Cours/TD en autonomie: théorie des ensembles

Lionel Vaux Auclair

Logique et automates
M1 Mathématiques et applications, 2020–2021

L'objectif de ce document est de vous accompagner dans une découverte de ZF : la théorie des ensembles de Zermelo–Fraenkel. Il s'agit d'une formalisation de la notion d'ensemble, qui permet de reconstruire tous les outils utilisés en mathématiques.

La théorie ZF

Les seuls symboles sont l'appartenance $\in$ et l'égalité $=$. On peut coder l'inclusion $(x \subset y) \equiv \forall z. z \in x \to z \in y$. Les axiomes de ZF sont ceux énoncés ci-dessous.

Extensionnalité : $\forall x. \forall y. (\forall z. z \in x \Leftrightarrow z \in y) \to x = y$. Cet axiome énonce qu'un ensemble est entièrement caractérisé par ses éléments.

Paire : $\forall x. \forall y. \exists z. \forall w. w \in z \Leftrightarrow w = x \vee w = y$. C'est-à-dire qu'étant donnés x et y, il existe un ensemble dont les éléments sont exactement x et y. Par extensionnalité cet ensemble est unique et on le note $\{x, y\}$. Quand $x = y$ c'est le singleton $\{x\}$.

Réunion : $\forall x. \exists y. \forall z. z \in y \Leftrightarrow \exists w. w \in x \wedge z \in w$. C'est-à-dire qu'on peut former l'ensemble des éléments des ensembles qui sont des éléments de x : c'est l'union des éléments de x, qu'on note $\cup x$. On obtient l'union de deux ensembles par $a \cup b = (\cup\{a, b\})$.

Parties : $\forall x. \exists y. \forall z. z \in y \Leftrightarrow z \subset x$. C'est-à-dire qu'on peut former l'ensemble des parties d'un ensemble x, qu'on note $\mathcal{P}(x)$.

Schéma de remplacement : pour chaque formule F on a un axiome qui est la clôture universelle de :

$$(\forall x. \forall z_1. \forall z_2. F[y \coloneqq z_1] \wedge F[y \coloneqq z_2] \to z_1 = z_2) \to \forall a. \exists b. \forall y. y \in b \Leftrightarrow \exists x. x \in a \wedge F.$$

Autrement dit, dès que F définit une relation fonctionnelle entre x et y, si a est un ensemble, on peut former l'ensemble des images des éléments de a par F.

En appliquant le schéma de remplacement à la formule absurde $\perp$, on obtient un ensemble qui n'a aucun élément : l'ensemble vide $\emptyset$.

Infini : $\exists x.\emptyset \in x \wedge \forall y.y \in x \rightarrow y \cup \{y\} \in x$. Cet axiome assure l'existence d'un ensemble infini. En effet, si x a cette propriété, $y \mapsto y \cup \{y\}$ définit une injection stricte de x dans x.

On va établir des conséquences de ZF, c'est-à-dire montrer $ZF \vdash A$ pour certaines formules A. Il ne s'agit pas ici de rentrer dans le détail des preuves en déduction naturelle : on se contente de raisonner comme d'habitude. Il faut simplement faire attention au fait qu'on construit tout à partir des axiomes précédents. Dans toute la suite, on fixe donc un modèle de ZF : quand on dit « ensemble », il faut comprendre « élément de cette interprétation ».

Premières conséquences

Compréhension : Soit F une formule quelconque et supposons $y \notin \mathsf{VL}(F)$. Vérifiez qu'en appliquant le schéma de remplacement à la formule $G \equiv x = y \wedge F$, on établit la formule :

$$\forall a.\exists b.\forall x.x \in b \Leftrightarrow x \in a \wedge F.$$

C'est le *schéma de compréhension* : étant donnés un ensemble a et une propriété F, on peut former le sous-ensemble $\{x \in a \mid F\}$ des éléments de a qui vérifient F.

Déduisez-en qu'on peut définir l'intersection des éléments d'un ensemble non vide :

$$\forall x.x \neq \emptyset \rightarrow \exists y.\forall z.z \in y \Leftrightarrow \forall w.w \in x \rightarrow z \in w$$

(il faut utiliser la réunion pour pouvoir appliquer la compréhension, et il est bien nécessaire que x soit non vide pour assurer qu'un élément de l'intersection est bien un élément de la réunion). On en déduit l'intersection de deux ensembles : $a \cap b$.

Déduisez-en également qu'il n'y a pas d'ensemble de tous les ensembles :

$$\neg\exists x.\forall y.y \in x$$

en appliquant le schéma de compréhension au paradoxe de Russel.

Couples, produits, fonctions : En posant $(x, y) = \{\{x\}, \{x, y\}\}$, vérifiez qu'on a :

$$(x, y) = (x', y') \Leftrightarrow x = x' \wedge y = y'.$$

Autrement dit, on peut former des couples. Vérifiez ensuite qu'on peut définir le produit de deux ensembles :

$$\forall a.\forall b.\exists c.\forall z.z \in c \Leftrightarrow \exists x.\exists y.x \in a \wedge y \in b \wedge z = (x, y)$$

(il faut utiliser judicieusement l'ensemble des parties pour pouvoir appliquer la compréhension).

La formule

$$\begin{aligned} &Fonc[f] \equiv \\ &\quad (\forall z.z \in f \rightarrow \exists x.\exists y.z = (x, y)) \wedge \forall x.\forall y.\forall y'.(x, y) \in f \wedge (x, y') \in f \rightarrow y = y' \end{aligned}$$

énonce que f est le graphe d'une fonction (c'est-à-dire une relation fonctionnelle : l'ensemble de départ n'est pas donné).

Vérifiez qu'on peut définir le domaine de f comme $Dom(f) = \{x \in \cup\cup f \mid \exists y.(x, y) \in f\}$ (le seul point important est de voir qu'il suffit de chercher x dans $\cup \cup f$). Faites la même chose pour l'image $Im(f)$. Si $x \in Dom(f)$ on note alors $f(x)$ l'unique y tel que $(x, y) \in f$.

Familles d'ensembles : on note $a = (a_i)_{i\in I}$ une famille d'ensembles indexée par I. C'est-à-dire que $Fonc[a] \wedge Dom(a) = I$ et qu'on note $a(i) = a_i$ quand $i \in I$. Montrez qu'on peut former la réunion $\bigcup_{i\in I} a_i$:

$$\exists b.\forall x.x \in b \Leftrightarrow \exists i.i \in I \wedge x \in a_i$$

(il suffit de prendre la réunion de l'image de a) et le produit cartésien $\prod_{i\in I} a_i$ des a_i des a_i :

$$\exists b.\forall f.f \in b \Leftrightarrow Fonc(f) \wedge Dom(f) = I \wedge \forall i.i \in I \to f(i) \in a_i.$$

Notez qu'un élément de $\prod_{i\in I} a_i$ est la donnée d'un élément de a_i pour chaque $i \in I$.

Si I est non vide, on peut former l'intersection $\bigcap_{i\in I} a_i$ des a_i :

$$\exists b.\forall x.x \in b \Leftrightarrow \forall i.i \in I \to x \in a_i.$$

Axiomes du choix

On ajoute généralement à ZF un axiome qui énonce que le produit d'un famille d'ensembles non vides est non vide : c'est-à-dire que si chaque a_i est non vide, on peut *choisir* un élément $y_i \in a_i$ pour chaque $i \in I$, afin de former une fonction $f \in \prod_{i\in I} a_i$ en posant $f : i \mapsto y_i$. Formellement :

$$\begin{aligned}&\forall a.\forall I.(I \neq \emptyset \wedge Fonc[a] \wedge Dom(a) = I \wedge \forall i \in I.a \neq \emptyset)\\ &\qquad\qquad\to \exists f.Fonc[f] \wedge Dom(f) = I \wedge \forall i \in I.f(i) \in a_i.\end{aligned}$$

Vous pouvez montrer que c'est équivalent (modulo les axiomes de ZF) au fait que, pour tout ensemble a, il existe une fonction f définie sur les parties non vides de a telle que $f(x) \in x$:

$$\forall a.\exists f.Fonc[f] \wedge Dom(f) = \{x \in \mathcal{P}(a) \mid x \neq \emptyset\} \wedge \forall x.x \in Dom(f) \to f(x) \in x.$$

On note généralement ZFC la théorie ZF augmentée avec l'axiome du choix.

C'est typiquement ce qu'on utilise pour montrer que toute surjection admet un inverse à droite :

$$\begin{aligned}&\forall f.Fonc[f] \to\\ &\quad \exists g.Dom(g) = Im(f) \wedge Im(g) \subset Dom(f) \wedge \forall y.y \in Dom(g) \to f(g(y)) = y.\end{aligned}$$

Vous pouvez d'ailleurs montrer que cette dernière propriété est équivalente à l'axiome du choix, modulo le reste de ZF.

Ordinaux

Un bon ordre est un ordre tel que toute partie non vide a un plus petit élément. Vérifiez qu'un bon ordre est toujours un ordre total.

Un ordinal est un ensemble a tel que : (1) la relation $\in$ définit un bon ordre strict sur a ; (2) si $x \in a$ alors $x \subset a$. Donnez une formule $Ord[a]$ qui caractérise les ordinaux.

Un segment initial d'un ensemble a est une partie b de a telle que si $x \in y \in b$ alors $x \in b$: donnez une formule $Init(a, b)$ qui dit que b est un segment initial de a. Si $x \in a$, on note $a_x = \{y \in a \mid y \in x\}$.

Montrez que :

1. $\emptyset$, $\{\emptyset\}$ et $\{\emptyset, \{\emptyset\}\}$ sont des ordinaux (on les note respectivement 0, 1 et 2).
2. Les segments initiaux d'un ordinal a sont a et les a_x pour $x \in a$.
3. Si $Ord[a]$ et $x \in a$ alors $x = a_x$.
4. Les segments initiaux d'un ordinal a sont a et les élements de a.
5. Les éléments d'un ordinal sont des ordinaux.
6. Pour tout ordinal a, $a \notin a$.
7. Si a et b sont des ordinaux, on a $a \in b$ ou $a = b$ ou $b \in a$ (et ces alternatives sont mutuellement exclusives).
8. Si a et b sont des ordinaux, on a $a \subset b$ ssi $a = b$ ou $a \in b$.
9. Si a est un ordinal alors $a \cup \{a\}$ aussi (et on note $a + 1$ cet ordinal).
10. Si b est un ordinal et $a \in b$ alors $a + 1 \subset b$.

Arithmétique dans ZF

On dit qu'un ordinal a est fini si toutes ses parties non vides sont des successeurs : si $b \subset a$ et $b \neq \emptyset$ alors il existe c tel que $b = c + 1$.

1. Donnez une formule qui caractérise les ordinaux finis.
2. Montrez qu'il existe un plus petit ordinal ω contenant $\emptyset$ et clos par successeur (si $a \in \omega$ alors $a + 1 \in \omega$).
3. Montrez que ω est exactement l'ensemble des ordinaux finis, et que c'est le plus petit ordinal non fini.
4. On définit Add comme le plus petit ensemble tel que, pour tous ordinaux a et b, on a $(0, (a, a)) \in Add$, et si $(a, (b, c)) \in Add$ alors $(a + 1, (b, c + 1)) \in Add$. Justifiez ce qui autorise cette construction, et vérifiez que Add définit une fonction totale $\omega \to \omega \to \omega$: c'est l'addition des ordinaux finis.
5. Définissez une multiplication $Mult$ sur le modèle précédent, en suivant la structure des axiomes de Peano pour la multiplication.
6. Démontrez que, muni de 0, du successeur et des fonctions Add et $Mult$, ω est un modèle de l'arithmétique de Peano.

Autrement dit, dans tout modèle de ZF, on peut construire un modèle de PA dont la trame est un ensemble (au sens du modèle de ZF fixé) : ω est l'ensemble des entiers naturels.

Et donc pour établir la cohérence de l'arithmétique, il « suffit » de supposer celle de ZF.