow \Omega$ tel que pour tout mono $m : M \rightarrow X$ il existe un unique morphisme $\chi_m = X \rightarrow \Omega$ (appelé fonction caractéristique de m) qui transforme le diagramme suivant en produit fibré.

$$\begin{array}{ccc} M & \xrightarrow{m} & X \\ \downarrow \scriptstyle !m & & \downarrow \scriptstyle \chi_m \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Un tel classificateur est unique à isomorphisme près. Ceci est dû au fait que c'est un représentant du foncteur de sous-objets.

On peut démontrer que si $\chi_m = \chi_n$ alors $m \cong n$, ce qui justifie l'appellation de fonction caractéristique.

On note \top_M le morphisme $!_M \top$, ce qui permet de lire le produit fibré au-dessus comme $m\chi_m = \top_M$.

On nomme également valeurs de vérités l'ensemble Ω , la justification de ce nom est ce qui a motivé ce mémoire. La réponse viendra lorsque nous interpréterons les phrases logiques dans un topos. Il est important de noter que $Sub(X)$ n'est pas un objet de la catégorie, c'est Ω^X qui jouera le rôle interne d'ensembles des parties de X .

Remarques

La plupart des définitions dans l'approche catégorique ont en réalité plusieurs définitions selon le niveau. Par exemple demander que \mathbb{C} aie un classificateur de sous-objet n'est rien d'autre que demander que le foncteur $Sub : \mathbb{C} \rightarrow Ens$ soit représentable. Cela donne une définition en termes internes à la catégorie et en termes inter-catégoriques.

Ces doubles définitions font la force des catégories, car une question posée en termes internes à une catégorie a rapidement une réponse en termes inter-catégoriques et vice versa, mais également est la cause de beaucoup d'incompréhension ("categorical nonsense"), car le changement de niveau ambiant cause une perte de l'intuition. Par exemple, la caractérisation de $\mathcal{P}(X)$ en termes catégoriques paraît relativement compréhensible en termes internes (l'ensemble qui a telles propriétés) mais cette intuition disparaît si on est introduit par la définition externe, donné par un isomorphisme naturel $Sub(B \times A) \simeq \mathbb{C}(A, \mathcal{P}(B))$.

3.5 Exemples

La catégorie Ens est un topos. La catégorie Ens_f des ensembles finis est un topos, avec les mêmes limites, exponentielles et classificateur de sous-objets.

La plupart des exemples sont construits à partir d'autres topos.

Soit \mathbb{C} une catégorie petite, alors $Ens^{\mathbb{C}}$ la catégorie des foncteurs de \mathbb{C} vers Ens est un topos.

La catégorie comma entre deux topos est un topos. En particulier la catégorie $\mathbb{C} \uparrow A$ des morphisme partant de A , $\mathbb{C} \downarrow A$ des morphisme vers A , et $\mathbb{C} \rightarrow$ la catégorie des flèches de \mathbb{C} sont des topos.

Soit G un groupe, potentiellement non petit, alors Ens^G est aussi un topos.

Si (C, T) est un site alors $Sheaves(C, T)$ la catégorie des faisceaux sur (C, T) est un topos.

Si M est un monoïde, on peut définir un topos $M-Set$. Les objets sont (X, λ) où λ est une action de M sur l'ensemble X , et les morphismes $f : (X, \lambda) \rightarrow (Y, \mu)$ sont des fonctions $f : X \rightarrow Y$ tel que le diagramme suivant commute pour tout $m \in M$.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \lambda_m \downarrow & & \downarrow \mu_m \\ X & \xrightarrow{f} & Y \end{array}$$

4 Les topos comme ensembles

4.1 Les morphismes sont des fonctions

On commence par montrer que les épis et monos se comportent comme des fonctions surjectives et injectives et que les fonctions ont une factorisation canonique.

Théorème 4.1.1. *Dans un topos, soit $f : A \rightarrow B$. On a :*

1. f est un mono si et seulement si f est un mono régulier ;
2. f est mono et épi implique f est un isomorphisme ;
3. f admet une décomposition épi-mono qui correspond à l'image de f dans B .

Démonstration. 1) Par la définition de classificateur de sous-objets, un mono $f : A \rightarrow B$ est l'égalisateur de χ_f et de \top_B

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \chi_A & \searrow & \downarrow \chi_f \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Rappelons qu'un mono régulier est toujours un mono.

$$\begin{array}{ccc} X & & \\ \downarrow u & \searrow t & \\ A & \xrightarrow{m} & B \xrightarrow[x]{y} C \end{array}$$

$t = um = vm$ implique que ce morphisme égalise aussi x, y , donc il existe un unique morphisme $p : X \rightarrow A$ tel que $pm = t$. Comme u, v sont tous les deux des morphismes acceptables, par unicité on déduit que $p = u = v$.

2) C'est en fait un résultat plus général des catégories. On sait que $f\chi_f = f\top_B$ car f est un égalisateur, mais comme f est épi, on en déduit $\chi_f = \top_B$, et donc f est l'égalisateur de \top_B avec lui-même. Par les propriétés de l'égalisateur, f doit être un isomorphisme.

3) Un théorème plus général du cours de théorie des catégories que j'ai suivi à l'université de Coimbra, affirme que (épi,mono) est un système de factorisation si une catégorie a les propriétés suivantes :

- La catégorie est complète et cocomplète ;
- Les monos sont tous réguliers ;
- Le produit fibré préserve les épimorphismes.

Malheureusement, je n'ai pas trouvé de preuve facile pour démontrer que les produits fibrés des topos préservent les épimorphismes. Nous ferons donc la preuve du point 3) sans utiliser ce résultat.

La preuve est contenue dans le diagramme suivant :

$$\begin{array}{ccccccc} & & f & & & & \\ & \curvearrowright & & \curvearrowleft & & & \\ A & \dashrightarrow & M & \dashrightarrow & B & \xrightarrow[x]{y} & Y \\ \parallel & & & & \parallel & & \downarrow u \\ A & \xrightarrow{e'} & N & \xrightarrow{m'} & B & \dashrightarrow[s]{t} & Z \end{array}$$

Construisons le diagramme étape par étape. x, y est la paire conoyau de f , c'est-à-dire c'est celle obtenue en faisant le coproduit fibré de f avec lui-même. Cela veut dire en particulier que $fx = fy$.

On considère maintenant l'égalisateur de x, y . C'est un morphisme $m : M \rightarrow B$. Par la propriété universelle, comme $fy = fx$, il existe un morphisme $e : A \rightarrow M$ tel que $em = f$.

Il nous reste à prouver que e est épi et que toute factorisation se termine par le même sous-objet de B . Soit e', m' une autre factorisation, représentée par la ligne du dessous. Par le point 1, on sait que m' est l'égalisateur de deux flèches, disons $s, t : B \rightarrow Z$. On a alors $fs = e'm's = e'm't = ft$. Par la propriété universelle de la paire conoyau, il existe $u : Y \rightarrow Z$ tel que $s = xu$ et $t = yu$.

On vérifie que $ms = mxu = myu = mt$. Par la propriété universelle de l'égalisateur, m se factorise dans m' , c'est-à-dire que $m \leq m'$ en tant que sous-objets de B . Un raisonnement similaire est appliqué dans l'autre sens pour déduire que m et m' représentent le même sous-objet de B .

Pour prouver que e est épi, on passe par un cas intermédiaire. Si m est un iso, alors $mx = my \Rightarrow m^{-1}mx = m^{-1}my \Rightarrow x = y$. La paire conoyau de f est x, x , ce qui implique que f est épi.

Dans le cas général on factorise e et on trouve :

$$A \xrightarrow{e''} M' \xrightarrow{m''} M \xrightarrow{m} B$$

$\underbrace{\hspace{10em}}_f$

$e'', m''m$ est une autre factorisation de f , donc $m''m$ doit représenter le même sous-objet que m . On en déduit que m'' est un isomorphisme et, par la remarque précédente, e est épi. \square

Ces démonstrations sont tirées de [8, IV.2, IV.6].

4.2 Topos et power-objet

Dans la vision ensembliste des mathématiques, un ensemble est construit à partir d'éléments qui existe indépendamment de l'ensemble. En catégories par contre, les éléments en eux-même ont peu d'importance, seules comptent les relations entre eux. Ceci a amené à la construction de théories des ensembles structurelles (en opposition à une théorie des ensembles matérielle comme ZFC). L'exemple le plus important est *ETCS* de Lawvere. Dans cette théorie les éléments d'un ensemble existent toujours en relation aux autres éléments, mais pas forcément dans l'absolu.

Pour prendre des exemples plus pratiques, l'ensemble \mathbb{N} est souvent pensé de manière matérielle, les nombres $1, 2, 3 \dots$ existent indépendamment de la manière dont on définit \mathbb{N} . De plus on utilise ces nombres sans faire appel à l'ensemble \mathbb{N} , par exemple lors de constructions finies. L'ensemble S_1 du cercle est quant à lui pensé en termes de relations, on ne pense généralement pas aux éléments du cercle en dehors de leur contexte : peut importe que les éléments de S_1 soient des angles ou des nombres complexes de la forme $e^{i\theta}$, ou encore le segment $[0, 1]$ avec une identification entre le premier et le dernier élément. Tant que le cercle se referme, on a bien le "même" objet.

Pour capturer ces subtilités, une généralisation d'ensemble doit avoir quelque chose qui joue le rôle de l'appartenance \in , quitte à restreindre ce symbole à une appartenance en contexte \in_A .

Nous allons maintenant prouver que les topos ont cette propriété, ce que rend plus naturelle leur lecture comme ensembles généralisés. Nous suivons [2, section 4.7].

Dans la théorie des ensembles classique, on peut définir

$$\in_A = \{(x, S) \mid x \in S \subseteq A\} \subseteq A \times \mathcal{P}(A).$$

Pour traduire cet ensemble en termes catégoriques, il faut un objet qui traduise $\mathcal{P}(A)$ et caractérise le sous-ensemble \in_A en termes propre au topos. Ceci se fait grâce aux fonctions caractéristiques. Dans *Set* on a

$$\in_A \simeq \{(x, \chi_S) \mid \chi_S(x) = 1\} \subseteq 2^A \times A.$$

On utilise maintenant la fonction d'évaluation (car un topos est cartésien fermé), pour caractériser \in_A par le produit fibré suivant :

$$\begin{array}{ccc} \in_A & \hookrightarrow & 2^A \times A \\ \text{!} \downarrow & & \downarrow \text{ev} \\ 1 & \xrightarrow{\top} & 2 \end{array}$$

Pour un objet $A \in \mathbb{C}$, on souhaite définir son power-objet (son ensemble de parties) comme étant un objet $\mathcal{P}(A) = \Omega^A$ et un morphisme \in_A donné par le produit fibré suivant :

$$\begin{array}{ccc} \in_A & \hookrightarrow & \Omega^A \times A \\ \text{!} \downarrow & & \downarrow \text{ev} \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Cette caractérisation dépend des objets d'un topos, mais il existe heureusement une autre caractérisation qui est plus générale et qui peut sortir du cadre des topos.

Dans *Set*, une relation quelconque $R \subseteq B \times A$ peut être associée à une fonction $F_R : B \rightarrow \mathcal{P}(A)$ de l'ensemble des éléments de A en relation avec B . Cette fonction vérifie $(x, y) \in R$ ssi $y \in F_R(x)$ ssi $(F_R(x), y) \in \in_A$. Cette dernière relation nous donne le produit fibré suivant :

$$\begin{array}{ccc} R & \hookrightarrow & B \times A \\ g \downarrow & & \downarrow F_R \times \text{id}_A \\ \in_A & \hookrightarrow & \mathcal{P}(A) \times A \end{array}$$

Avec g la restriction de $F_R \times \text{id}_A$ au sous-ensemble R . En d'autres termes, la relation d'appartenance permet de classifier les relations, de la même manière que les valeurs de vérités classifient les sous-objets, et la fonction $F_R : A \rightarrow B$ joue le rôle de fonction caractéristique.

On introduit la définition suivante :

Définition 4.2.1. Soit \mathbb{C} une catégorie avec des produits. On dit que \mathbb{C} a des power-objet si pour tout objet $A \in \mathbb{C}$ il existe un objet $\mathcal{P}(A)$ et un monomorphisme $\in : \in_A \rightarrow \mathcal{P}(A) \times A$ tel que pour tout $B \in \mathbb{C}$ et toute relation $r : R \rightarrow B \times A$,

il existe un unique mono $f_r : B \rightarrow \mathcal{P}(A)$ qui rend le produit fibré suivant possible.

$$\begin{array}{ccc} R & \xrightarrow{r} & B \times A \\ \downarrow & & \downarrow f_r \times id_A \\ \in_A & \xrightarrow{\epsilon} & \mathcal{P}(A) \times A \end{array}$$

On appelle f_r le nom de la relation r .

On va maintenant démontrer le résultat suivant, qui justifie de percevoir un topos comme étant un ensemble généralisé.

Théorème 4.2.2. *Soit \mathbb{C} un catégorie complète, alors les deux conditions suivantes sont équivalentes :*

1. \mathbb{C} est un topos ;
2. \mathbb{C} a des power-objet.

La démonstration va être coupée en plusieurs parties, le début provient de [2, ch.4.7], et la fin de [8, IV.2].

(1) \Rightarrow (2). On reprend la construction dans *Ens* et prouve qu'elle se généralise. Soit $A \in \mathbb{C}$, on pose $\mathcal{P}(A) = \Omega^A$ et \in_A le sous-ensemble caractérisé par la fonction d'évaluation, c'est-à-dire que le carré suivant est un produit fibré :

$$\begin{array}{ccc} \in_A & \hookrightarrow & \Omega^A \times A \\ \downarrow ! & & \downarrow ev \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Vérifions maintenant la propriété, soit $r : R \rightarrow B \times A$, on peut construire sa fonction caractéristique :

$$\begin{array}{ccc} R & \xrightarrow{r} & B \times A \\ \downarrow ! & & \downarrow \chi_r \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

comme χ_R est un morphisme de $B \times A \simeq A \times B$ vers Ω , on utilise le fait que \mathbb{C} est cartésien fermé pour avoir un unique $\hat{\chi}_R : B \rightarrow \Omega^A$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} \Omega^A \times A & \xrightarrow{ev} & \Omega \\ \hat{\chi}_R \times 1_A \uparrow \vdots & \nearrow \chi_R & \\ B \times A & & \end{array}$$

On conclut avec le diagramme suivant :

$$\begin{array}{ccc} R & \xrightarrow{r} & B \times A \\ \downarrow g & & \downarrow \hat{\chi}_R \times 1_A \\ \in_A & \hookrightarrow & \Omega^A \times A \\ \downarrow ! & & \downarrow ev \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

(A curved arrow on the left points from the bottom-left corner to the top-left corner.)

Le carré externe commute, car c'est le diagramme de χ_R , le carré du bas est le produit fibré, donc par la propriété universelle, il existe un unique morphisme g qui fasse commuter le tout. Comme le carré externe et celui du bas sont tout les deux des produits fibrés, on en déduit que le carré du haut est également un produit fibré. La preuve de cette propriété est dans [9, 4.4] ou dans [7]. \square

Dans l'autre sens, comme \mathbb{C} est une catégorie complète, il ne reste qu'à reconstruire un classificateur de sous-objets et une exponentielle.

Power-objet \Rightarrow Classificateur de sous-objets. Pour retrouver le classificateur de sous-objets, on remarque que $A \simeq 1 \times A$ et on pose $\Omega = \mathcal{P}(1)$

On affirme maintenant que $\epsilon: \epsilon_1 \rightarrow \Omega$ est un classificateur de sous-objet.

Soit $M \succrightarrow A$ un sous-objet de A , on construit sa fonction caractéristique comme suit :

$$\begin{array}{ccc} M & \succrightarrow & A \times 1 \simeq A \\ \downarrow & & \downarrow f_m \times id_1 \\ \epsilon_1 & \xrightarrow{\epsilon} & \mathcal{P}(1) \times 1 \simeq \Omega \end{array}$$

où f_m est le nom de la relation $M \leq A \times 1$. La propriété universelle découle directement de la propriété universelle du power-objet.

C'est un représentant du foncteur de sous-objet donc isomorphe à $1 \rightarrow \Omega$. \square

4.2.3 Remarque sur les sous-objets

Le classificateur de sous-objets

$$\begin{array}{ccc} M & \xrightarrow{m} & B \\ \downarrow \chi_m & & \downarrow \chi_m \\ 1 & \xrightarrow{\tau} & \Omega \end{array}$$

assigne à chaque sous-objet $m \subseteq B$ un morphisme $\chi_m : X \rightarrow \Omega$. Comme le produit est unique à isomorphisme près, on peut aller dans l'autre sens. Cela nous fournit donc un isomorphisme canonique entre $Sub(B)$ et $\mathbb{C}(B, \Omega)$.

De même le power-objet donne un isomorphisme canonique pour $M \subseteq B$

$$\begin{array}{ccc} M & \hookrightarrow & 1 \times B \\ g \downarrow & & \downarrow f \times id \\ \epsilon_A & \xrightarrow{\epsilon} & \mathcal{P}(B) \times B \end{array}$$

qui assigne à chaque sous-objet $m \subseteq B$ un morphisme $f : 1 \rightarrow \mathcal{P}(B)$.

On a donc un isomorphisme :

$$Sub(B) \simeq \mathbb{C}(1, \mathcal{P}(B)) \simeq \mathbb{C}(B, \Omega)$$

qui permet de noter un sous-objet de trois manières :

$$m : S \succrightarrow B, \quad \phi : B \rightarrow \Omega, \quad f : 1 \rightarrow \mathcal{P}(B)$$

avec comme formules utiles :

$$S = \{b \in B \mid \phi(b)\}, \quad \phi = \chi_S, \quad f = [\phi].$$

Dans les traitements catégoriques, ces isomorphismes sont appelés des transposées et les détails technique de la transposition sont laissés sous silence. Dans certains livres (comme [8]) le power-objet est défini en termes de transposées. Il arrive aussi de réserver le symbole \in_A pour le morphisme que l'on a noté ev_A . Il semblait plus clair de noter le symbole d'appartenance dans la structure d'ensemble et l'évaluation dans la structure logique. De plus ev_A est également le morphisme évaluation obtenu par l'exponentielle Ω^A .

Power-objet \Rightarrow Exponentielles. On va commencer par prouver un cas particulier d'exponentielle, puis construire le cas général.

Remarquons tout d'abord que la définition de power-objet nous donne certaines exponentielles, à savoir Ω^A pour tout objet $A \in \mathbb{C}$. Soit un morphisme $B \times A \rightarrow \Omega$, on peut voir ce morphisme comme classifiant un sous-objet de $B \times A$, et écrire le diagramme suivant :

$$\begin{array}{ccc} M & \xrightarrow{m} & B \times A & \xrightarrow{\chi_M} & \Omega \\ g \downarrow & & \downarrow f \times id_A & \nearrow \chi_\epsilon = ev_A & \\ \in_A & \xrightarrow{\epsilon} & \Omega^A \times A & & \end{array}$$

Sur ce graphe le carré de droite est commutatif, ce qui nous donne $m(f \times id_A) = g \epsilon$, et les lignes du haut et du bas sont composées d'un sous-ensemble et de sa fonction caractéristique, ce qui donne $m\chi_m = \top_M$ et $\epsilon \chi_\epsilon = \top_{\Omega^A}$. Comme m est mono, il suffit de prouver que $m(f \times id_A)\chi_\epsilon = m\chi_m$.

On a

$$\begin{aligned} m(f \times id_A)\chi_\epsilon &= g \epsilon \chi_\epsilon \\ &= g \top_\epsilon \\ &= \top_M \\ &= m\chi_m \end{aligned}$$

L'unicité de f est laissé en exercice au lecteur.

On remarque que le power-objet nous demande d'avoir une relation $R \rightarrow A \times B$. Par la remarque précédente, c'est équivalent à avoir un morphisme $\phi : A \times B \rightarrow \Omega$, représenté ici par le triangle de droite. Cette forme de trapèze va être utilisée par la suite.

Pour le cas général, on s'inspire à nouveau du cas des ensembles.

Dans la théorie *ZFC*, les fonctions sont définies formellement à partir de leur graphes, c'est-à-dire comme un ensemble de paires d'éléments, qui nous donne une identification $f : A \rightarrow B \simeq F \subseteq A \times B$ ou F est une relation qui a certaines propriétés. Nous allons étendre cette construction à un topos quelconque et vérifier que cela coïncide avec l'exponentielle. La démonstration est tirée de [8, IV.2].

Une fonction $f : A \rightarrow B$ est une relation qui à chaque élément de A , associe un élément de B . On peut donc construire pour une relation $R \subseteq A \times B$ les éléments suivants :

- $v(a, R) = \{b \in B \mid aRb\} = \{b \mid \langle a, b \rangle \in R\} \in \mathcal{P}(B)$ qui regarde pour un élément de A , quels éléments de B sont en relation ;
- $u(R) = \{a \in A \mid v(a, R) \text{ est un singleton}\} \in \mathcal{P}(A)$.

On pourra conclure que R est le graphe d'une fonction de A vers B ssi $u(R) = A$.

Pour traduire ceci en termes internes au topos, on commence par identifier le morphisme $A \in \mathcal{P}(A)$, avec le diagramme suivant.

$$\begin{array}{ccc} A & \longleftarrow & 1 \times A \\ g \downarrow & & \downarrow f \times id \\ \in_A & \xrightarrow{\epsilon} & \mathcal{P}(A) \times A \end{array}$$

L'unique $f : 1 \rightarrow \mathcal{P}(A)$ donné par le power-objet sera noté $[\top_A]$. Ce nom vient de la transposition de $A = \{a \in A \mid \top\} \subseteq A$, qui donne la formule logique $\phi = \top_A = \chi_A : A \rightarrow \Omega$ en transposant une seconde fois, on obtient le morphisme $[\top_A] : 1 \rightarrow \mathcal{P}(A)$.

On passe maintenant à la construction de u et v .

Par souci de clarté, on omettra les isomorphismes relatifs à l'ordre du produit, c'est-à-dire on considère $A \times B = B \times A$ et $A \times (B \times C) = (A \times B) \times C$, que l'on écrira $A \times B \times C$.

On définit $v = A \times \mathcal{P}(A \times B) \rightarrow \mathcal{P}(B)$ comme suit :

$$\begin{array}{ccc} \in_{A \times B} & \xrightarrow{\epsilon} & B \times A \times \mathcal{P}(A \times B) \xrightarrow{ev} \Omega \\ g \downarrow & & \downarrow id_B \times v \\ \in_B & \xrightarrow{\epsilon} & B \times \mathcal{P}(B) \end{array}$$

C'est-à-dire que v est la transposée de $ev_{A \times B}$.

Pour définir u , il nous faut une manière de déterminer si un élément est un singleton, et cela se fait à l'aide du diagramme suivant :

$$\begin{array}{ccc} B & \xrightarrow{\Delta} & B \times B \xrightarrow{\delta} \Omega \\ g \downarrow & & \downarrow id_b \times \{\cdot\}_B \\ \in_B & \xrightarrow{\epsilon} & B \times \mathcal{P}(B) \end{array}$$

Ce qui nous donne un morphisme $\{\cdot\}_B : B \rightarrow \mathcal{P}(B)$, qui assigne à chaque élément b l'ensemble $\{b\}$ contenant cet élément. Comme c'est un monomorphisme, on peut regarder sa fonction caractéristique $\sigma_B = \chi_{\{\cdot\}_B} : \mathcal{P}(B) \rightarrow \Omega$, qui s'interprète comme la phrase logique "être un singleton".

La construction de Δ et de δ est une construction plus générale que le cas du topos, aussi ces morphismes reviennent dans d'autres contexte dès qu'il s'agit de formaliser une égalité. Par exemple dans un topos, δ classe l'égalité en ce sens que :

Lemme 4.2.4. *Soit $f, g : A \rightarrow B$, on a $f = g$ si et seulement si $(f, g)\delta_B = \top_A$*

Démonstration. Un sens est immédiat, si $f = g$ alors

$$(f, f)\delta_B = f(id_B, id_B)\delta_B = f\top_B = \top_A.$$

Dans l'autre sens si $(f, g)\delta_B = \top_A$ alors par la propriété du produit, on a

$$\begin{array}{ccccc}
 & & A & & \\
 & & \curvearrowright & & \\
 & & \downarrow k & & \\
 & & B & \longrightarrow & 1 \\
 (f, g) & & \downarrow (id_B, id_B) & & \downarrow \top \\
 & & B \times B & \xrightarrow{\delta} & \Omega
 \end{array}$$

et donc $(f, g) = k(id_B, id_B) = (k, k)$. On en déduit $f = k = g$. \square

On a maintenant les outils pour définir les morphismes u, v correspondant aux fonctions respectives dans Ens .

On définit $u : \mathcal{P}(A \times B) \rightarrow \mathcal{P}(A)$ comme la transposée de $v\sigma_B$.

Soit $\phi : A \times \mathcal{P}(A \times B) \xrightarrow{v} \mathcal{P}(B) \xrightarrow{\sigma_B} \Omega$, qui correspond à la propriété " $v(a, R)$ est un singleton".

$$\begin{array}{ccc}
 R & \xrightarrow{\{x|\phi\}} & A \times \mathcal{P}(A \times B) \xrightarrow{\phi} \Omega \\
 g \downarrow & & \downarrow id_A \times u \quad \searrow ev \\
 \in_A & \xrightarrow{\epsilon} & A \times \mathcal{P}(A)
 \end{array}$$

Le morphisme ev n'est pas strictement nécessaire pour l'instant, mais reviendra plus tard. On note que le graphe commute toujours, car $\mathcal{P}(A) = \Omega^A$.

On souhaite maintenant construire l'ensemble des fonctions, interprétées comme graphes. C'est-à-dire l'ensemble des relations $R \subseteq A \times B$ tel que $u(R) = A$ et on le trouve en construisant le produit fibré de u par $[\top_A]$.

$$\begin{array}{ccc}
 B^A & \longrightarrow & 1 \\
 \downarrow m & & \downarrow [\top_A] \\
 \mathcal{P}(A \times B) & \xrightarrow{u} & \mathcal{P}(A)
 \end{array}$$

Comme $[\top_A]$ est un monomorphisme, alors par les propriétés des produits fibrés ([7]), m aussi.

Il reste à trouver la fonction d'évaluation. L'idée est qu'un élément de B^A est (un graphe d')une fonction $f : A \rightarrow B$ et calculer $f(a)$ doit être équivalent à retrouver tous les éléments en relation avec a par la relation induite par f . En d'autres mots, on souhaite que le carré suivant commute :

$$\begin{array}{ccc}
 A \times B^A & \xrightarrow{ev} & B \\
 id_A \times m \downarrow & & \downarrow \{\cdot\}_B \\
 A \times \mathcal{P}(A \times B) & \xrightarrow{v} & \mathcal{P}(B)
 \end{array}$$

Catégoriquement, comme B^A est un produit, on trouve la fonction \hat{g} par le diagramme suivant :

$$\begin{array}{ccccc}
 C & & & & \\
 \curvearrowright & \xrightarrow{\hat{g}} & B^A & \longrightarrow & 1 \\
 & & \downarrow m & & \downarrow [\Gamma_A] \\
 & \xrightarrow{h} & \mathcal{P}(A \times B) & \xrightarrow{u} & \mathcal{P}(A)
 \end{array}$$

Il reste à prouver que ce \hat{g} est unique.
Par définition on a $g = (\hat{g} \times id_A)ev$, et en reprenant la définition de ev on obtient :

$$g\{\cdot\}_B = (\hat{g} \times id_A)ev\{\cdot\}_B = (id_A \times \hat{g}m)v : A \times C \rightarrow \mathcal{P}(B)$$

En transposant cette équation on obtient :

$$(id_A \times g)\delta_B = (id_A \times id_B \times \hat{g}m)ev_{A \times B} : C \times A \times B \rightarrow \Omega.$$

Cette équation montre que $h = \hat{g}m$ est déterminé de manière unique par g . Comme m est un mono, \hat{g} doit être unique. \square

4.3 Le foncteur \mathcal{P}

On a introduit des power-objet, à chaque objet $X \in \mathbb{C}$ est associé $\mathcal{P}(X) \in \mathbb{C}$, mais il est également possible de définir $\mathcal{P}(f)$ tel que \mathcal{P} soit un foncteur sur \mathbb{C} .

Il y a deux manières de faire qui correspondent à la vision $\mathcal{P}(X)$ et Ω^X .

Dans le premier cas, il s'agit d'un foncteur contravariant, noté sous forme covariante $\mathcal{P} : \mathbb{C}^{op} \rightarrow \mathbb{C}$.

Soit $f : A \rightarrow B$, on définit $\mathcal{P}(f)$ comme étant la transposée de la relation classifiée par $(id \times f)ev_B$.

$$\begin{array}{ccccc}
 R & \xrightarrow{\quad} & \mathcal{P}(B) \times A & \xrightarrow{id_{\mathcal{P}(B)} \times f} & \mathcal{P}(B) \times B & \xrightarrow{ev_B} & \Omega \\
 \downarrow & & \downarrow \mathcal{P}(f) \times id_A & & & & \\
 \in_A & \xrightarrow{\quad} & \mathcal{P}(A) \times A & & & &
 \end{array}$$

On peut récrire $\mathcal{P}(f)$ comme étant l'unique morphisme qui fait commuter :

$$\begin{array}{ccc}
 A \times \mathcal{P}(B) & \xrightarrow{f \times id} & B \times \mathcal{P}(B) \\
 \downarrow id \times \mathcal{P}(f) & & \downarrow ev_B \\
 A \times \mathcal{P}(A) & \xrightarrow{ev_A} & \Omega
 \end{array}$$

Dans Ens , cela correspond à la fonction image inverse qui à $f : A \rightarrow B$ associe $f^{-1} : x \subseteq B \mapsto \{y \in A \mid f(y) \in x\}$.

On vérifie ensuite que $\mathcal{P}(id_A) = id_{\mathcal{P}(A)}$ et que $\mathcal{P}(f \circ g) = \mathcal{P}(g) \circ \mathcal{P}(f)$.

$$\begin{array}{ccc}
 A \times \mathcal{P}(A) & \xrightarrow{id \times id} & A \times \mathcal{P}(A) \\
 \downarrow id \times \mathcal{P}(id) & & \downarrow ev_A \\
 A \times \mathcal{P}(A) & \xrightarrow{ev_A} & \Omega
 \end{array}$$

On peut ensuite construire :

$$\begin{array}{ccccc}
 A \times \mathcal{P}(C) & \xrightarrow{f \times id} & B \times \mathcal{P}(C) & \xrightarrow{g \times id} & C \times \mathcal{P}(C) \\
 \downarrow id \times \mathcal{P}(g) & & \downarrow id \times \mathcal{P}(g) & & \downarrow ev_C \\
 A \times \mathcal{P}(B) & \xrightarrow{f \times id} & B \times \mathcal{P}(B) & \xrightarrow{ev_B} & \Omega \\
 \searrow id \times \mathcal{P}(f) & & \nearrow ev_A & & \\
 & & A \times \mathcal{P}(A) & &
 \end{array}$$

Le carré de gauche commute, car chaque flèche n'agit que sur un des membres du produit à la fois, le carré de droite est la définition de $\mathcal{P}(g)$, le triangle du bas est la définition de $\mathcal{P}(f)$ un peu déformé, et la figure extérieure est la définition de $\mathcal{P}(f \circ g)$. Cela définit bien un foncteur contravariant $\mathcal{P} : \mathcal{C}^{op} \rightarrow \mathcal{C}$.

On regarde maintenant le power-objet comme Ω^X et on cherche à définir Ω^f

On remarque que f associe par image directe à chaque sous-ensemble de A , un sous-ensemble de B , c'est-à-dire :

$$\begin{array}{ccccc}
 X & \xrightarrow{x} & A & \xrightarrow{f} & B \\
 & \searrow & & \nearrow & \\
 & & f(X) & &
 \end{array}$$

On définit l'image de f comme suit :

$$\begin{array}{ccccc}
 \in_A & \xrightarrow{\quad} & A \times \mathcal{P}(A) & \xrightarrow{ev_A} & \Omega \\
 \downarrow & & \downarrow f \times id & \nearrow \chi_{Im(\in(id \times f))} & \\
 Im(\in(f \times id)) & \xrightarrow{\quad} & B \times \mathcal{P}(A) & &
 \end{array}$$

On peut construire Ω^f comme l'adjoint de cette fonction caractéristique, c'est-à-dire l'unique morphisme tel que :

$$\begin{array}{ccc}
 \Omega^B \times B & & \\
 \uparrow & \searrow ev_B & \\
 \Omega^f \times id_B & & \Omega \\
 \uparrow & \nearrow \chi_{Im(\in(id \times f))} & \\
 \Omega^A \times B & &
 \end{array}$$

Dans Ens , $\Omega^f : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ est défini par $X \subseteq A \mapsto \{f(x) \mid x \in X\}$.

Il est ensuite un exercice de transposées de démontrer que $\Omega^{id_A} = id_{\Omega^A}$ et que $\Omega^{fg} = \Omega^f \Omega^g$. Ceci crée un foncteur covariant $\Omega : \mathcal{C} \rightarrow \mathcal{C}$.

Conclusion sur les power-objet

On a vu et démontré que la structure de topos était une structure d'ensembles avec une notion interne de sous-ensembles, d'appartenance et d'égalité. Il est donc naturel de penser les objets d'un topos comme étant des ensembles généralisés, et le topos en lui-même comme étant la théorie de ces ensembles.

Cette théorie autorise toujours $\mathcal{P}(x)$ comme ensemble, autorise de séparer le sous-ensemble $\{x \mid \phi\}$ et pour toute fonction, les fonctions image et image inverse sont bien définies.

5 La logique interne

Les ensembles de ZFC et inclusions forment une algèbre de Boole, et donc permettent d'interpréter des formules logiques. Nous allons maintenant montrer qu'il en est de même pour les topos.

5.1 Logique intuitionniste

La première manière de parler de logique interne à un topos, est de motiver l'existence de morphismes correspondant aux connecteurs logiques $\wedge, \vee, \neg, \Rightarrow$. Ceci se fera sur base de l'exemple canonique de la catégorie Ens . Dans Ens , nous avons $\{1, 0\} = \Omega$. De plus nous avons la caractérisation de $\wedge, \vee, \neg, \Rightarrow$ en termes de fonctions caractéristiques, c'est-à-dire reformulé en termes internes au topos. On peut donc définir les termes suivants (tirés de [2, ch6.6-7]) :

- \perp . Dans Ens on a $0_1 : \emptyset \rightarrow \{\cdot\}$ qui n'a aucune image et donc représente le sous-ensemble $\emptyset \in \mathcal{P}(\{\cdot\})$. Sa fonction caractéristique est $\chi_{0_1} : \{\cdot\} \rightarrow \{0, 1\}$ défini par $\chi_{0_1}(\cdot) = 0$. Dans un topos on définit $\perp = \chi_{0_1}$ et on l'interprète comme étant la valeur de vérité "faux" en opposition à \top qui représente la valeur "vrai" ;
- \neg . Comme vu précédemment, la fonction \perp utilise précisément le sous-ensemble de Ω que l'on souhaite caractériser. On pose $\neg = \chi_{\perp}$ et en écrivant la définition, on remarque :

$$\begin{array}{ccc} 1 & \xleftarrow{\perp} & \Omega \\ \downarrow & & \downarrow \neg \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Ce qui signifie que dans un topos quelconque on a $\neg \circ \perp = \top$. On remarque que l'inverse est vrai aussi $\neg \circ \top = \perp$

$$\begin{array}{ccc} 0 & \xrightarrow{!} & 1 \\ \downarrow ! & & \downarrow \top \\ 1 & \xleftarrow{\perp} & \Omega \\ \downarrow & & \downarrow \neg \\ 1 & \xrightarrow{\top} & \Omega \end{array}$$

Il serait tentant de demander que $\neg \circ \neg = id_{\Omega}$ mais cette égalité n'est pas vérifiée en général. Nous reviendrons plus tard sur les conséquences d'avoir cette égalité ;

- \cap . Dans Set \cap est la fonction caractéristique de l'ensemble $\{\{1, 1\}\} \subseteq \Omega \times \Omega$. On définit donc $\cap = \chi_{\langle \top, \top \rangle}$ avec $\langle \top, \top \rangle : 1 \rightarrow \Omega \times \Omega$.
- \cup . Avec une phrase $A \cup B$ on souhaite soit que, ou bien le membre de droite soit vrai, ou bien le membre de gauche. Il paraît donc logique de demander ces conditions sous la forme de ce diagramme :

$$\begin{array}{ccccc} 2 & \longrightarrow & 2 + 2 & \longleftarrow & 2 \\ & \searrow & \downarrow f & \swarrow & \\ \langle \top, id \rangle & & 2 \times 2 & & \langle id, \top \rangle \end{array}$$

Malheureusement le morphisme f n'est pas un mono. Comme on est intéressé par son image, on peut faire la décomposition épi-mono :

$$\begin{array}{ccc} 2 + 2 & \xrightarrow{f} & 2 \times 2 \\ & \searrow e & \nearrow m \\ & & D \end{array}$$

On peut donc définir $\cup = \chi_m$ ou m est l'image de $[\langle \top_\Omega, id_\Omega \rangle, \langle id_\Omega, \top_\Omega \rangle] : \Omega + \Omega \rightarrow \Omega \times \Omega$;

- \Rightarrow . Dans *Ens*, cet opérateur est caractérisé par $\textcircled{\leq} = \{(1, 1), (0, 1), (0, 0)\}$. On avait fait la remarque que cela donnait l'interprétation "au moins aussi vrai que", ce qui justifie de nommer cet ensemble $\textcircled{\leq}$.

En termes interne au topos, on peut le reconstruire de la manière suivante : $Sub(\Omega)$ muni des opération \cup, \cap est un treillis. Tous les treillis respectent :

$$x \leq y \Leftrightarrow x \cap y = x.$$

Ce qui permet de reconstruire $\textcircled{\leq}$ comme l'égalisateur de \cap et la projection sur x .

On définit donc $\Rightarrow = \chi_{\textcircled{\leq}}$ ou $\textcircled{\leq}$ est l'égalisateur de

$$\Omega \times \Omega \xrightarrow[\text{pr}_1]{\cap} \Omega$$

On peut maintenant définir une interprétation dans un topos, de manière similaire aux interprétations dans les algèbres de Boole de de Heyting.

Soit \mathbb{C} un topos, une \mathbb{C} -interprétation est une fonction $V = \Phi_0 \rightarrow \mathbb{C}(1, \Omega)$ qui assigne à chaque variable une valeur de vérité et cette fonction est étendue à Φ par

- $V(\sim \alpha) = \neg \circ V(\alpha)$;
- $V(\alpha \vee \beta) = \cup \circ \langle V(\alpha), V(\beta) \rangle$;
- $V(\alpha \wedge \beta) = \cap \circ \langle V(\alpha), V(\beta) \rangle$;
- $V(\alpha \supset \beta) = \Rightarrow \circ \langle V(\alpha), V(\beta) \rangle$.

Une phrase α est \mathbb{C} -valide si pour toute \mathbb{C} -interprétation, on a $V(\alpha) = \top$.

Les morphismes $\cup, \cap, \neg, \Rightarrow$ sont définis dans $\mathbb{C}(\Omega, \Omega)$. Par composition il est possible de définir des opérateurs $\cup, \cap, \neg, \Rightarrow$ dans $\mathbb{C}(A, \Omega) \simeq Sub(A)$. On demande que pour $s, t \in Sub(A)$ leur union (par exemple) soit le sous-objet caractérisé par $\chi_s \cup \chi_t$. Ces opérateurs fournissent une structure d'algèbre de Heyting. Tout les détails sont parcourus dans [2, ch.7].

En particulier $Sub(1) \simeq \mathbb{C}(1, \Omega)$ est une algèbre de Heyting, ce qui implique que la validité dans un topos se réduit à la validité dans l'algèbre de Heyting $Sub(1)$. En corollaire, on obtient :

- Corollaire 5.1.1.** — *La logique intuitionniste est toujours valide dans un topos;*
- *Si $Sub(1)$ est une algèbre de Boole alors la logique classique est valide dans ce topos.*

On se permet de mentionner la condition suivante.

Sont équivalents :

1. $Sub(\Omega)$ est une algèbre de Boole ;
2. $Sub(A)$ est une algèbre de Boole pour tout objet A ;
3. Dans $Sub(\Omega)$ on a $[f] \Rightarrow [g] = \neg[f] \cup [g]$;
4. Dans $Sub(\Omega)$, $[\top] = \neg[\perp]$;
5. Dans \mathbb{C} , $\neg\neg = id_\Omega$;
6. Dans $Sub(\Omega)$ $[\top]$ a un complément (ce complément sera toujours $[\perp]$) ;
7. Dans $Sub(\Omega)$ on a $[\top] \cup [\perp] = [id_\Omega]$;
8. $[\top, \perp] : 1 + 1 \rightarrow \Omega$ est un iso. ($1 + 1$ est le coproduit de 1 avec lui-même) ;
9. $i_1 : 1 \rightarrow 1 + 1$ est un classificateur de sous-objets ;
10. Le diagramme suivant commute :

$$\begin{array}{ccc}
 \Omega & \xrightarrow{\langle id, \neg \rangle} & \Omega \times \Omega \\
 \downarrow & & \downarrow \cup \\
 1 & \xrightarrow{\top} & \Omega
 \end{array}$$

Un topos qui vérifie cette condition est appelé **Booléen** (par respect de la condition 2) ou **classique** (d'après la condition 8). Un topos Booléen à bien sûr $Sub(1)$ algèbre de Boole, donc sa logique interne est classique.

La démonstration de toute ces équivalences se trouve dans [2, Ch7.3, 7.5, 8.3].

5.2 Logique intuitionniste de premier ordre

On va maintenant rajouter les connecteurs \forall, \exists au topos. Les définitions suivent [2, Ch.11.4], et un traitement plus catégorique est fait en [9, 13.6].

Dans la démonstration sur les power-objets 4.2.3, on avait une propriété $\phi : A \rightarrow \Omega$ "il n'y a qu'un élément de B en relation avec cet élément" et on a vérifié si cette propriété était vraie pour tous les éléments de A . Il est naturel de décrire cela comme la vérification de $\forall a \in A[\phi(a)]$.

On avait demandé que l'ensemble $\{a \mid \phi(a)\} \in \mathcal{P}(A)$ soit exactement A . Cela signifie qu'ils ont la même fonction caractéristique et on peut écrire $\forall_A = \chi_{[\top_A]}$.

$$\begin{array}{ccc}
 1 & \xrightarrow{[\top_A]} & \mathcal{P}(A) \\
 \downarrow & & \downarrow \forall_A \\
 1 & \xrightarrow{\top} & \Omega
 \end{array}$$

Pour l'existence, on va procéder de manière similaire : on souhaite que $C = \{a \mid \phi(a)\}$ ne soit pas vide.

Or on connaît déjà $\in_A = \{(B, x) \mid B \subseteq A, x \in A\}$ donc la projection sur $\mathcal{P}(A)$ nous donne tous les sous-ensembles non vides de A , sa fonction caractéristique est donc une fonction qui est vraie exactement sur les ensembles non vides, c'est la relation \exists_A

$$\begin{array}{ccc}
\in_A & \xrightarrow{\epsilon} & \mathcal{P}(A) \times A \\
\downarrow & & \downarrow \pi_{\mathcal{P}(A)} \\
im(\in \pi_{\mathcal{P}(A)}) & \hookrightarrow & \mathcal{P}(A) \\
\downarrow & & \downarrow \exists_A \\
1 & \xrightarrow{\top} & \Omega
\end{array}$$

Il est possible maintenant de définir une interprétation d'un modèle de théorie intuitionniste de premier ordre. Par souci de facilité, on se concentre sur une théorie avec une seule relation binaire R , distincte de l'égalité, et une seule constante c , afin d'avoir la vision la plus claire possible sans rajouter de complexité calculatoire. L'extension à plusieurs relations et constantes se fait de manière intuitive. Les définitions viennent de [2, Ch11.4].

Soit \mathcal{U} une théorie de premier ordre avec une relation binaire R , l'égalité et une constante c . Un \mathbb{C} -modèle de la théorie est un triple $(A, r, c) = \mathcal{A}$ avec $A \in \mathbb{C}$, $r : A \times A \rightarrow \Omega$ et $c : 1 \rightarrow A$.

Soit une certaine phrase ϕ dépendant $m \in \mathbb{N}$ variables, c'est-à-dire que toutes ses lettres se trouvent dans la liste v_1, \dots, v_m . Il est évident que pour un même ϕ , plusieurs valeurs de m conviennent. On appelle un m qui convient, approprié à ϕ . On peut regarder la réalisation de ϕ dans le modèle, c'est-à-dire

$$\phi^m = \{(x_1, \dots, x_m) \in A^m \mid \mathcal{U} \models \phi(x_1, \dots, x_m)\}.$$

On a pris comme raccourci de notation :

$$A^m := \underbrace{A \times \dots \times A}_m$$

Dans notre topos, pour un terme t , on associe à chaque m approprié, une flèche $\rho^m : A \times \dots \times A \rightarrow A$ selon les règles suivantes :

$$\rho_t^m = \begin{cases} pr_i^m & \text{si } t = v_i \\ !_{A^m} c : A^m \rightarrow 1 \xrightarrow{c} A & \text{si } t = c \end{cases}$$

La phrase $[[\phi]]^m$ est une flèche vers Ω construite selon les règles suivantes :

- $[[t = u]]^m = \delta_A \circ \langle \rho_t^m, \rho_u^m \rangle$;
- $[[tRu]]^m = r \circ \langle \rho_t^m, \rho_u^m \rangle$;
- $[[\phi \wedge \psi]]^m = [[\phi]]^m \cap [[\psi]]^m$;
- $[[\phi \vee \psi]]^m = [[\phi]]^m \cup [[\psi]]^m$;
- $[[\sim \phi]]^m = \neg [[\phi]]^m$;
- $[[\phi \supset \psi]]^m = [[\phi]]^m \Rightarrow [[\psi]]^m$;
- $[[\forall v_i \phi]]^m = \forall_A \circ |\phi|_i^m$;
- $[[\exists v_i \phi]]^m = \exists_A \circ |\phi|_i^m$.

avec $|\phi|_i^m$ le fait de remplacer la i ème composante par une variable libre, formellement c'est l'adjoint de :

$$A \times A^m \xrightarrow{T_i^{M+1}} A^m \xrightarrow{[[\phi]]^m} \Omega$$

$T_i^{M+1} : A \times A^m \rightarrow A^m$ est défini par $\langle \pi_1, \dots, \pi_{i-1}, \pi_{m+1}, \pi_{i+1}, \dots, \pi_m \rangle$. Ceci correspond à transformer la i ème lettre en une variable.

Il est également possible de définir le changement de variables :

$$\delta^m [i/t] \langle \pi_1, \dots, \pi_{i-1}, t, \pi_{i+1}, \dots, \pi_m \rangle$$

qui remplace la i ème variable par le terme $t : A^m \rightarrow A$.

Les termes entre $\llbracket \cdot \rrbracket$ sont définis sur des lettres qui potentiellement n'interviennent pas dans la formule ϕ . On peut donc supprimer ces lettres et avoir un morphisme $\llbracket \phi \rrbracket_U : A^n \rightarrow \Omega$ qui est défini sur les n variables dont ϕ dépend vraiment. Pour cela on définit $f : A^n \rightarrow A^m$ qui transmet les n variables dont ϕ dépend, le reste des variables ne jouent aucun rôle.

Formellement on peut définir pour $\phi(v_{i_1}, \dots, v_{i_n})$ et $g : A^n \rightarrow A$ quelconque, $f = \langle p_1, \dots, p_m \rangle$ avec :

$$p_j = \begin{cases} \pi_{i_k}^n : A^n \rightarrow A & \text{si } j = i_k \text{ pour un certain } k \\ g & \text{sinon} \end{cases}$$

et on définit $\llbracket \phi \rrbracket_U = \llbracket \phi \rrbracket_m \circ f$

$$A^n \xrightarrow{f} A^m \xrightarrow{\llbracket \phi \rrbracket_m} \Omega$$

$\llbracket \phi \rrbracket_U$

Comme ϕ ne dépend pas de variables où g intervient, cette définition ne dépend pas du choix de g . Une démonstration plus en détail de ce fait se trouve dans [2, Ch11.4]. La seule subtilité est le cas $n = 0$, où il faut s'assurer que A n'est pas vide. On peut alors dire que le modèle \mathcal{A} vérifie ϕ , noté $\mathcal{A} \models \phi$, ssi $\llbracket \phi \rrbracket_U = \top_{A^n}$ ssi $\llbracket \phi \rrbracket^m = \top_{A^m}$ pour un m approprié (et donc tous les m appropriés). La notation est légèrement trompeuse, $\llbracket \alpha \rrbracket_U$ dépend non seulement de la théorie \mathcal{U} mais également du choix de modèle dans \mathbb{C} .

La question maintenant est de savoir quelles règles de dérivations s'appliquent dans un topos. En premier lieu, on vérifie que le *modus ponens* s'applique toujours.

Théorème 5.2.1. *Si $\mathcal{A} \models \phi$ et $\mathcal{A} \models \phi \supset \psi$ alors $\mathcal{A} \models \psi$.*

Démonstration. En prenant un m approprié pour ϕ et ψ on a

$$\llbracket \phi \rrbracket^m = \top_{A^m}, \quad \llbracket \phi \rrbracket^m \Rightarrow \llbracket \psi \rrbracket^m = \llbracket \phi \supset \psi \rrbracket^m = \top_{A^m}.$$

En interprétant $\mathbb{C}(A^m, \Omega)$ comme une algèbre de Heyting, alors dans cette algèbre on a \top_{A^m} qui est l'élément maximum 1 et on sait que $1 \Rightarrow \llbracket \psi \rrbracket^m = 1$. On interprète cela comme $\llbracket \psi \rrbracket^m$ est au moins aussi grand que 1, c'est-à-dire $1 \leq \llbracket \psi \rrbracket^m$. Comme 1 est le maximum, on en déduit que $\llbracket \psi \rrbracket^m = 1$ et donc $\llbracket \psi \rrbracket^m = \top_{A^m}$. Comme m est approprié à ψ on en conclut que $\mathcal{A} \models \psi$. \square

Comme $Sub(A^m)$ est une algèbre de Heyting, on sait que les règles de logique intuitionniste sont toujours vérifiées dans un topos. De plus, vérifier :

$$\mathcal{A} \models \phi \supset \psi$$

veut dire par l'exercice précédent que $\llbracket \phi \rrbracket^m$ est au moins aussi grand que $\llbracket \psi \rrbracket^m$ pour un m approprié. La transposition dans $Sub(A^m)$ donne le diagramme commutatif :

$$\begin{array}{ccc} \llbracket \phi \rrbracket^m & \xrightarrow{\{x \mid \phi(x)\}} & A^m \\ \downarrow \text{---} & \nearrow \{x \in A^m \mid \psi(x)\} & \\ \llbracket \psi \rrbracket^m & & \end{array}$$

Par abus de notation, on a noté $\llbracket \phi \rrbracket^m$ pour le domaine canonique du sous-objet classifié par $\llbracket \phi \rrbracket^m : A^m \rightarrow \Omega$.

La vérification des règles intuitionnistes de premier ordre sont laissée en exercice. Les détails se trouvent dans [2, Ch 11.5]. On remarque que le lemme 4.2.4, implique que l'égalité interne dans un topos coïncide avec l'égalité externe.

On peut maintenant définir pour un topos, $\mathbb{C} \models \phi$ si $\mathcal{A} \models \phi$ pour tous les \mathbb{C} -modèles de \mathcal{U} . En particulier la logique intuitionniste de premier ordre est toujours vérifiée dans un topos.

5.3 Théorie des types

Cette méthode s'étend facilement à la théorie des types. Nous suivons principalement la construction de Johnstone dans [5, D1.2.3].

La théorie de Johnstone considère que les termes et variables ont des types, mais que les phrases n'ont pas de type. Lambek et Scott considèrent une théorie dans laquelle les phrases ont un type (Ω) c'est-à-dire que les formules ϕ ont une certaine valeur de vérité. Cette différence fait que Johnstone interprète la théorie en regardant l'extension d'une phrase en contexte $x.\phi$. C'est-à-dire qu'il considère le sous-ensemble du contexte

$$x.\phi = \{(x_1, \dots, x_m) \in x \mid \mathcal{U} \models \phi(x_1, \dots, x_m)\}$$

tandis que Lambek considère la valeur de vérité (dans Ω) de la phrase ϕ . Toutefois, au vu de l'équivalence $Sub(A_1 \times \dots \times A_n) \simeq \mathbb{C}(A_1 \times \dots \times A_n, \Omega)$ les deux reviennent au même. On peut dans un cas définir une interprétation :

$$\llbracket x.\phi \rrbracket \triangleright \longrightarrow A_1 \times \dots \times A_n$$

et dans l'autre cas une interprétation :

$$A_1 \times \dots \times A_n \xrightarrow{\llbracket x.\phi \rrbracket} \Omega$$

Le choix de Johnstone se justifie par le fait qu'il étend l'interprétation à des catégories qui n'ont pas nécessairement un classificateur de sous-objets. Il obtient ainsi des résultats beaucoup plus généraux sur des catégories moins restrictives que les topos. Notamment, il montre qu'une catégorie cartésienne fermée est un modèle d'une théorie λ , qui modèle le concept de fonction, curryfication et composition. Dans notre cas, nous allons ignorer cette plus grande généralité afin de simplifier les définitions.

Il faut faire attention à la manière dont l'équivalence du classificateur de sous-objets est donné. En effet, à partir de $\chi_S \rightarrow \Omega$ il n'existe qu'un seul sous-objet S , mais une infinité de morphismes qui correspondent au sous-objet. Si on travaille dans une métathéorie avec l'axiome du choix, alors on peut fixer un choix de représentant. Sinon il est nécessaire de demander l'existence d'un choix canonique de sous-objets, par exemple dans la définition de topos.

Soit \mathcal{U} une théorie des types intuitionniste et soit \mathbb{C} un topos. On définit M un \mathbb{C} -modèle comme étant le choix de :

- Un objet A_i pour tout les types \mathbf{A}_i ;
- Un morphisme $R : A_1 \times \dots \times A_n \rightarrow \Omega$ pour toute relation \mathbf{R} d'arité n .

Par souci de lisibilité, tout ce qui est dans la théorie est noté en gras tandis que les objets et morphisme du topos sont écrits normalement. On demande de ce choix qu'il respecte les conditions suivantes :

- 1 est l'objet correspondant au type $\mathbf{1}$;
- Ω est l'objet correspondant au type Ω ;
- $A \times B$ est l'objet correspondant au type $\mathbf{A} \times \mathbf{B}$;
- $\mathcal{P}(A)$ est l'objet correspondant au type $\mathcal{P}(\mathbf{A})$.

Dans ce modèle, pour un terme en contexte $\vec{x}.t$, avec t de type \mathbf{B} , on associe une interprétation $\llbracket \vec{x}.t \rrbracket : X = A_1 \times \cdots \times A_n \rightarrow B$. et pour une formule $\vec{x}.\phi$, on associe une valeur de vérité $\llbracket \vec{x}.\phi \rrbracket : X \rightarrow \Omega$, de la manière suivante :

- Si t est une variable x_i du contexte alors $\llbracket \vec{x}.t \rrbracket = \pi_i$ est la projection $\pi_i : X = A_1 \times \cdots \times A_n \rightarrow A_i$;
- Si t est $\mathbf{1}$, de type $\mathbf{1}$ alors $\llbracket \vec{x}.t \rrbracket = !_X : X \rightarrow 1$;
- Si t est c un constante de type \mathbf{B} alors $\llbracket \vec{x}.t \rrbracket = !_X c$;
- Si t est \top alors $\llbracket \vec{x}.t \rrbracket = \top_X$;
- Si t est \perp alors $\llbracket \vec{x}.t \rrbracket = \perp_X$;
- Si t est (r, s) de type $\mathbf{B}_1 \times \mathbf{B}_2$ alors $\llbracket \vec{x}.t \rrbracket = \langle \llbracket \vec{x}.r \rrbracket, \llbracket \vec{x}.s \rrbracket \rangle : X \rightarrow B_1 \times B_2$.
On peut retrouver r et s grâce aux projections canoniques du produit dans \mathbb{C} . Ces projections correspondent aux fonctions fst et sec ;
- Si ϕ est $a \in \theta$, avec $a : \mathbf{B}$, et $\theta : \mathcal{P}(\mathbf{B})$ alors $\llbracket \vec{x}.\phi \rrbracket = (\llbracket \vec{x}.a \rrbracket, \llbracket \vec{x}.\theta \rrbracket) ev_B$;
- Si ϕ est une relation entre des éléments $\mathbf{R}(a_1, a_2, \dots, a_n)$, alors $\llbracket \vec{x}.\phi \rrbracket = (\llbracket \vec{x}.a_1 \rrbracket, \llbracket \vec{x}.a_2 \rrbracket, \dots, \llbracket \vec{x}.a_n \rrbracket) R$;
- Si ϕ est une formule logique, par exemple $a \wedge b, a \vee b, a \supset b, \neg a$ alors $\llbracket \vec{x}.\phi \rrbracket = \llbracket \vec{x}.a \rrbracket \wedge \llbracket \vec{x}.b \rrbracket$ (respectivement \vee, \Rightarrow, \neg). Dans un cadre plus général on peut accepter, si a, b sont de type $\mathbf{A} \neq \Omega$, que $(a \wedge b)$ soit de type \mathbf{A} . Dans ce cas, il s'agit de l'objet correspondant dans l'algèbre des sous-objets, c'est-à-dire $\llbracket \vec{x}.t \rrbracket$ est le sous-objet caractérisé par $\chi_{\llbracket \vec{x}.a \rrbracket} \wedge \chi_{\llbracket \vec{x}.b \rrbracket}$, ou de manière équivalente, le sous-objet décrit par $\{x \in A \mid a \wedge b\}$;
- Si $\mathbf{B} = \mathcal{P}(\mathbf{C})$ et $t = \{z : \mathbf{C} \mid \phi\}$ en supposant que z n'est pas une variable du contexte, alors $\llbracket \vec{x}.t \rrbracket$ est le nom de la relation classifiée par $\llbracket \vec{x}, z.\phi \rrbracket$, au sens de la définition 4.2.1. On attire l'attention sur le fait que $\{x \in A \mid \phi\}$ est un sous-objet de A , c'est-à-dire une flèche vers A , tandis que $\llbracket x.\{x : A \mid \phi\} \rrbracket$ est un élément de $\mathcal{P}(A)$;
- Si $\phi = \exists_{y:\mathbf{B}} \phi$ alors $\llbracket \vec{x}.\phi \rrbracket = \exists_B \circ \llbracket \llbracket \vec{x}, y.\phi \rrbracket \rrbracket$. Cette définition plus concise est exactement la même construction que dans le cas de premier ordre ;
- Si $\phi = \forall_{y:\mathbf{B}} \phi$ alors $\llbracket \vec{x}.\phi \rrbracket = \forall_B \circ \llbracket \llbracket \vec{x}, y.\phi \rrbracket \rrbracket$;
- *Formule de changement de variables* : Si y est un contexte acceptable pour $t : \mathbf{C}$ et soit s_i du même type que y_i , avec x un contexte approprié aux s_i . Alors $\llbracket \vec{x}.t(s/y) \rrbracket$ est la composée :

$$A_1 \times \cdots \times A_n \xrightarrow{(\llbracket \vec{x}.s_1 \rrbracket \dots \llbracket \vec{x}.s_m \rrbracket)} B_1 \times \cdots \times B_m \xrightarrow{\llbracket y.t \rrbracket} C$$

À nouveau, le seul contexte qui va être important est le contexte canonique, contenant seulement les variables dont dépend ϕ .

Nous sommes désormais en mesure d'interpréter un modèle M dans \mathbb{C} . On dit M satisfait $\phi \vdash_x \psi$ si $\llbracket \vec{x}.\phi \rrbracket \leq \llbracket \vec{x}.\psi \rrbracket$ dans l'algèbre $\mathbb{C}(X, \Omega) \simeq Sub(A_1 \times \cdots \times A_n)$. On dit M est un modèle d'une théorie \mathcal{U} si tous les séquents de \mathcal{U} sont satisfaits par M .

Théorème 5.3.1. *Dans un topos, les axiomes de la théorie des types intuitionniste sont vérifiés.*

Démonstration. Il suffit de développer le tout. Par l'équivalence entre séquent et phrases mentionné en 1.3.4, on a déjà montré que les axiomes logiques et du premier ordre sont vérifiés. Il ne reste plus qu'à vérifier les axiomes supplémentaires.

Montrons l'extensionnalité : $\top \vdash_w \{x : A \mid x \in w\} = w$. Les autres séquents se font de la même manière.

Ce séquent signifie que dans le contexte $w \in \mathcal{P}(A)$, on a

$$\llbracket w.\top \rrbracket \leq \llbracket w.\{x : A \mid x \in w\} = w \rrbracket$$

en temps qu'éléments de l'algèbre $\mathbb{C}(\mathcal{P}(A), \Omega)$.

$\llbracket w.\top \rrbracket = \top_{\mathcal{P}(A)}$ est l'élément maximum de cette algèbre, l'inégalité est donc une égalité et le séquent est vérifié ssi

$$\top = \llbracket \{x : A \mid x \in w\} = w \rrbracket = \delta \circ (\llbracket w.w \rrbracket, \llbracket w.\{x : A \mid x \in w\} \rrbracket).$$

Par la propriété 4.2.4, cette égalité est vraie ssi $\llbracket w.w \rrbracket = \llbracket w.\{x : A \mid x \in w\} \rrbracket$ en tant que morphisme du topos.

D'un coté $\llbracket w.w \rrbracket = \pi_1 : \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ est le morphisme d'identité.

De l'autre coté $\llbracket w.\{x : A \mid x \in w\} \rrbracket$ est le nom de la relation classifié par :

$$\llbracket w, x.x \in w \rrbracket = (\llbracket w, x.x \rrbracket, \llbracket w, x.w \rrbracket)ev_A$$

Comme $\llbracket w, x.x \rrbracket, \llbracket w, x.w \rrbracket$ sont tout les deux des morphismes d'identité, cela donne :

$$\mathcal{P}(A) \times A \xrightarrow{id \times id} \mathcal{P}(A) \times A \xrightarrow{ev_a} \Omega$$

Donc $\llbracket w, x.x \in w \rrbracket = ev_a : \mathcal{P}(A) \times A \rightarrow \Omega$. On note $\llbracket \vec{x}.t \rrbracket$ pour $\llbracket w.\{x : A \mid x \in w\} \rrbracket$ et on construit le diagramme de power-objet pour trouver l'adjoint.

$$\begin{array}{ccc} \in_A & \xrightarrow{\quad} & \mathcal{P}(A) \times A \xrightarrow{ev} \Omega \\ \downarrow & & \downarrow \llbracket \vec{x}.t \rrbracket \times id_A \quad \uparrow \\ \in_A & \xrightarrow{\quad} & \mathcal{P}(A) \times A \xrightarrow{ev_a} \Omega \end{array}$$

On en déduit $\llbracket \vec{x}.t \rrbracket = id_{\mathcal{P}(A)}$. Le séquent d'extensionnalité est donc vérifié. \square

Théorème 5.3.2. *Si ϕ est vérifié par la théorie intuitionniste des types, alors $\mathbb{C} \models \phi$ pour tout topos \mathbb{C} .*

La preuve vient d'être faite, par la vérification des axiomes et règles de dérivations.

En fait ce théorème s'étend à toute théorie qui a au moins les axiomes de la théorie des types et au plus les règles de déduction de la théorie intuitionniste. Si une théorie possède plus d'axiomes, rien ne garantit qu'il existe un modèle dans un topos, mais si un modèle existe, il vérifie les axiomes supplémentaires (par définition) et les règles de dérivations.

En particulier, il existe une théorie adaptée à un topos \mathbb{C} , la théorie qui contient comme types tous les objets de \mathbb{C} , comme constantes, ou termes tous les morphismes $c : 1 \rightarrow X$, comme relations, ou phrases, toutes les relations $r : A \times B \rightarrow$

Ω , etc. Les axiomes sont tous les séquents tel que $\mathbb{C} \models \phi \Leftrightarrow \llbracket \phi \rrbracket = \top$, les règles de dérivation sont celles mentionnées plus haut. Cette théorie est appelée **le langage interne** de \mathbb{C} , noté $\mathcal{T}(\mathbb{C})$. Le topos \mathbb{C} peut être vu comme un modèle particulier de cette théorie logique.

5.4 Quelques résultats notables

On mentionne maintenant, sans démonstration, quelques résultats de la logique interne. En premier lieu, les équivalences entre les termes $=, \wedge, \vee, \neg, \supset, \forall, \exists$, sont valides dans un topos.

Ensuite, la logique interne est une théorie des ensembles à plusieurs types. En effet les objets sont des ensembles au sens que le langage interne d'un topos valide toujours :

- *Extensionnalité* : $\mathbb{C} \models \forall_{Y, Z: \mathcal{P}(A)} [Y = Z \equiv \forall_{x:A} (x \in Y \equiv x \in Z)]$;
- *Ensemble vide* : $\mathbb{C} \perp_A = \{x : A \mid \perp\}$;
- *Singleton* : $\mathbb{C} \models x \in \{y\} \equiv x = y$ pour le singleton défini en 4.2.3;
- *Union binaire* : $\mathbb{C} \models x \in Y \cup Z \equiv (x \in Y \wedge x \in Z)$ pour $\cup : \mathcal{P}(A) \times \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ l'union interne;
- *Union arbitraire* : $\mathbb{C} \models x \in \bigcup Z \equiv \exists_{y:\mathcal{P}(A)} (y \in Z \wedge x \in Y)$ pour $\bigcup \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ l'union externe;
- *Powerset* : $\mathbb{C} \models Y \in [\mathcal{P}] Z \equiv Y \subseteq_A Z$ avec $Y, Z : \mathcal{P}(A)$,
 $\subseteq_A = \{(Y, Z) \mid \forall_{x:A} x \in Y \supset x \in Z\}$
et $[\mathcal{P}] = \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ le powerset interne (adjoint de \subseteq_A);
- *Séparation* : "il existe une unique fonction f_ϕ tel que $\mathbb{C} \models y \in f_\phi \equiv \phi$.

Les dérivations logiques proviennent de [10].

Soit $f : A \rightarrow B$ est un morphisme de \mathbb{C} et t est un terme de type A . En contexte, $\llbracket \vec{x}.t \rrbracket$ est un morphisme $t : X \rightarrow A$. En prenant le point de vue d'éléments généralisé, il convient d'appeler $f(t)$ le terme $f(t) : X \rightarrow B$ obtenu par composition. En réalité cette notation a un pendant théorique, qui touche à l'équivalence entre λ -théorie et catégorie cartésienne fermée, mais les détails sont laissés pour un autre mémoire. Avec cette notation, le langage interne a les propriétés suivantes :

- $f = g$ en temps que morphisme ssi $\mathbb{C} \models \forall_x f(x) = g(x)$;
- Si $\mathbb{C} \models \forall_{x:A} \exists!_{y:B} \phi(x, y)$ alors il existe dans \mathbb{C} une flèche $g : A \rightarrow B$ tel que $\mathbb{C} \models \forall_{x:A} \phi(x, g(x))$;
- f est un mono ssi $\mathbb{C} \models \forall_{x:A} \forall_{x':A} (f(x) = f(x')) \supset (x = x')$;
- f est un épi si $\mathbb{C} \models \forall_{y:B} \exists_{x:A} f(x) = y$;
- f est un iso si $\mathbb{C} \models \forall_{y:B} \exists!_{x:A} f(x) = y$;
- Si $\mathbb{C} \models \forall_{x:A} \forall_{y:B} \forall_{y':B} xRy \wedge xRy' \supset (y = y')$ et $\mathbb{C} \models \forall_{x:A} \exists_{y:B} xRy$, alors il existe un morphisme $f : A \rightarrow B$ tel que $\mathbb{C} \models \forall_{x:A} \forall y : By = f(x) \equiv xRy$.

Théorèmes tirés de [6, II.5-6] et [9, 16].

6 Compléter l'équivalence

On a déjà vu que les topos *ont* une logique interne et *sont* une structure d'ensembles. On va maintenant montrer que les topos *ont* des ensembles internes et *sont équivalent* à une structure de théorie.

En particulier, il existe une équivalence de catégories entre certaines théories des ensembles et les topos booléens et une autre équivalence entre les théories des types intuitionnistes et les topos.

Johnstone ([5]) montre ces équivalences en définissant une catégorie des théories logiques, mais cela nécessite de se mettre dans une métathéorie catégorique. Il m'a semblé plus juste de montrer les injections dans les deux sens, mais de ne pas introduire de catégorie des théories logiques pour rester fidèle au point de vue Logiciste.

Les livres de Lambek et Scott ([6]), et Goldblatt ([2]) sont aussi deux très bons ouvrages pour comprendre l'équivalence en termes logique et des ensembles respectivement.

6.1 Équivalence topos-ensemble

Un topos bien pointé (défini en 3.3) est équivalent à un modèle de la théorie des ensembles Z , dans le sens qu'un modèle donne lieu à un topos, et un topos donne lieu à un modèle de Z . Ces deux constructions sont presque l'inverse l'une de l'autre dans un sens qui sera précisé plus tard. La démonstration entière ne rentre pas dans ce mémoire mais nous allons introduire les outils nécessaires. Cette section suit [2, Ch12].

Il est possible de construire d'autres équivalences entre théorie des ensembles et topos, comme dans [1], mais celle-ci est la plus courante dans la littérature.

6.1.1 La théorie des ensembles engendre un topos

Soit \mathcal{U} une théorie des ensembles ayant au moins les axiomes de Z_0 . Alors la construction de Ens_{Z_0} se fait comme dans le cas ZFC, et Ens_{Z_0} est un topos bien pointé.

Les objets de Ens_{Z_0} sont les ensembles de \mathcal{U} . Les fonctions sont les triples (a, f, b) qui respectent la formule :

$$\mathbf{Fonct}(f) \wedge (\mathbf{Dom}(f) = a) \wedge \mathbf{Im}(f) \subseteq b.$$

L'identité est donné par $(a, \Delta(a), a)$ avec $\Delta(a) \equiv \{(v, v) : v \in a\}$.

La composition est définie de manière usuelle $f \circ g$.

Le produit $A \times B$ correspond à l'ensemble $\{(u, v) : u \in A \wedge v \in B\}$.

Le power-objet est donné par $\mathcal{P}(A) = \{u : u \subseteq A\}$.

Tous ces ensembles existent et sont bien définis par les axiomes de Z_0 .

6.1.2 Un topos engendre une théorie des ensembles

En catégories, il arrive souvent que les objets manipulés soient déjà des ensembles avec une certaine structure, au sens Bourbakiste. Dans ce cas, il est naturel de demander s'il existe un objet $C \in \mathbb{C}$ possédant une structure en plus, comme par exemple respecter les axiomes de groupes et déclarer que cet objet C est un objet-groupe.

L'idée va être de faire la même chose avec des objet-ensembles et de montrer que dans un topos, la collection d'objet-ensembles respecte les axiomes de la théorie des ensembles. Cela permettrait de dire que le topos contient un modèle de la théorie des ensembles.

Commençons par définir un objet- \mathbb{N} , qui respecterait les axiomes de Peano.

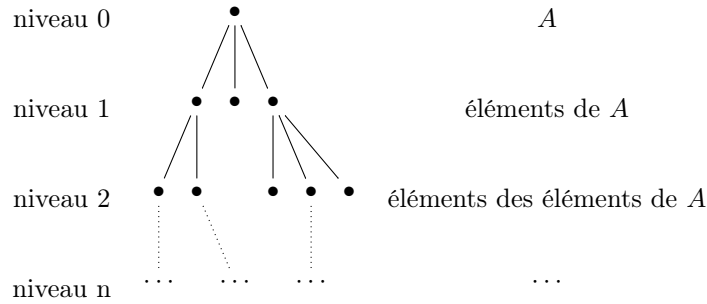
Définition 6.1.3. Soit \mathbb{C} une catégorie, un **Objet de nombres naturels** (ONN) est un objet $n \in \mathbb{C}$ muni de deux morphisme $0 : 1 \rightarrow n$ et $s : n \rightarrow n$ tel que pour tout autre candidat (A, q, f) , il existe un unique u qui fait commuter le diagramme suivant :

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & n & \xrightarrow{s} & n \\ & \searrow q & \downarrow u & \searrow f & \downarrow u \\ & & a & \xrightarrow{f} & a \end{array}$$

Par définition cet objet est unique à isomorphisme près. Dans Ens , $(\mathbb{N}, 0, f)$, où $f(n) = n+1$ est un ONN. Pour un topos, avoir un ONN signifie que sa théorie des ensembles vérifie l'axiome de l'infini.

L'objectif maintenant est de créer des objet-ensembles et définir des notions d'appartenance et d'égalité, ce qui nous donne un modèle de la théorie des ensembles supporté par \mathbb{C} . On regarde ensuite la théorie qui est valide pour tous les objet-ensembles.

Pour cela on doit d'abord parler de la notion d'ensemble transitif, notion qui existe car l'appartenance dans Z_0 est globale. Dans Z_0 , les éléments d'un ensemble, sont eux aussi des ensembles, qui se distinguent par leurs éléments, eux aussi des ensembles, ... on peut donc faire un arbre comme suit :



C'est le diagramme d'appartenance à l'ensemble A . Si on enlève le point du haut, le reste de l'arbre T_A , vu comme ensemble de points a une propriété appelé transitivité. La transitivité est la propriété $x \in T_A \Rightarrow x \subseteq T_A$, c'est-à-dire que si x est un élément de T_A , tout les éléments de x sont aussi des éléments de T_A . De manière équivalente on peut écrire $x \in T_A \Rightarrow x \in \mathcal{P}(T_A)$.

La théorie ZFC a des axiomes suffisamment forts pour avoir des ensembles transitifs, malheureusement ce n'est pas le cas de Z_0 , et il est nécessaire de demander un axiome en plus.

Axiome de transitivité (*trans*)

$$\forall t \exists u (t \subseteq u \wedge \mathbf{TR}(u))$$

avec $\mathbf{TR}(u)$ la formule $\forall v (v \in u \supset v \subseteq u)$, qui exprime la transitivité de u .

Avec cet axiome il est possible de déduire dans $Z_0 + TR$

$$\forall t \exists ! u [t \subseteq u \wedge \mathbf{TR}(u) \wedge \forall v (t \subseteq v \wedge \mathbf{TR}(v) \supset u \subseteq v)]$$

qui exprime que pour tout ensemble t l'unique $u = T_t$ existe bel et bien.

Si A' est un autre ensemble transitif qui contient A , alors on en déduit que $T_A \subseteq A'$, donc on peut décrire T_A comme le plus petit ensemble transitif contenant A . La preuve se fait avec une certaine induction, qui indique que cet axiome joue un rôle important dans le processus d'induction.

La raison de s'intéresser aux ensembles transitifs, c'est qu'ils ont une relation d'inclusion interne, appelons la $\epsilon : T_A \times T_A \rightarrow \Omega$ pour ne pas la confondre. Par transposition on obtient $E \subseteq T_A \times T_A$ et $r_E : T_A \rightarrow \mathcal{P}(T_A)$, qui est défini par $r_E(x) = \{y \mid y \in T_A \wedge yEx\}$ mais comme T_A est transitif et E est la relation d'inclusion, on peut réduire

$$r_E(x) = \{y \mid y \in T_A \wedge y \in x\} = \{y \mid y \in x\} = x$$

$$\begin{array}{ccc} & 1 & \\ s \swarrow & & \searrow [s] \\ T_A & \xrightarrow{r_E} & \mathcal{P}(T_A) \end{array}$$

On a déjà donné un sens à $a \in b$ si $a \in A, b \in \mathcal{P}(A)$, mais la question resterait de savoir pour $a, b \subseteq A$ si $a \in b$, comme cela pourrait être le cas avec un ensemble transitif.

Travaillons dans *Ens*

Soit A un ensemble transitif et $f : B \rightarrow A, g : C \rightarrow A$ deux sous-ensembles de A . Si jamais on a $C \in B$ alors il doit exister un élément global $1 \rightarrow B$ qui corresponde à C , et $\hat{g} : 1 \rightarrow A$ qui corresponde à l'inclusion $C \in B \subseteq A$. En diagramme cela donne :

$$\begin{array}{ccc} & 1 & \\ \swarrow & & \searrow \hat{g} \\ B & \xrightarrow{f} & A \end{array}$$

Dans l'autre sens, si on a un élément global $\hat{g} : 1 \rightarrow A$, la question de savoir si $\hat{g} \in B$ est équivalente à savoir si le morphisme \hat{g} se factorise à travers le morphisme f .

Dans *Ens*, pour $C \subseteq A$ via le morphisme g , la transposée de g est $[g] = [\chi_C] : 1 \rightarrow \mathcal{P}(A)$. Si en plus A est transitif, on a l'inclusion $r_E : A \rightarrow \mathcal{P}(A)$, et on déduit que $C \in A$ ssi il existe \hat{g} qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} & 1 & \\ \hat{g} \swarrow & & \searrow [g] \\ A & \xrightarrow{r_E} & \mathcal{P}(A) \end{array}$$

La théorie des ensembles locale, sur les sous-ensembles de A est donc la suivante : pour $f : B \rightarrow A, g : C \rightarrow A$ deux sous-ensembles de A , on a $g \in f$ ssi $C \in B$ ssi $[g]$ se factorise a travers $r_E \circ f$.

$$\begin{array}{ccc}
& 1 & \\
\swarrow & & \searrow [g] \\
B & \xrightarrow{f} & A \xrightarrow{r_E} \mathcal{P}(A)
\end{array}$$

Il reste maintenant à passer de théorie des ensembles locale, à la théorie globale. Dans *Ens* savoir si $f : B \rightarrow A$, $g : C \rightarrow A$ représentent le même ensemble peut se vérifier avec la fonction caractéristique, mais il reste encore un cas. Pour $f : B \rightarrow A$, $g : C \rightarrow D$, on peut avoir $f(B) = g(C) \subseteq A \cap D$.

Dans ce cas on a également $f(B) = g(C) \subseteq A \cup D$, et donc pour tout T qui inclu A et D on a $i : A \rightarrow T$ et $j : D \rightarrow T$ et $f(B) = g(C)$ ssi $i(f(b)) = j(g(C))$. On ne peut pas demander n'importe quel T , mais il est suffisant de demander que T soit transitif.

On définit $g \in f$ si il existe un T transitif tel que $A, D \subseteq T$ et $g \in f$ dans la théorie locale de T . C'est-à-dire que :

$$\begin{array}{ccc}
& C & \\
\swarrow & & \searrow [j \circ g] \\
B & \xrightarrow{i \circ f} & T \xrightarrow{r_E} \mathcal{P}(T)
\end{array}$$

Nous allons faire un exercice pour clarifier les concepts :

Théorème. Dans *Ens*, $A \in B$ si et seulement si $id_A \in id_B$

Démonstration. Dans un sens, on prend $T = T_B$ la fermeture transitive de B , c'est-à-dire l'ensemble formé par l'arbre d'appartenance. On a alors les fonctions d'inclusions évidentes et :

$$\begin{array}{ccc}
& A & \\
\swarrow A \in B & & \searrow [j \circ id_A] \\
B & \xrightarrow{i \circ id_B} & T \xrightarrow{r_E} \mathcal{P}(T)
\end{array}$$

Par définition des objets, l'image de $i \circ id_B$ n'est autre que l'ensemble B , et $r_E(x) = x$ par la théorie des ensembles locale. $r_E \circ i$ est donc une fonction qui, à chaque $b \in B$, assigne le même élément vu comme élément de $\mathcal{P}(T)$ Par ailleurs $[j \circ id_A] = \{a \mid a \in A\} = A$. Comme $A \in B$, on a bien la flèche $A \in B$ qui fait commuter le diagramme.

Dans l'autre sens :

$$\begin{array}{ccc}
& A & \\
\swarrow & & \searrow [j \circ id] \\
B & \xrightarrow{i \circ id} & T \xrightarrow{r_E} \mathcal{P}(T)
\end{array}$$

□

La question maintenant est de savoir comment caractériser $r_E : A \rightarrow \mathcal{P}(A)$ pour pouvoir généraliser à un topos.

On annonce ici le "lemme de Mostowski", sans démonstration.

Lemme. Soit $R \subseteq A \times A$, une relation sur A . Les deux conditions suivantes sont équivalentes :

- Il existe un ensemble B transitif tel que $\langle A, R \rangle \simeq \langle B, r_E \rangle$;
- R est une relation extentionnelle et noetherienne.

Il est possible de démontrer ce lemme dans ZFC , et même dans ZF , mais la théorie Z_0 n'est pas assez forte pour démontrer ce résultat. En particulier le lemme de Mostowski implique que la relation (B, r_E) est une relation bien fondée, ce qui demande l'axiome *Reg* pour être démontrable. Par la suite, on demandera que ce théorème soit vrai, ce qui peut se faire en demandant que cet énoncé soit un axiome de notre théorie. On appellera cet axiome *Mostowski*.

Que R soit extentionnelle, s'exprime dans le topos par le fait que R soit un mono. La condition d'être noetherien signifie que tout sous-ensemble non vide $C \subseteq A$, a un un élément minimal au sens de R , c'est-à-dire un $x \in C$ tel que $\forall y \in C, \neg yRx$.

On peut énoncer un autre théorème sans démonstration, théorème qui est prouvable dans Z_0 .

Théorème. Soit R une relation sur A . R est Noetherien si et seulement si pour toute fonction $g : \mathcal{P}(B) \rightarrow B$, il existe une unique fonction $f : A \rightarrow B$ telle que

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow r_R & & \uparrow g \\ \mathcal{P}(A) & \xrightarrow{\mathcal{P}(f)} & \mathcal{P}(B) \end{array}$$

On a donc une caractérisation, à isomorphisme près, des ensembles transitifs et des relations r_E .

Définition 6.1.4. Dans un topos, un **objet ensemble transitif** (oet) est une flèche $r : A \rightarrow \mathcal{P}(A)$ qui est

- Un mono;
- **Réursive**, c'est-à-dire pour tout $g : \mathcal{P}(B) \rightarrow B$, il existe un unique morphisme $f : A \rightarrow B$ tel que

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow r & & \uparrow g \\ \mathcal{P}(A) & \xrightarrow{\mathcal{P}(f)} & \mathcal{P}(B) \end{array}$$

La deuxième propriété est appelé réursive car elle permet de définir f dans des condition similaires à l'induction transfinitie.

Définition 6.1.5. Un **objet-ensemble** est une paire de morphismes (f, r) de la forme $B \rightarrow A \rightarrow \mathcal{P}(A)$, avec r un objet ensemble transitif

Deux objet-ensembles sont dit égaux $(f, r) \simeq_{\mathcal{C}} (g, s)$ s'il existe un oet t :

$E \rightarrow \mathcal{P}(E)$ tel que $r \subseteq t$ et $s \subseteq t$

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 & & \searrow i \\
 & & E \\
 & & \nearrow j \\
 C & \xrightarrow{g} & D
 \end{array}$$

et on a $i \circ f = j \circ g$ dans $Sub(E)$, c'est-à-dire $\chi_{i \circ f} = \chi_{j \circ g}$

Un objet-ensemble est inclus dans un autre, noté $(g, s) \in_{\mathbb{C}} (f, r)$ si il existe un objet $t : E \rightarrow \mathcal{P}(E)$ tel que $r \subseteq t$, $s \subseteq t$ et $j \circ g \in_t i \circ f$, i.e.

$$\begin{array}{ccc}
 & 1 & \\
 & \swarrow & \searrow [j \circ g] \\
 B & \xrightarrow{i \circ f} & E \xrightarrow{t} \mathcal{P}(E)
 \end{array}$$

Cette définition ne dépend pas du choix de t .

On vient de construire un modèle de la théorie des ensembles.

Théorème 6.1.6. *Si \mathbb{C} est un topos bien pointé, alors $\mathcal{U}(\mathbb{C})$ est un modèle de la théorie $Z_0 + Reg + trans$. De plus si \mathbb{C} a un NNO, alors la théorie respecte l'axiome de l'infini, et enfin si dans \mathbb{C} tout les épis sont scindés, alors l'axiome du choix est respecté dans $\mathcal{U}(\mathbb{C})$.*

La démonstration se fait en vérifiant que les axiomes de la théorie et que les règles de dérivations sont vérifiées. La preuve sera omise.

6.1.7 Les deux constructions sont inverses

On a vu une construction Ens qui assigne à chaque modèle de Z_0 un topos Ens_{Z_0} et une construction \mathcal{U} qui assigne à chaque topos \mathbb{C} un modèle de $Z_0 + reg + trans$. La question est de savoir dans quelle mesure ces constructions sont l'inverse l'une de l'autre.

Certains axiomes sont des traductions directes, ainsi l'axiome de l'infini se traduit par l'existence d'un ONN, et inversement. De même l'axiome du choix (toute collection d'ensemble non vide admet un choix) correspond à l'axiome du choix catégorique (les épis ont un inverse à droite).

Toutefois, tous les ensembles des modèles de Z_0 n'ont pas toujours de fermeture transitive. De l'autre côté, tous les objets d'un topos ne sont pas équivalents à un ensemble selon notre construction. Pour contrer ces difficultés nous allons demander aux topos et aux modèles les conditions manquantes.

On définit $B \in \mathbb{C}$ est **partiellement transitif** si il existe $r : A \rightarrow \mathcal{P}(A)$ objet et $f : B \rightarrow A$, ce qui fait que (f, r) est un objet-ensemble. Le topos \mathbb{C} est partiellement transitif si tout objet est partiellement transitif.

On définit $Z = Z_0 + reg + trans + Mostowski$, la théorie des ensembles avec les axiomes de Z_0 , l'axiome de régularité, transitivité et le lemme de Mostowski en axiome.

On annonce le théorème suivant :

Théorème 6.1.8. Soit \mathbb{C}_0 un topos bien pointé et partiellement transitif, et \mathcal{V} un modèle de Z , on a :

1. $\mathcal{U}(Ens_{\mathcal{V}})$ est isomorphe à \mathcal{V} ;
2. $Ens_{\mathcal{U}(\mathbb{C}_0)}$ est équivalent à \mathbb{C}_0 au sens des catégories.

Esquisse de preuve. 1) Soit \mathcal{V} un modèle de Z . Soit b un ensemble de \mathcal{V} , c'est-à-dire $b \in Ens_{\mathcal{V}}$. Par l'axiome *trans*, il existe a , ensemble de \mathcal{V} qui est la fermeture transitive de b et une fonction d'inclusion $f : b \hookrightarrow a$. À nouveau, on peut voir ces objets comme appartenant à $Ens_{\mathcal{V}}$.

Avec les axiomes d'extensionnalité et de régularité, on déduit $r_a : a \rightarrow \mathcal{P}(a)$ une fonction injective et noetherienne donc un morphisme récursif.

En regardant tous ces objet dans $Ens_{\mathcal{V}}$, on a (f, r_a) qui est un objet ensemble et on peut vérifier les relations suivantes :

- $a = b$ ssi $(f, r_a) \simeq_{Ens_{\mathcal{V}}} (f', r_c)$;
- $a \in_{\mathcal{V}} b$ ssi $(f, r_a) \in_{Ens_{\mathcal{V}}} (f', r_c)$.

Dans l'autre sens si X est un ensemble de $\mathcal{U}(Ens_{\mathcal{V}})$, on a $X = (f, r)$ un objet-ensemble de $Ens_{\mathcal{V}}$. r est mono et récursive dans $Ens_{\mathcal{V}}$, donc une relation extensionnelle et noetherienne de \mathcal{V} . Comme \mathcal{V} vérifie *Mostowski*, il existe un ensemble c du modèle \mathcal{V} et une bijection $g : a \rightarrow c$ tel que r est isomorphe à la relation d'appartenance sur c . On note $St(X) = g(f(a))$ l'image de a dans c . Comme les représentations transitives sont uniques dans \mathcal{V} , cela nous donne une fonction unique $St : \mathcal{U}(Ens_{\mathcal{V}}) \rightarrow \mathcal{V}$ qui satisfait :

- $X \simeq_{Ens_{\mathcal{V}}} Y$ ssi $St(X) =_{\mathcal{V}} St(Y)$;
- $X \in_{Ens_{\mathcal{V}}} Y$ ssi $St(X) \in_{\mathcal{V}} St(Y)$.

2) Soit \mathbb{C}_0 un topos bien pointé, partiellement transitif. On construit un foncteur $F : Ens_{\mathcal{U}(\mathbb{C}_0)} \rightarrow \mathbb{C}_0$.

Si $X \in Ens_{\mathcal{U}(\mathbb{C}_0)}$ alors c'est un ensemble du modèle $\mathcal{U}(\mathbb{C}_0)$, c'est-à-dire un objet-ensemble $(f, r) \in \mathbb{C}_0$. On pose $F(X) = dom(f)$. Il est possible de définir ce foncteur sur les morphismes. Ce foncteur peut être défini pour tout topos bien pointé \mathbb{C} , mais son image est la sous-catégorie pleine des objets transtifs de \mathbb{C} . En demandant au topos d'être partiellement transitif, on garantit que ce foncteur est surjectif et donc une équivalence de catégories. De plus cette condition a un impact sur le modèle $\mathcal{U}(\mathbb{C}_0)$, à savoir que le lemme de Mostowski est vérifié et donc ce $Z_0 + reg + trans$ -modèle est en fait un Z -modèle. \square

Mentionnons que l'axiome du choix dans un topos implique que tous les objets sont partiellement transitifs. La preuve prend le bon ordre sur un ensemble (qui existe par l'axiome du choix) et cela devient un objet $A \rightarrow \mathcal{P}(A)$. En particulier l'équivalence peut se restreindre entre $Z + Choix$ et les topos avec l'axiome du choix.

6.2 Équivalence topos-logique

Un topos est équivalent à une théorie des types intuitionniste. Nous allons d'abord construire un topos à partir d'une théorie des types, et puis montrer que les deux sont équivalents dans un sens qui sera précisé ensuite. La preuve est tirée de [6, II.13].

On montre tout d'abord qu'une théorie des types telle que définie au début (1.3) admet un modèle particulier qui sera un topos. L'idée est similaire à celle de Lindenbaum en 2.4, prendre la structure logique en elle-même et la transformer

en un topos. La même remarque sur le cadre Logiciste s'applique, la construction fonctionne en dehors du cadre de la logique formelle mais peut rencontrer des problèmes ontologiques.

6.2.1 Une théorie des types engendre un topos

Soit \mathcal{T} une théorie des types. Remarquons tout d'abord que par l'équivalence de 1.3.4, considérer toutes les formules est équivalent à considérer tous les séquents. Si $\alpha \vdash_{\bar{x}} \beta$ est un séquent, $\forall_{\bar{x}} \alpha \supset \beta$ est une formule de type \mathbf{X} , et son extension $\{x \in X \mid \alpha(x) \supset \beta(x)\}$ est un terme de $\mathcal{P}(\mathbf{X})$. Notons que les termes $a : \mathbf{A}$ peuvent similairement être interprétés comme $\{x \mid x \in a\} : \mathbf{X}$.

A nouveau par lisibilité, les types de la théorie sont en gras, tandis que les objets des topos sont notés en italique. Un objet/type qui a été transformé deux fois sera noté en gras et italique.

Construisons la catégorie $\mathbb{C}(\mathcal{T})$.

On pose pour objets les termes de type $\mathcal{P}(\mathbf{A})$ et fermé par l'égalité, c'est-à-dire si $\mathcal{T} \vdash a = a'$ et $a, a' \in \mathcal{P}(\mathbf{A})$ alors ces objets sont égaux.

Si A est un terme de $\mathcal{P}(\mathbf{A})$ et B un terme de $\mathcal{P}(\mathbf{B})$, on définit un morphisme $f : A \rightarrow B$ comme étant $|f|$ un terme de $\mathcal{P}(\mathbf{A} \times \mathbf{B})$ qui vérifie $\mathcal{T} \models |f| \subseteq a \times b$ et $\mathcal{T} \models \forall_{x \in A} [x \in a \supset \exists!_{y \in B} (x, y) \in |f|]$. À nouveau, on demande que ces morphismes soient fermés par égalité, c'est-à-dire $f = g$ en tant que morphismes si $\mathcal{T} \models |f| = |g|$.

On mentionne les morphismes identité, $|id_A| = \{(x, y) : \mathbf{A} \times \mathbf{A} \mid x = y\}$, et on introduit la notation suivante $|f| : A \rightarrow B$ comme raccourci pour la formule $|f| \subseteq A \times B \wedge \forall_{x \in A} [x \in A \supset \exists!_{y \in B} (x, y) \in |f|]$. Cette notation nous permet de dire f est un morphisme dans $\mathbb{C}(\mathcal{T})$ ssi $\mathcal{T} \models |f| : A \rightarrow B$.

Il est possible de montrer que la catégorie $\mathbb{C}(\mathcal{T})$ est un topos. Soit en construisant un power objet, comme [5, D4.3.8], soit en montrant que c'est une catégorie cartésienne fermée avec classificateur de sous-objet comme [6, section 12]. La preuve sera laissée au lecteur curieux.

On mentionne pour celui qui souhaiterait vérifier.

- L'objet terminal 1 est $\{\blacksquare\}$;
- Le produit $A \times B$ est $\{(x, y) : \mathbf{A} \times \mathbf{B} \mid x \in A \wedge y \in B\}$;
- L'exponentielle B^A est $\{w : \mathcal{P}(\mathbf{A} \times \mathbf{B}) \mid w : A \rightarrow B\}$;
- le classificateur de sous-objets est donné par Ω est $\{t : \Omega \mid \top\}$ et le morphisme \top est donné par $|\top| = \{(\blacksquare, \top)\}$;
- Le power-objet $\mathcal{P}(A)$ est donné par $\{w : \mathcal{P}(\mathbf{A}) \mid w \subseteq A\}$.

6.2.2 Les deux constructions sont inverses

On a défini une théorie intuitionniste à partir d'un topos : le langage interne à \mathbb{C} et on a défini un topos à partir d'une théorie intuitionniste $\mathcal{C}(\mathcal{T})$. À nouveau la question est de savoir à quel point ces constructions sont inverses l'une de l'autre. Avant de répondre à cette question, il faut clarifier la notion d'équivalence entre théories logiques.

On pourrait être tenté de dire que deux théories sont équivalentes s'il existe dans \mathcal{T}_2 un modèle de \mathcal{T}_1 et vice versa. Cependant dans la conception Logiciste, les objets de la théorie n'existent pas vraiment. La théorie prescrit les règles que les objets doivent suivre, mais ne décrit pas forcément des objets qui existent. Par exemple, l'axiome du choix prescrit qu'il doit y avoir un bon ordre sur les

réels mais il se peut qu'aucun mathématicien n'arrive jamais à exhiber un tel ordre, et donc qu'il n'existe pas, au sens de n'avoir aucun représentant. Pour combler ce problème, on introduit la notion de traduction, qui est une règle pour passer d'une théorie à une autre. De plus comme on considère uniquement des théories des types, on peut se permettre d'imposer des contraintes, comme demander que $\Omega_{\mathcal{T}_1}$ soit traduit par $\Omega_{\mathcal{T}_2}$.

Soit $\mathcal{T}_1, \mathcal{T}_2$ deux théories logiques, une traduction de \mathcal{T}_1 dans \mathcal{T}_2 est une application F de \mathcal{T}_1 vers \mathcal{T}_2 qui préserve la structure de types. C'est-à-dire que

- Les types $\mathbf{A}, \Omega, \mathcal{P}(\mathbf{X})$ de \mathcal{T}_1 sont envoyés sur les types $\mathbf{A}, \Omega, \mathcal{P}(\mathbf{F}(\mathbf{X}))$ de \mathcal{T}_2 ;
- Les termes $\blacksquare, \in, =, (a, b), \{a : \mathbf{A} \mid \phi\}, \top, \perp, \wedge, \vee, \neg, \supset, \exists_{\mathbf{A}}, \forall_{\mathbf{B}}$ de \mathcal{T}_1 sont envoyés vers les termes correspondants de \mathcal{T}_2 ;
- Les variables $a_i : \mathbf{A}$ de \mathcal{T}_1 sont envoyées vers $a_i : F\mathbf{A}$ de \mathcal{T}_2 ;
- Les constantes sont envoyées vers d'autres constantes et les relations d'arité n sont envoyées sur d'autres relations de même arité;
- Les séquents $\alpha \vdash_x \beta$ de \mathcal{T}_1 sont envoyés vers $F(\alpha) \vdash_{F(x)} F(\beta)$ de \mathcal{T}_2 ;
- Tous les théorèmes de \mathcal{T}_1 sont envoyés sur des théorèmes de \mathcal{T}_2 .

Une traduction est appelée une **extension conservatrice** à la condition suivante : le séquent $F(\alpha) \vdash_{F(x)} F(\beta)$ est un théorème de \mathcal{T}_2 ssi le séquent $\alpha \vdash_x \beta$ est un théorème de \mathcal{T}_1 .

L'intuition est qu'une extension conservatrice peut avoir rajouté des types et des axiomes sur ces nouveaux types mais aucune nouvelle démonstration sur les anciens types utilise ces nouveaux axiomes.

Dans le cadre de ZFC, les théories sont confondues avec leur modèles et F est une fonction. Dans le cadre catégorique, F est un foncteur.

On peut maintenant passer au théorème suivant :

Théorème 6.2.3. *Soit \mathbb{C} un topos et \mathcal{V} une théorie des types intuitionniste, on a :*

1. \mathbb{C} est équivalent à $\mathcal{C}(\mathcal{T}(\mathbb{C}))$;
2. $\mathcal{T}(\mathcal{C}(\mathcal{V}))$ est une extension conservatrice de \mathcal{V} .

Esquisse de preuve. 1) On commence par construire un foncteur $\xi_{\mathbb{C}} : \mathbb{C} \rightarrow \mathcal{C}(\mathcal{T}(\mathbb{C}))$.

Soit A un objet de \mathbb{C} . Il peut être vu comme un type du langage interne $\mathcal{T}(\mathbb{C})$ et donc l'ensemble $\mathbf{A} = \{x : \mathbf{A} \mid \top\}$ est un objet de $\mathcal{C}\mathcal{T}(\mathbb{C})$. On écrit $\xi_{\mathbb{C}}(A) = \mathbf{A}$.

Soit $f : A \rightarrow B$ un morphisme de \mathbb{C} . On peut définir $\xi_{\mathbb{C}}(f) = \mathbf{f} : \mathbf{A} \rightarrow \mathbf{B} = (\mathbf{A}, |\mathbf{f}|, \mathbf{B})$ avec $|\mathbf{f}| = \{(x, y) : \mathbf{A} \times \mathbf{B} \mid fx = y\}$.

On peut vérifier que $\xi_{\mathbb{C}}$ est un foncteur. C'est même un foncteur logique (strict), des définitions se trouvent dans [6, II.13],[4, A.2.1.1], mais l'idée est que $\xi_{\mathbb{C}}(A \times B) = \xi_{\mathbb{C}}(A) \times \xi_{\mathbb{C}}(B)$ et $\xi_{\mathbb{C}}(\mathcal{P}(A)) = \mathcal{P}(\xi_{\mathbb{C}}(A))$.

Maintenant, il ne reste plus qu'à vérifier que tout objet de $\xi_{\mathbb{C}}$ est isomorphe à un de cette sous catégorie, et que $\xi_{\mathbb{C}}$ est plein et fidèle.

Soit \mathbf{A} un objet de $\mathcal{C}\mathcal{T}(\mathbb{C})$, c'est un terme $a : \mathcal{P}(\mathbf{A})$ de $\mathcal{T}(\mathbb{C})$, et donc un morphisme $\alpha \in \mathbb{C}(1, \mathcal{P}(A))$. Par l'isomorphisme $Sub(A) \simeq \mathbb{C}(1, \mathcal{P}(A))$, il existe un sous-objet $m : A' \rightarrow A$ qui lui est associé.

On affirme maintenant que $\mathbf{A} \simeq \mathbf{A}'$ dans $\mathcal{C}\mathcal{T}(\mathbb{C})$. En effet, on a les fonctions données par $|\mathbf{f}| = \{(x, y) : \mathbf{A} \times \mathbf{A}' \mid my = x\}$ et $|\mathbf{f}^{-1}| = \{(y, x) : \mathbf{A}' \times \mathbf{A} \mid my = x\}$ qui sont inverse l'une de l'autre, donc $\mathbf{f}, \mathbf{f}^{-1}$ forment un isomorphisme entre \mathbf{A} et $\mathbf{A}' = \xi_{\mathbb{C}}(A')$.

Pour voir que $\xi_{\mathbb{C}}$ est plein, on prend $f : \mathbf{A} \rightarrow \mathbf{B}$ un morphisme de $\mathcal{CT}(\mathbb{C})$ entre deux objets de l'image de $\xi_{\mathbb{C}}$. On a donc un terme $\mathbf{f} : \mathbf{A} \times \mathbf{B}$ tel que

$$\mathcal{T}(\mathbb{C}) \models \forall_{x:\mathbf{A}} \exists!_{y:\mathbf{B}} (x, y) \in \mathbf{f}.$$

Comme cette description est vraie dans le langage interne de \mathbb{C} , par les propriétés du langage interne 5.4, il existe une unique fonction $f : A \rightarrow B$ dans \mathbb{C} qui lui correspond et le graphe de f nous redonne \mathbf{f} .

Pour voir que $\xi_{\mathbb{C}}$ est fidèle, on prend dans \mathbb{C} deux morphismes $f, g : A \rightarrow B$. Si $\xi_{\mathbb{C}}(f) = \mathbf{f} = \mathbf{g} = \xi_{\mathbb{C}}(g)$, alors on a $\mathbf{f} = \mathbf{g}$ dans le langage interne, et donc

$$\mathcal{T}(\mathbb{C}) \models \forall_{x:\mathbf{A}} f x = g x.$$

L'égalité interne implique l'égalité interne (5.4), on en déduit $f = g$.

Pour l'extension conservatrice, on définit une traduction $\eta_{\mathcal{V}} : \mathcal{V} \rightarrow \mathcal{T}(\mathcal{C}(\mathcal{V}))$

Si \mathbf{A} est un type de \mathcal{V} , alors $A = \{x : \mathbf{A} \mid \top\}$ est un objet de $\mathcal{C}(\mathcal{V})$, donc un type de $\mathcal{T}(\mathcal{C}(\mathcal{V}))$. On pose $\eta_{\mathcal{V}}(\mathbf{A}) = \mathbf{A} = \{x : \mathbf{A} \mid \top\}$. Remarquons que cela coïncide dans le cas $A = 1$ et $A = \Omega$. Si $t : \mathbf{A}$ est un terme de \mathcal{V} on écrit $\eta_{\mathcal{V}}(t) = t : 1 \rightarrow A$ avec $|t| = \{(\blacksquare, a)\}$

Vérifions que c'est bien une extension conservatrice. Par la remarque 1.3.4, il ne faut vérifier que les séquent $\vdash \phi$ donc que les formules, qui sont des termes de type Ω .

On introduit le lemme suivant, qui a du sens dans le cadre métathéorique de ZFC et des catégories.

Lemme 6.2.4. *Si \mathbf{A} est un type de \mathcal{V} alors il y a une correspondance entre les classes de termes démontrablement égaux de type $\mathcal{P}(\mathbf{A})$ dans \mathcal{V} et les termes de types $\eta_{\mathcal{V}}(\mathcal{P}(\mathbf{A})) = \mathcal{P}(\mathbf{A})$ dans $\mathcal{T}(\mathcal{C}(\mathcal{V}))$.*

Démonstration. Un terme de type $\mathcal{P}(\mathbf{A})$ dans $\mathcal{T}(\mathcal{C}(\mathcal{V}))$ est une flèche $f : 1 \rightarrow \mathcal{P}A$ dans le topos $\mathcal{C}(\mathcal{V})$.

Le graphe de f est un terme de $\mathcal{P}(1 \times \mathcal{P}(\mathbf{A}))$ dans \mathcal{V} tel que :

$$\mathcal{V} \models \forall_{x:1} \exists!_{u:\mathcal{P}\mathbf{A}} (x, u) \in f.$$

En utilisant les règles de dérivation, on obtient

$$\mathcal{V} \models \exists!_{u:\mathcal{P}\mathbf{A}} (\blacksquare, u) \in f.$$

On appelle $\theta = \{x : \mathbf{A} \mid \exists_{u:\mathcal{P}\mathbf{A}} [x \in u \wedge (\blacksquare, u) \in f]\}$. On vérifie ensuite que $\mathcal{V} \models f = \{(\blacksquare, \theta)\}$ Donc $f = \theta$ dans $\mathcal{C}(\mathcal{V})$. Ceci montre la surjectivité. Pour voir l'injectivité, on suppose que $A = A'$ en tant que morphisme. On déduit :

$$\mathcal{V} \models |\mathbf{A}| = |\mathbf{A}'|$$

c'est-à-dire :

$$\mathcal{V} \models \{(\blacksquare, \theta)\} = \{(\blacksquare, \theta')\}$$

et donc :

$$\mathcal{V} \models \theta = \theta'.$$

□

Corollaire 6.2.5. *$\eta_{\mathcal{V}}$ est une extension conservatrice.*

En effet Ω est isomorphe à $\mathcal{P}(1)$ dans $\mathcal{C}(\mathcal{V})$ donc une formule est envoyé sur $\{\blacksquare, T\}$ ssi elle est démontrable. \square

On peut définir une catégorie des théories des types intuitionniste et une catégorie de topos. Dans ce cas \mathcal{T} et \mathcal{F} peuvent être étendu en des foncteurs et ξ, η jouent le rôle d'unité et de co-unité. Plus de détails se trouvent dans [5, D4.3.13] et dans [6, II.13].

Il est malheureux de ne pas pouvoir construire l'extension conservatrice dans le cadre Logiciste. Il est possible qu'il existe une autre démonstration, mais elle n'est pas apparue au cours de mes recherches. La plupart des auteurs ont choisi comme cadre métathéorique celui des catégories pour discuter de ce sujet, laissant de côté cette distinction entre la théorie et la formalisation de la théorie.

Conclusion

Au cours de ce mémoire, nous avons vu que les topos peuvent être vu comme des ensembles généralisés, et que cette structure d'ensembles génère une logique interne. Inversement, les topos peuvent être perçus comme un modèle d'une théorie des types intuitionniste et dans ce cadre, les types se comportent comme des ensembles contenant des variables et des éléments.

Dans les deux cas, il est possible, à l'intérieur d'un topos, de raisonner comme si on était dans *Ens*. On suppose que les objets sont des ensembles avec des éléments et les morphismes sont des fonctions. Toutes les conclusions qui suivent de cette supposition et d'arguments de logique intuitionniste seront valides dans la logique interne, et donc dans le topos en lui-même.

De plus, les topos contiennent toujours des objets-ensembles, qui forment un modèle de la théorie des ensembles. Si un topos a un NNO, alors il est possible de refaire les constructions des rationnels et des nombre réels. Il est également possible de reconstruire des catégories et des foncteurs à l'intérieur de \mathcal{C} .

Il est donc possible de voir un topos comme une métathéorie dans laquelle les mathématiques peuvent avoir lieu. Tous les topos ne redonnent pas le cadre classique des mathématiques. Clairement le tiers exclu n'est pas vrai en général, mais certains topos ont des propriétés qui peuvent sembler contre intuitives. Ainsi la construction des réels par la complétion des suites de Cauchy ou par les coupures de Dedekind donnent en général des ensembles réels distincts. On peut mentionner qu'il existe un topos où toutes les fonctions des réels vers les réels doivent être continues, ainsi qu'un topos où $\mathbb{N}^{\mathbb{N}}$ est un quotient d'un sous-objet de \mathbb{N} . Cela implique que dans cette métathéorie, il existe un nombre dénombrable de fonctions de \mathbb{N} vers \mathbb{N} .

La théorie des topos offre des outils pour forcer une relation dans une théorie et voir les conséquences de ce nouvel axiome. Cela permet notamment de démontrer l'indépendance, ou l'équivalence, de certains axiomes.

Références

- [1] S. Awodey, C. Butz, A. Simpson, and T. Streicher, *Relating first-order set theories, toposes and categories of classes*, *Annals of Pure and Applied Logic* **165** (2014), no. 2, 428–502.
- [2] R. Goldblatt, *Topoi : the categorial analysis of logic*, Elsevier, 2014.
- [3] Y. Gurevich, *The logic in computer science column*, *Bulletin of European Assoc. for Theor. Comp. Science* **35** (1988), 71–82.
- [4] P. T. Johnstone, *Sketches of an Elephant : A Topos Theory Compendium*, Vol. 1, Oxford University Press, 2002.
- [5] ———, *Sketches of an Elephant : A Topos Theory Compendium*, Vol. 2, Oxford University Press, 2002.
- [6] J. Lambek and P. J. Scott, *Introduction to higher-order categorical logic*, Vol. 7, Cambridge University Press, 1988.
- [7] S. Mac Lane, *Categories for the working mathematician*, Vol. 5, Springer Science & Business Media, 1998.
- [8] S. Mac Lane and I. Moerdijk, *Sheaves in geometry and logic : A first introduction to topos theory*, Springer Science & Business Media, 2012.
- [9] C. McLarty, *Elementary categories, elementary toposes*, Clarendon Press, 1992.
- [10] G. Osius, *Logical and set theoretical tools in elementary topoi*, *Model Theory and topoi*, 1975, pp. 297–346.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Faculté des sciences

Place des sciences, 2 bte L6.06.01, 1348 Louvain-la-Neuve, Belgique | www.uclouvain.be/sc