Ensembles & applications
(version chantier)

Marc SAGE

20 septembre 2007

Table des matières

1 Langage fonctionnel des classes **5**

2 Il y existe au moins un ensemble **5**

3 Axiome d'extensionalité **5**
3.1 Qu'est-ce qu'une égalité ? . . . 5
3.2 L'égalité ensembliste . . . 6
3.3 L'égalité prouvabilitiste . . . 7
3.4 L'axiome d'extensionalité . . . 8
3.5 Existence et unicité . . . 8
3.6 Caractérisation d'un ensemble . . . 9

4 Axiomes de collecte / récolte **9**

5 Axiomes de séparation (ou schéma de compréhension) **9**
5.1 Ensembles définis par compréhension . . . 9
5.2 L'ensemble vide $\emptyset$ . . . 10
5.3 L'intersection d'un h-nombre d'ensembles, d'un ensemble qcq d'ensembles . . . 11

6 Axiome de la paire **11**
6.1 Agrégation de deux ensembles . . . 11
6.2 Singletons . . . 11
6.3 Le retour de l'extensinalité . . . 12

7 Axiomes de l'union **12**
7.1 Union d'un ensemble . . . 12
7.2 Sur le choix d'un unique élément vérifiant une propriété donnée . . . 13
7.3 Ensembles décrits par extension, ordre et répétitions . . . 13
7.4 Quantificatation finie et entiers usuels . . . 14
7.5 Réunion d'un nombre usuel d'ensembles . . . 15

8 Axiomes des parties **15**
8.1 Ensemble des parties (d'un ensemble donné) . . . 15
8.2 Le paradoxe de Rusell . . . 15
8.3 Union et parties sont dans un bateau . . . 16
8.4 Paire, parties et fonctions . . . 16

9 Axiome de l'infini **16**
9.1 Successeur (d'un ensemble donné) . . . 17
9.2 Le "plus petit" ensemble infini $\mathbb{N}$, de départ $\emptyset$ et successeur s . . . 17
9.3 La récurrence : induction par successeur partant de 0 . . . 18
9.4 L'itération : caractérise l'infini . . . 18
9.5 Le transfini : induction par successeur et récurrence (à partir de 0) . . . 18
9.6 Des h-entiers vers les entiers naturels . . . 19

10 Axiome de fondation **19**
10.1 La relation $\in$ est "bien fondée" . . . 20
10.2 Univers de Von Neumann & axiome de régularité . . . 20

11 Axiomes de remplacement **20**
11.1 Remplacement des éléments du domaine d'une fonctionnelle par leur image . . . 21
11.2 Remplacement, séparation, extensionalité . . . 21
11.3 Remplacement et union . . . 22
11.4 Remplacmenet et produit cartésien . . . 22
11.5 Transition vers AC . . . 23

12 Axiome du choix **23**
12.1 AC et interversion $\forall\exists$ (ou distrib généralisée $\wedge$ sur $\vee$) . . . 23
12.2 AC et remplacement . . . 24
12.3 AC et produit cartésien . . . 24
12.4 AC et fonction de choix . . . 24
12.5 AC et minima . . . 25
12.6 AC et maximaux . . . 25
12.7 AC plus faibles . . . 25
12.8 culture . . . 26
12.9 Pathologies . . . 26
12.10Lectures . . . 26

13 Cardinaux innaccssibles **27**

14 Divers **28**
14.1 ZF avec atomes . . . 28
14.2 théorie alternative à ZFC : von Neumann–Bernays–Gödel (NBG) . . . 28
14.3 De l'art de conceptualiser : des sacs aux ensembles . . . 28
14.4 Pourquoi les indécisables ne le sont pas autant que ça, notion de vérité . . . 29
14.5 Discussion David D après *braquage à l'anglaise* . . . 29
14.6 Une idée pour se rassurer d'utiliser ZF . . . 30
14.7 Kripke-Platek : un ZF sans partie . . . 30

Acte de foi : ZF possède (au moins) une intérprétation, avec valeur de vérité exclusive. Corollaire : ZF est consistant)

Le but de cette présentation n'est pas de donner un système épuré selon le principe du rasoir d'Ockham, mais de reconstituer un système utilisé par la plupart des matheux d'aujourd'hui (sans qu'ils ne s'en rendent bien compte, d'ailleurs).

Le langage utilisé est composé d'un seul symbole de relation $\in$ dit d'***appartenance*** :

$a \in b$ se lit « a ***appartient à*** b » ou « a est un ***élément*** de b »
$b \ni a$ se lit « b ***contient*** a ***comme élément*** »

Principal schéma est la **compréhension**. Premier pb est Berry –> *bonne* syntaxe (cf chapitre précédent). Second Pb est Russell, première solution est le typage (un ensemble de choses de type n est de type $n+1$), mais on préfère Zermelo (1908) qui a *borné* la compréhension. TOus les axiomes suivants sont de la compréhesnio cachée, à l'excetsion d'extsnnalit qui asure l'uncité de lesnbmel considéré (et de fondation qui n'est qu'un choix d'ensemble, AC et infini)

NOTATION :pour chaque formcule φ et chaque générique a, on a abrégera ($\exists E$ devient $\maltese$)

$$\maltese_a \varphi :\equiv \exists E,\ \forall a,\ (a \in E \iff \varphi)$$
(lire "il existe l'ensemble des a tels que φ)

(la lettre générique a doit rester la même ! elle précise en quoi on collecte) –> énoncé *collectivisant* chez Bourbaki

Avec "extens", on peut remplacer $\exists E$ par $\exists! E$ en gardant un énoncé équivalent.

Par exemple, on a toujours $\maltese_a\ a \in A$ (prendre A pour E). Se réécrivent alors :

vide $\emptyset$ $\quad \maltese_a\ \bot$ (implique $\forall a,\ a \notin \emptyset$)

h-extension $\{a, b, ..., z\}$ $\quad \forall a, b, ..., z,\ \maltese_\xi\ (\xi = a) \vee (\xi = b) \vee \cdots \vee (\xi = z)$ (implique : paire, singleton)
(si pas d'argument, $\vee$ devient $\bot$ et on retrovue vide)

h-réunion $A \cup B \cup \cdots \cup Z$ $\quad \forall A, B, ..., Z,\ \maltese_x\ (x \in A) \vee (x \in B) \vee \cdots \vee (a \in Z)$ (avec singleton, implqiue h-extension)

réunion $\bigcup_{i \in I} A_i$ $\quad \maltese_a\ (\exists i \in I,\ a \in A_i)$ (pour chaque fonctionnelle $i \mapsto A_i$ définie sur I)

union $\cup \mathcal{A}$ $\quad \forall \mathcal{A},\ \maltese_a\ \exists A \begin{matrix} \in \mathcal{A} \\ \ni a \end{matrix}$ $\quad (\bigcup_{A \in \mathcal{A}} \mathcal{A})$

h-intersection $A \cap B \cap \cdots \cap Z$ $\quad \forall A, B, ..., Z,\ \maltese_x\ (x \in A) \wedge (x \in B) \wedge \cdots \wedge (a \in Z)$

intersection $\bigcap_{i \in I} A_i$ $\quad \maltese_a\ (\forall i \in I,\ a \in A_i)$ (pour chaque fonctionnelle $i \mapsto A_i$ définie sur I)

intersection $\cap \mathcal{A}$ $\quad \forall \mathcal{A} \neq \emptyset,\ \maltese_a\ (\forall A \in \mathcal{A},\ a \in A)$ $\quad (\bigcap_{A \in \mathcal{A}} \mathcal{A})$

partie $\mathfrak{P} A$ $\quad \forall A,\ \maltese_P\ P \subset A$

séparation $\{a \in A\}_{aP}$ $\quad \forall A,\ \maltese_a \begin{matrix} a \in A \\ \exists P_a \end{matrix}$ (pour chaque 1-prédicat P)

remplacement (large) $\quad \forall A,\ \left(\forall a \in A,\ \exists^{\leq 1} b,\ P_a^b\right) \Longrightarrow \left(\maltese_b\ \exists a \in A,\ P_a^b\right)$ (pour chaque 2-prédicat P)

collecte (ou récolte) $\quad \forall A,\ \left(\forall a \in A,\ \maltese_b\ P_a^b\right) \Longrightarrow \left(\maltese_b\ \exists a \in A,\ P_a^b\right)$ (pour chaque 2-prédicat P)

itération $\quad \forall o,\ \maltese_n \left[\forall S,\ n \in S \Longleftarrow \left\{ \begin{matrix} o \in S \\ \forall s \in S,\ f(s) \in S \end{matrix} \right.\right]$ (pour chaque fonctionnelle f définie partout)

Dedekind (source : *La création des nombres*, H ; Sinaceur, Vrin)

p27 La contribution de Dedekind à la constitution de la théorie des ensembles est fondamentale, et même antérieure à celle de Cantor. Il faut par ailleurs rappeler que des développements important de cette théorie par Cantor sont indissociables de la rencontre de ce dernier avec Dedekind à Zürich

p 115 Les axiomes de Zermelo [...] pour la théorie des ensembles sont en partie tirés [du § 1 de *Qu'est-ce sont et à quoi servent les nombres ?*]

p 124 Zermelo écrira, en 1916, que l'ouvrage de Dedekind « est la première tentative, menée à bien, pour développer le concept et les propriétés fondamentales des nombres naturels, par des méthodes purement ensemblistes, à partir de l'idée simple de représentation »

P 175 *footnote* : Zermelo précise que [l'axiome de l'infini] « est dû pour l'essentiel à M. R. Dedekind »

p 216 Il est bien connu que Zermelo fut conduit à poster son « axiome de l'infini » [footnote : Zermelo l'appelait « axiome de Dedekind »] par ce que la tentative de démonstration de Dedekind (66) reposait sur le concept contradictoire d' « ensemble de tout le pensable »

Zermelo (inspiéré par Dedekind) donne en 1908 : extension, (vide,) séparation, paire, union, partie, infini (et AC, *cf.* plus bas) —> théorie Z (sans AC)

Les deux axiomes fondation & remplacement (attribués à Abraham FRAENKEL vers 1922), se rajoutent —> théorie ZF

(on devrait rajouter Thoralf Albert SKOLEM pour préciser le langage, et aussi pra rappor à remplacement)

l'axiome d'extenstinatlité est une "définition" de =
tous les autres axiomes sonts des axiome existentiels, donc de *création*.
La création peut être

1. (a) univoque/fonctionnelle $\exists!A, P_A$ (svt décrite par **compréhension** !), ce qui donne des "opérateurs" ensemblistes
   (b) lâche/sauvage $\exists$

création existence	*fonctionnelle* (images décrites par **compréhension**)	*plurivoque* sauvage
axiomes	paire, h-extens séparation union, partie remplacement (*opérateurs ensemblistes*)	itération fondation AC

(il convietn de rajouter l'opérateur "constant" $\emptyset$, qui peut se voir comme 0-extension)

Dessin :
fondation = la terre,
vide posé sur terre,
infini = ciel pointillé (audelà : transfini ; endeça : fini)
↑paire et partie
↓uninon
↻ sépration, ⟶ remplacement

Essai refonte ? ? ? :
(**existtence** codée dans la logique : cf. un modèle est par def *non vide*)
extensionéalité
parties (& union)
collecte
- ***remplacement & union***
- ***séparation***
- ***paire&extension***

infini, itération
fondation
choix
AXiome des grands cardinaux ? ? ?
Axiome de détermination projecive ? ? ? (contredit AC)

Souhaits intuitifs : pouvoir

1. **(=)** déterminer un ensemble par ses éléments
2. **(exten)** mettre des objet en nombre fini dans un sac : $\{a, b, c..., z\}$
3. **(réunion)** intersecter et réunir un ensemble d'enembles

4. **(itération)** pouvoir itérer indéfiniement
5. **(séparation)** pouvoir décrire l'extension d'un concept par *compréhension* (pb : Russell)
6. **(choix, remplact)** de $\forall a \in A,\ \exists b,\ P(a,b)$ parler d'une *fonction* $f : A \longrightarrow ?$ tq $\forall a \in A,\ P(a, f(a))$

MIse en garde sur les entiers usuels et naturels. À stade où on est, on ne peut pas parler d'entier ensemblisites (pas encore définis) et donc impossible de quantifier sur eux. Mais on peut parler des entiers usuels que l'on sait lister : un, deux, trois, quatre..., mille quarante-et-un, mille quarante-deux,... Par ***entier usuel*** on entend un concept de la vie usuelle, sans beson de préciser les limites de ce concept. C'est pourquoi certaines propriétés qui suivent s'écriront $\forall a, b, c, ..., z$, sous-entendu qu'on prend un liste de symboles que l'on peut écrire à la suite, *et que l'on pourra expliciter au besoin* (les ... sous-entend qu'un tel procédé est clair).

Toutes les propositions portant sur des entiers usuels pourront êtres "formalisées" puis "généraliséees" ? ? ? aux entiers naturels une fois construit $\mathbb{N}$, ce qui nécessite l'axime de l'infini.

comme en logique, on utilise le h-principe de récurrence.

1 Langage fonctionnel des classes

correspondance : un 2-prédicat (ou *relation globale*)
(classe) *graphe* : ens de couples (trop tôt) (ou *correspondance locale*)
correspondance *réciproque* : un 2-prédicat
(classes) *domaine* et *image* (et *champ* = domUim ?)
univoque (ou fonctionnelle) (au plus une image) EG $\cup$
(une *fonctionnelle* est une corres univoque)
injective : réciproqu univoque EG $\mathfrak{P}$
biunivoque : univque et injective EG $a \mapsto \{a\}$, s, $\mathfrak{P}$
EXO : composer deux corres

2 Il y existe au moins un ensemble

On va tout construire sur une brique élémentaire ; il nous faut au moins disposer d'un ensemble ! Il suffit pour cela d'une invoaction *ex nihilo* :

Soit un ensemble a.

(On rappelle l'idée : on part d'un 1-prédicat $\mathcal{R}(a)$ et d'une 1-tautologie $\tau(p)$, par exemple $a \in a$ et $p \Longrightarrow p$, lesquels permettent de poser l'axiome prédicatif $\exists a,\ \tau(\mathcal{R}(a))$, d'où l'on tire l'invocation)

3 Axiome d'extensionalité

3.1 Qu'est-ce qu'une égalité ?

Rant sur l'égalité comme "sélection" de ce que l'on souhaite retenir : tous les objets équivalents / indistinguables pour nos critères seront dits égaux.

Citer Bergson dans le rire (eg des moutons)

et Frege (151 *abstraire, c'est oublier*) *Faire abstraction de quelque chose, ce n'est rien d'autre que ne pas y prêter une attention particulière. Le cœur de l'affaire est évidemment dans le mot « particulière ». L'inattention est une lessive très mordante, elle ne doit pas être employée avec une concentration trop forte si on ne veut pas qu'elle dissolve tout ; mais elle ne doit pas non plus avoir une concentration trop faible si on veut qu'elle produise une altération suffisante. Tout repose donc sur le juste degré de la solution, et il n'est pas facile de tomber juste.*

3.2 L'égalité ensembliste

Critère ensembliste : on ne s'intéresse qu'aux éléments qu'il y dedans, sans tenir compte ni de l'ordre des éléments ni des éventuelles répétitions.

(On reprendra cette remarque avec l'axiome de la paire, car nous disposerons alors de suffisamment d'ensembles pour qu'elle devienne pertinente.)

Définition (l'inclusion $\subset$).
On dira qu'un ensemble A ***est inclus dans*** *un ensemble B si les éléments de A sont tous des éléments de B. On notera*

$$A \subset B \overset{\text{déf.}}{\iff} [\forall a \in A,\ a \in B]\,.$$

On dit aussi que A est une ***partie*** *(ou un* ***sous-ensemble***[1] *) de B.*

On notera de suite la transitivité de l'inclusion

$$(A \subset B) \wedge (B \subset C) \implies A \subset C$$

(et on en profite pour observer l'importance de bien différencier le symbole $\subset$ d'un C majuscule...) ainsi qu'une certaine transitivité des symboles $\in$ et $\subset$:

$$x \in A \subset E \implies x \in E.$$

(mais on n'a pas $x \subset a \in E \implies x \in E$)

Définition (l'égalité $=$).
Deux ensembles sont dit ***égaux*** *s'ils contiennent les mêmes éléments :*

$$A = B \overset{\text{déf.}}{\iff} \begin{cases} A \subset B \\ B \subset A \end{cases}.$$

Ainsi, pour montrer que deux ensemble sont égaux, on montrera très souvent une inclusion puis l'autre : c'est la méthode de la ***double-inclusion*** (qui n'est autre que revenir aux définitions).

RQ égalité RST (exo), ce qui est cool.

RQ prouvabilitisite Si $A = B$, alors par déf on peut dire $P(A) \iff P(B)$ pour $P(X)$ le prédicat $x \in X$ à variable fixée x.

Rq : que signiefie être différent ?

$$\begin{aligned} A \quad \neq \quad & B \iff (A \not\subset B \text{ ou } B \not\subset A) \\ \iff \quad & [\exists a,\ (a \in A) \wedge (a \notin B) \text{ ou } \exists b,\ (b \in B) \wedge (b \notin A)] \\ \iff \quad & \exists x,\ \begin{cases} x \in A \\ x \notin B \end{cases} \text{ ou } \begin{cases} x \in B \\ x \notin A \end{cases}. \end{aligned}$$

Traduction : il y a un éléments dans l'un et pa d'ans l'autre.

Définition (l'inclusion stricte $\subsetneq$).
Une inclusion $A \subset B$ est dite ***stricte*** *lorsque de plus $A \neq B$. On note alors*

$$A \subsetneq B \overset{\text{déf.}}{\iff} (A \subset B \text{ et } A \neq B)$$

(on peut voir le symbole $\subsetneq$ comme la fusion des symboles $\subset$ et $\neq$).

Ainsi, lorsque $A \subsetneq B$, on peut affirmer qu'il y a un élément de B qui n'est pas dans A (l'inverse contredirait l'inclusion $A \subset B$) :

$$A \subsetneq B \implies \exists b \in B,\ b \notin A$$

[1] Il est préférable d'utiliser le terme ***partie*** . En effet, on définit en mathématique beaucoup de termes de une forme très standardisée ***sous-[truc]***, tout comme le *2-buthy-pent-2-ène* en chimie. Avouer que l'on réfléchit moins à parler de vinaigre. On parlera également de ***suite*** pour parler d'une application définie sur $\mathbb{N}$. De même, il est beaucoup plus clair d'écire $3+8$ plutôt que la notation fonctionelle très générale $a(3,8)$ où a désignerait la fonction addition.

3.3 L'égalité prouvabilitiste

Critère de prouvabilité : on ne distinguera pas des objets qui donnent les même énoncés.

Afin de comprendre ce que l'on souahite d'une égalité prouvabilitiste, notée provisoirement $\overset{\circ}{=}$, essyaons de montrer l'énoncé (où P est un 1-prédicat)

$$[a \overset{\circ}{=} b] \overset{?}{\Longrightarrow} [P(a) \iff P(b)] .$$

D'après le th de déduction, il suffit d'inférer $P(a) \iff P(b)$ d'une invocation $\downarrow a, b,\ a \overset{\circ}{=} b$. On raisonne par induction sur la forme de P.

Si P est propositionnel, on peut le supposer de la forme $Q * R$. Par récurrence, on a les équivalences $Q(a) \iff Q(b)$ et $R(a) \iff R(b)$. Or on a pour chaque connecteur $*$ la tautologie

$$[(p * q) \wedge (p \iff p') \wedge (q \iff q')] \Longrightarrow [p' * q'] .$$

Si P est quantifé, disons $\forall x, Q(x, a)$, invoquons un variable c. On a par récurrence appliqué à $Q(x, \cdot)$ le théorème $Q(c, a) \iff Q(c, b)$, d'où par généralisation $\forall x,\ Q(x, a) \iff Q(x, b)$, et on utilsie la règle de substitution dans les énoncés quantifés. On conclut par syméterie.

Tout ce qui précède ressort uniquement de la logique prédicative. En revnache, si P est relationel, il est de la forme $c_0 \in a$ ou $a \in c_0$ pour une cste ou fixée c_0 et l'on peut enfin discuter d'ensemble.

Définition (égalités latérales $\rightrightarrows$, $\leftrightarrows$, $\leftrightarrows$). *On dit que deux ensembles sont* ***égaux à droite/gauche*** *s'ils appartiennent à / contiennet les mêmes ensembles,* ***égaux des deux côtés*** *s'ils sont égaux à droite et à gauche :*

$$\begin{aligned} a \rightrightarrows b &\overset{\text{déf.}}{\iff} \forall X,\ (a \in X) \iff (b \in X) \\ A \leftrightarrows B &\overset{\text{déf.}}{\iff} \forall x,\ (x \in A) \iff (x \in B) \\ E \leftrightarrows F &\overset{\text{déf.}}{\iff} (E \rightrightarrows F) \wedge (E \leftrightarrows F) . \end{aligned}$$

(dans l'égalité *à droite* $a \rightrightarrows b$, les génériques X sont *à droite* de a et b, dans l'égalité *àgacueh* $A \leftrightarrows B$, les génériques x sont *à gauche* de A et B.

En reprenant la démonstratino ci-dessus, on voit que l'on peut conclure en prenant pour $\overset{\circ}{=}$ l'égalité bilatère sus-définie (la définition ci-dessus a été posée pour ça).

Mais on a mieux, à savoir la réciproque : nécessairement $\overset{\circ}{=}$ implique $\leftrightarrows$. On montre cela et on résume tout dans le h-théorème suivant.

h-théorème (substitution des termes "égaux").
Soit $\overset{\circ}{=}$ un 2-prédicat et a, b deux symboles d'objet (localement) singulier. Pour que l'énoncé

$$[a \overset{\circ}{=} b] \Longrightarrow [P(a) \iff P(b)]$$

soit pour chaque 1*-prédicat P un théorème de la théorie des ensembles, il faut et il suffit que cette dernière prouve l'implication*

$$(a \overset{\circ}{=} b) \Longrightarrow (a \leftrightarrows b) .$$

h-Démonstration.
Le sens réciproque a déjà été fait (et nous a conduit à définir l'égalité bilatère).

Dans l'autre sens, supposons $a \overset{\circ}{=} b$ et montrons $a \leftrightarrows b$. Pour chacune des deux égalités "sided", on invoque un x. On forme alors les prédicats $x \in \ell$ et $\ell \in x$ d'argument libre ℓ d'où les équivalences voulues

Rq : les deux égalités ci-dessus sont bien RST (exo) donc l'égalité bilatère aussi.

Il est aisé de montrer qu'aucune de ces deux égalités "latéralisées" ne se réduit à l'autre avec des modèles tous simples :

On passe de l'un à l'autre de ces modèles en renvserant le sens des flèches (on peut même retirer l'étoile, ce qui rend "vide" une des égalités).

3.4 L'axiome d'extensionalité

Intuivement, on veut que les égalité ensemblistes et prouvabilitiste coïncident. Vu ce qui précède, cela revient à demander que les égalité ensembliste (*i. e.* à gauche) et bilatère coïncident, ou encore que égalité (ensembliste) implique égalité à droite. Le h-théorème précédent donne un h-corollaire immédiat.

Axiome d'extensionalité.

$$[a = b] \implies [(a \in E) \iff (b \in E)] .$$

h-Corollaire (égalité et substitution). *Pour chaque* 1*-prédicat* P*, on a*

$$[a = b] \implies [P(a) \iff P(b)] .$$

La termlinogie d'extensionalité sera jusfiera plus tard (*cf.* section *Ensembles décrits par extension*)

Mq extensinnalité est nécessaire : $\begin{array}{ccc} \triangle & \longrightarrow & \blacktriangle \\ & & \\ \square & \longrightarrow & \blacksquare \end{array}$ $\triangle$et$\square$ ont me^mes éléméents mais n'appartiennent pas au mêmes ensembles.

3.5 Existence et unicité

Donnons nous un 1-prédicat p.

Une première question qui doit se poser est l'***existence*** d'un objet vérifiant ce prédicat ; au niveau syntaxique, cela revient à se demander si l'on dispose de l'énoncé

$$\exists a,\ p(a) \ ?$$

Lorsque la réponse est oui, disons $p(a_0)$, il est naturel de dire alors que le prédicat p est ***réalisable*** et que l'objet a_0 le ***réalise***.

Une fois la première question résolue, ou bien notre prédicat n'est pas réalisable (et l'on passe à autre chose), ou bien il l'est, mettons par un objet a_0 : avant de chercher à décrire tous les objets le réalisant, on peut déjà se demander s'il en existe d'*autres* que a_0. En termes syntaxiques, a-t-on l'énoncé

$$\exists a,\ [p(a) \wedge (a \neq a_0)] \ ?$$

La seconde question peut en fait être découplée de la première grâce à la reformulation suivante : dire qu'il ne peut pas y avoir *plus* d'un objet réalisant notre prédicat, c'est dire que "deux" objets le réalisant doivent être indistiguables – *i. e.* égaux. En d'autres termes, dispose-t-on de l'énoncé (dit d'***unicité***)

$$[p(a) \wedge p(b)] \implies [a = b] \ ?$$

(Sanity check : si la réponse est oui, de la donnée $p(a_0)$ l'on déduit l'énoncé $\forall a,\ p(a) \implies [a = a_0]$, ce qui est précisément la négation de $\exists a,\ p(a) \wedge (a \neq a_0)$; traduction : non, il n'y a pas d'autres objets que a_0 réalisant notre prédicat.)

Il est usuel de condenser les énoncés l'existence et d'unicité à l'aide du quantificateur $\exists!$ (lire "*il existe un, et un seul*" ou "*il y a un unique*" ou tout autre variante) : ? ? ? définir avant

$$\exists^{\leq 1} a,\ p(a) :\equiv \forall^2 a, b,\ ([p(a) \wedge p(b)] \implies [a = b])$$

$$\exists! a,\ p(a) :\equiv [\exists a,\ p(a)] \wedge \left[\exists^{\leq 1} a,\ p(a)\right] .$$

3.6 Caractérisation d'un ensemble

Dans notre démarche d'axiomatisation, comme nous partons de rien, ils nous faudra des axiomes d'existence pour "créer" des ensembles – à commencer par le tout premier : il existe un ensemble !

Il arrivera très souvent que ces axiomes de création assurent l'*unicité* de la créature engendrée. Ils seront en effet souvent de la forme

$$\exists a,\ \forall x,\ (x \in a \iff \pi(x)) \text{ pour un certain prédicat } \pi,$$

de sorte que, si b est un autre ensemble vérifiant une telle proposition, on a à x fixé les équivalences $x \in a \overset{P(a)}{\iff} \pi(x) \overset{P(b)}{\iff} x \in b$, d'où l'égalité $a = b$. On dit alors que le prédicat π ***caractérise*** (ou ***détermine*** ou ***définit*** voire ***dépeint***[2]) l'unique ensemble le réalisant. Par exemple, n'importe quel ensemble a est caractérisé par le prédicat "appartenir à a", ce que l'on énonce traditionnellement :

un ensemble est entièrement déterminé par ses éléments.

AInsi, un ensemble peut être décrit par un prédicat.
Réciproqe ? est-ce que chaque prédicat décrit un ensemble ? –> séparation

4 Axiomes de collecte / récolte

<=> remplacment (large) + union.
(et rempalcaement large <=> reamplcamt stricite + sépération)

5 Axiomes de séparation (ou schéma de compréhension)

Soit p un 1-prédicat. On a envie de regrouper par la pensée les objets réalisant p : on parle de la ***classe*** (des objets réalisant) p. Est-ce qu'une classe est un *ensemble* ? En d'autres termes, existe-t-il un ensemble caractérisé par le prédicat p ?

Le paradoxe de Rusell nous dit que non, à l'aide d'un joli argument diagonal : si on le pouvait, la classe des ensembles ne s'appartenant pas serait un ensemble Ω, caractérisé par $\forall x,\ (x \in \Omega) \iff (x \notin x)$, ce qui donne une contradiction blatante en spécialisant x en Ω.

VISION TYPES ? ? ? VISION ENSEMBLE ? ? ? Ce paradoxe est dû essentiellement à la "taille" de la classe considérée. Afin de pouvoir quand même parler d'un ensemble entièrement déterminée par p, on va restreindre la classe à des objets appartenant *déjà* à un ensemble préexistant.

5.1 Ensembles définis par compréhension

Axiome de séparation.
Pour chaque 1*-prédicat* P*, on dispose de l'énoncé*

$$\forall A,\ \exists A',\ [a \in A'] \iff [(a \in A) \wedge P(a)].$$

Intuitivement, on *sépare* dans l'ensemble A les a qui vérifient la proposition P et ceux qui ne la vérifient pas. On notera

$$A' = \{a \in A\ ;\ P(a)\}.$$

et la notation $\{x\}_{P(x)}$? Par exemple $\left\{x^2\right\}_{x \geq 0}$. *On met d'ailluer la précistion* $P(x)$ *où on veut, à droit à gauche, dedans... tant que c'est clair.*

[2] le verbe ***qualifier*** ne convient pas car une qualification n'a aucun raison d'être exhaustive

Lorsqu'on décrit un ensemble A de la sorte selon les propriétés que vérifient ses éléments, on dit que l'on décrit A ***par compréhension***.

Les axiomes ci-dessus étant tous tissés de la même étoffe, on parle pour les désigner tous d'un ***schéma*** d'axiomes, d'où la terminologie ***"schéma de compréhension"***.

CULTURE Dans *La logique ou l'art de penser* d'Antoine Arnauld et Pierre Nicole, citons I 6 : « *J'appelle* compréhension *de l'idée les attributs qu'elle enferme en soi et qu'on ne peut lui ôter sans la détruire.... J'appelle* étendue *de l'idée, les sujets à qui cette idée convient...* » (il faut comprendre *étendue* au sens frégéen de *extension*, qui à l'époque cartésienne désigne l'attribue essentiel de la matièe)

5.2 L'ensemble vide $\emptyset$

En séparant dans un ensemble quelconque (dont l'existence est assurée par ue invocation *ex nihilo*) à l'aide d'un prédicat contradictoire (par exemple ne pas être égal à soit même), on obtient un ensemble qui ne possède aucun élément. Un tel ensemble est unique au vu des équivalences (on note $\emptyset$ et $\emptyset'$ deux tels ensembles) $x \in \emptyset \iff x \in \emptyset'$ valides (faux $\iff$ faux) pour chaque x. On l'appelle ***ensemble vide*** et on le note $\emptyset$:

$$\exists!\emptyset,\ \forall x,\ x \notin \emptyset.$$

Remarquer que l'ensemble vide vérifie chaque propriété[3] : pour chaque 1-prédicat P, on a l'énoncé

$$\forall x \in \emptyset,\ P(x).$$

Donnons quatre bonnes raisons à cela.

1. **(souhait)** Un tel énoncé ne dit rien, on dit qu'il est ***vide***. Si l'on devait lui valeur de vérité (vrai ou faux), sa fausseté nous conduirait à hurler à la contradiction dès que quelqu'un se tairait. Il est bien plus serein de supposer que ne rien dire ne nuit pas à la cohérence de ce qui a déjà été dit.
2. **(heuristique)** Un tel énoncé est une conjonction vide, donc est le neutre pour la conjonction, à savoir le vrai.
3. **(sens)** Revenir à la définition permet d'écrire $[\forall x \in \emptyset,\ P(x)] \equiv [\forall x,\ x \in \emptyset \implies P(x)]$; or du faux impique n'importe quoi.
4. **(preuve)** Invoquer un x tel que $x \in \emptyset$: on sait donc que $x \neq x$; or le théorème $\forall a, a = a$ se spécialise en $x = x$; des deux on déduit n'importe quoi, *a fortiori* $P(x)$.

On prendra par conséquent soin, lorsqu'on étudiera les propriétés d'un ensemble, de vérifier que cet ensemble est *non vide* (intuitivement, que ses éléments existent bel et bien) afin de ne pas s'étonner de lui trouver des propriétés miraculeuses.

CULTURE : on peut citer la définition originelle de Frege dans *Les fondements de l'arithmétiques* ainsi que les commentaires qui suivent (point 74) :

Puisque rien ne tombe sous le concept : « non identique à soi-même », je pose par définition : 0 est le nombre cardinal qui appartient au concept « non identique à soi-même ».

On trouvera peut-être étrange que je parle ici d'un concept. On objectera que ce concept implique contradiction et que cela rappelle de vielle connaissances, telles que le fer en bois et le cercle carré. Après tout, je pense qu'elles ne méritent pas le mal qu'on en dit. On ne prétendra pas que ces concepts soient utiles, mais ils ne peuvent pas nuire non plus si on prend soin de ne pas supposer qu'ils subsument quelque chose ; et cela n'est pas supposé dans le simple usage du concept. La contradiction éventuellement enveloppée dans un concept n'est pas toujours si évidente qu'elle apparaisse sans recherche ; encore faut-il d'abord prendre ce concept en considération et le traiter selon les lois logiques, comme n'importe quel autre. Or la logique et la rigueur des preuves exigent seulement qu'un concept ait des limites parfaitement définies, que pour tout objet on puisse dire s'il tombe sous ce concept ou non. Les concepts qui recèlent une contradiction comme « non identique à soi- même » satisfont entièrement à cette exigence ; quel que soit l'objet choisi, on sait qu'il ne tombe pas sous un tel concept. [...]

Pour définir le 0, j'aurais pu prendre n'importe quel concept sous lequel rien ne tombe. Mais il convenait de choisir un concept tel que cette particularité puisse en être démontrée par des moyens purement logiques ; ce à quoi le concept « non identique à soi-même » semble plus favorable, étant entendu que je donne à « identique » la définition leibnizienne introduite plus haut, définition purement logique.

[3] On parle ici uniquement des propriétés se rapportant aux *éléments* de l'ensemble considéré (il est évident que le vide, comme chaque ensemble, ne vérifie pas la propriété $a \neq a$).

5.3 L'intersection d'un h-nombre d'ensembles, d'un ensemble qcq d'ensembles

Étant donnés deux ensembles A et B, on peut former leur ***intersection***

$$A \cap B := \{x \in A \ ; \ (x \in A) \wedge (x \in B)\}$$

dont on montre aisément (exercice !) la commutativité $A \cap B = B \cap A$. De même, on forme l'intersection d'un h-nombre (non nul) d'ensembles $A, B, ..., Z$, laquelle est caractérisée par

$$\forall \varepsilon, \ [\varepsilon \in (A \cap B \cap \cdots \cap Z)] \iff [(\varepsilon \in A) \wedge (\varepsilon \in B) \wedge \cdots \wedge (\varepsilon \in Z)] \, .$$

Ainsi, les propriétés du connecteur $\wedge$ se reflètent exactement sur $\cap$ (commutatitivé, associativité).

On notera que l'ensemble vide est ***absorbant*** pour $\cap$, au sens où

$$\forall A, \ A \cap \emptyset = \emptyset.$$

(preuve : mq $A \cap E \subset E$ et mq $\emptyset \subset E$)

EXo *: soit $\mathcal{A}$ un ensemble non vide. Montrer qu'il y a un unique ensemble $\cap\mathcal{A}$ (l'intersection de $\mathcal{A}$) tel que*

$$a \in \cap\mathcal{A} \Longleftrightarrow \forall A \in \mathcal{A}, \ a \in A.$$

DEM unicité par extensionl. Soit $A_0 \in \mathcal{A}$. Définission $\cap\mathcal{A} := \{a \in A_0, \ \forall A \in \mathcal{A}, \ a \in A\}$. Soit a : si $a \in A_0$, l'équivalence est tauto, sinon est dit faux<=>faux

6 Axiome de la paire

c'est un axiome de création *verticale* descendante (partie créé horizontale ascendant)

6.1 Agrégation de deux ensembles

On peut toujours mettre dans un même sac deux ensembles donnés :

$$\forall a, \ \forall b, \ \exists \{a, b\}, \ (x \in \{a, b\}) \iff (x = a \ ou \ x = b) \, .$$

Un tel $\{a, b\}$ est unique par ce qui précède : on parle de la ***paire*** formée des éléments a et b.

Puisque le « ou » est commutatif, on a

$$\{a, b\} = \{b, a\} \, .$$

Il faut retenir de cela qu'*a priori il n'y a pas d'ordre dans un ensemble* (*cf.* section coresopindante dans union)

Remarque. Paire est un axime de création par "agrégation". Si l'on veut en agréger trois, mettons a, b, c, on peut essayer en pairant $\{a, b\}$ avecc c, mais cela donne la paire $\{\{a, b\}, c\}$. Pour faire disparaître l'enveloppe de $\{a, b\}$ à l'intérieur de cette dernière paire, on va utilisrr l'axiome *de l'union.*

6.2 Singletons

ON peut toujours mettre un ensemble a donné dans un sac $\{a\}$:

$$(x \in \{a\}) \iff (x = a) \, .$$

Il suffit de prendre la paire $\{a, b\}$ avec $a = b$, appelé ***singleton***

$$\{a, a\} =: \{a\}$$

Prop (singleton et égalité). *le singleton préserve l'égalité :*

$$a = b \Longleftrightarrow \{a\} = \{b\}$$

DEM Supposos$a = b$. Alors $x \in \{a\}$ ssi (prop) $x = a$, ie ssi (transititivé de $=$) $x = b$, ie ssi $x \in \{b\}$ (c'est un cas particulier du h-théorème de substitution).

Suppsons $\{a\} = \{b\}$, ie $\forall x,\ x \in \{a\} \iff x \in b$ ou encore $\forall x,\ x = a \iff x = b$. Spécialiser en $x \leftarrow a$ et invoquer la réflxeité $a = a$ donne $a = b$.

Montée vers l'infini ou ...descente aux enfers.

En itérant l'opération "associer à un ensemble a le singleton $\{a\}$", on peut forme un nombre usuel aussi grand que voulu d'ensemble différents ; mais la sont-il vraiment ? Peut-on déjà avoir $a = \{a\}$? Si c'est le cas, en itérant cette égalité on aurait $a = \{a\} = \{\{a\}\} = \{\{\{a\}\}\} = \cdots$ et l'on aurait pas de raison d'arêter cette descente infernale. L'*axiome de fondation* nous assurera que cette creusée dans les entrailles de a s'arretera au bout d'un nombre fini d'étapes (on finit par tomber sur des fondations). Alors, on aura construit une suite d'ensembles en nombre usuel aussi grand que souhaité, ce qui donne une première idée pour représenter les entiers usuels dans les ensembles.

6.3 Le retour de l'extensinalité

EXO (singleton et extensionalité). *L'axiome d'extensionalité équivaut à l'un des énoncés suivants :*

$$a \in E \implies \{a\} \subset E \qquad a \in E \iff \{a\} \subset E$$

Dem

imp=>équi écrire $a \in \{a\} \subset E$.

Ext=>implication Fixons un $a \in E$. Alors $x \in \{a\}$ donne $x = a$, d'où (car $a \in E$ et extensinalité) $x \in E$, ce qui montre $\{a\} \subset E$.

équi=>ext . Supposons $a = b$. La conclusion $a \in X \overset{?}{\iff} b \in X$ se réécrit $\{a\} \subset X \overset{?}{\iff} \{b\} \subset X$, or on a montré la double inclusion $\{a\} \supset\subset \{b\}$ (sans extension !) et la transitité de $\subset$ fait le reste.

cor (carac des singletons) *Un ensemble S est un signleton ssi $\exists a \in S,\ \forall b \in S,\ a = b$*

DEM on a les équivalces

$$\begin{aligned} & \exists a \in && S,\ \forall b \in S,\ a = b \\ \iff\ & \exists a,\ a \in && S \text{ et } \forall b \in S,\ b \in \{a\} \\ \iff\ & \exists a,\ \{a\} \subset && S \text{ et } S \subset \{a\} \\ \iff\ & \exists a,\ \{a\} = && S. \end{aligned}$$

7 Axiomes de l'union

Union = réunion des éléments : $\cup A = \bigcup_{a \in A} a$

envie très naturelle de réunion de "famille" (A_i) –> il faudra remplacement (car on a pas encore l"ensemble $\{A_i\}_{i \in I}$)

7.1 Union d'un ensemble

Étant donné un ensemble, on peut vider tous ses éléments dans un même sac :

$$\forall A,\ \exists\, (\cup A)\,,\ [x \in \cup A \iff (\exists a \in A,\ x \in a)]\,.$$

$\cup A$ est appelée ***union*** de A ; il s'agit de l'ensemble des éléments *des éléments* de A. Par exemple :

$$\begin{aligned} \cup \{\{a\}\} &= \{a\}\,, \\ \cup \{\{a\}, \{b\}\} &= \{a, b\}\,, \\ \cup \emptyset &= \emptyset. \end{aligned}$$

De manière plus informelle, si A est le coffre de votre voiture rempli de sac de courses, l'union de A va être l'ensemble des courses (on vide les éléments du coffre puis on rassemble les courses ainsi privées de leurs sacs respectifs).

EXO Vider les courses des coffres de votre voiture et de votre camion revient à vider les courses du premier et à vider celles du second :

$$\cup (a \cup b) = (\cup a) \cup (\cup b) .$$

union est axiome de *création "interne"* qui permet de regarder "à l'intérieur" d'un ensemble.
c'est un axiome de création *verticale* descendante (partie créé horizontale ascendant)
(Cette descente "interne" sera limité par l'axiome de fondation)

7.2 Sur le choix d'un unique élément vérifiant une propriété donnée

L'axiome de l'union permet d'exhiber l'unique élément vérifiant une propriété P donnée – sous réserve que l'on ait montré ses existence et unicité, bien sûr. En effet, notons a_0 un tel élément où P est à argument libre dans A. L'axiome de séparation assure l'existence de l'ensemble $\{a \in A \ ; \ P(a)\}$, lequel contient a_0 et uniquement a_0 ; il est par conséquent réduit au singleton $\{a_0\}$ (l'inclusion $\subset$ traduit l'unicité et celle $\supset$ l'existence), ce qui permet d'écrire

$$a_0 = \cup \{a \in A \ ; \ P(a)\} .$$

BOF : on a remplacé le $\iota_x P(x)$ de Hilbert par $\cup$, et seulmenet les $\iota_x P(x)$ *bornés...* COmment par exemple désigner l'union d'un ensemble sans ι_x ? ? ?

7.3 Ensembles décrits par extension, ordre et répétitions

On *montre l'existence d'un ensemble* $\{a, b, c, ..., z\}$ *contenant exactement une h-suite d'ensembles* $a, b, c, ..., z$ *donnés :*

$$\forall a, b, ..., z, \ \exists \{a, b, , ..., z\} , \ [\xi \in \{a, b, ..., z\}] \iff [\xi = a \text{ ou } \xi = b \text{ ... ou } \xi = z] .$$

Observer pour cela que les axiomes de la paire et de l'union donnent existence successivement aux ensembles

$$\begin{aligned} \cup \{\{a, b\}, \{c\}\} &= \{a, b, c\} \\ \cup \{\{a, b, c\}, \{d\}\} &= \{a, b, c, d\} \\ \cup \{\{a, b, c, d\}, \{e\}\} &= \{a, b, c, d, e\} \\ \cup \{\{a, b, c, d, e\}, \{f\}\} &= \{a, b, c, d, e, f\} \\ &\cdots \ . \end{aligned}$$

Lorsqu'on décrit un ensemble A de la sorte $\{a, b, ..., z\}$ en « étendant » tous ses éléments comme sur une corde à linge, on dit que l'on décrit A ***par extension***.
(*EXO : autre preuve via remplacement)*
Par exemple, on pourra réécrire l'ensemble vide sous la forme

$$\emptyset = \{\} .$$

D'ailleurs, lorsque le nombre d'arguments dans $\forall a, b, ..., z$ est nul, la disjonction devient le neutre pour $\vee$, çàd l'absurde $\perp$, et l'on obtient

$$\exists \{\} , \ [\xi \in \{\}] \iff \perp$$

Répétitions & ordre. Il ne sert à rien de

1. *répêter* un même a (c'est la tautologie $p \vee p \vee \cdots \vee p \iff p$) –> *les ensembles ne voient pas les répétitions*

$$\{a, a, ..., a\} = \{a\}$$

2. *permuter* des élemnts (c'est la tautolgoies corresepndante avec les $\vee$) –> *les ensembles ne voient pas l'ordre*

$$\{a,b,c,d,e\} = \{e,d,c,b,a\} = \{c,d,b,e,a\} = \{a,d,c,b,e\} = \cdots$$

Ainsi, on pourr simplfier

$$\{a,b,b,b,c,a,c,c,a,c,b,a,a,b,c\} = \{a,b,c\}$$

Le point des répéitions est important : étant donné un ensemble A et un autre ensemble a, on peut se demander « Est-ce que a est dans A ? », mais pas « Combien de fois a apparaît-il dans A ? » : *l'ensemble a est dans A ou pas, point.* ? ? ? et l'ordre ? ? ? "est-ce que a est avant / après b ? ? ? ?

L'expérience montre que l'on peut très bien se passer des « multiplicités » des éléments d'un ensemble, de même que l'ordre[4].

La question est légitime : pourquoi empecher de distinguer des choses dont on peut avoir beosin ? D'une part parce qu'on peut les recréer à partir de cela[5], d'autre part car on a rarement envie de considérer les éléments $\left\{x^2 \ ; \ -1 \leq x \leq 2\right\}$ avec différentes multiplicités[6].

On dira qu'un ensemble A a ν éléments (ou ν désigne un nombe usuel) si l'on peut écrire

$$A = \{a,b,c,...,z\}$$

où les ensembles $a,b,c...,z$ sont en nombre ν et deux à deux différents.

7.4 Quantificatation finie et entiers usuels

Le h-théorème de substitution permis par extensionnalité va nous permettre d'établir l'interprétation usuelle des quantificateurs sur les ensembles décrits par extension (possèdant un h-nombre fini d'éléments).

Proposition (quantification finie). *Pour chaque 1-prédicat P , on a les deux équivalences*

$$\begin{array}{lll} \forall a,b,c,...,z, \ [\exists \xi \in \{a,b,...,z\}, P(\xi)] & \iff & [P(a) \vee P(b) \vee \cdots \vee P(z)] \\ \forall a,b,c,...,z, \ [\forall \xi \in \{a,b,...,z\}, P(\xi)] & \iff & [P(a) \wedge P(b) \wedge \cdots \wedge P(z)] \end{array}$$

Démonstration. Regardons pour simplifier le cas de deux variables.

Remarquer que le second énoncé se déduit du premier par contraposée en ppliqaunt à $\neg P$:

$$\neg [\exists \xi \in \{a,b\}, \ \neg P(\xi)] \iff \ \neg [\neg P(a) \vee \ \neg P(b)]$$

qui se réécrit avec les bonnes tautologies

$$\forall \xi \in \{a,b\}, \ P(\xi) \iff \ P(a) \wedge P(b), \text{ CQFD.}$$

Montrons le premier énoncé.

On invoque a,b tels que $\exists \xi \in \{a,b\}, P(\xi)$. On peut donc invoquer un tel ξ. Il appartient à la paire $\{a,b\}$, d'où $(\xi = a) \vee (\xi = b)$. Or on a $P(\xi)$, d'où (par tautologie) la disjonteion $[P(\xi) \wedge (\xi = a)] \vee [P(\xi) \wedge (\xi = b)]$. On utilsier alors la règle déduite du h-théorème[7] de substitution pour obtenir $[P(\xi) \wedge (\xi = a)] \implies P(a)$, de même pour b, d'où (d'après tautologie adéquate) $P(a) \vee P(b)$.

Invoquons réciproquement a,b tels que $\neg (\exists \xi \in \{a,b\}, P(\xi))$, ie $\forall \xi \in \{a,b\}, \neg P(\xi)$. On spécialise en les termes a et b, d'où $\neg P(a)$ et $\neg P(b)$, d'où l'on infère $\neg P(a) \wedge \ \neg P(b)$, ie $\neg (P(a) \vee P(b))$.

---

[4] Cela dit, si l'on veut vraiment introduire des multiplicités, on peut le faire en considérant des ***familles*** (qui autorisent donc les répétitions) *modulo réindexation* (parce qu'on se fiche de l'ordre dans un ensemble. On parle alors de ***multi-ensembles***.

Par exemple, le multi-ensemble des racines d'un polynôme complexe de degré n est un élément de ${}^{\mathbb{C}^n}\!/_{\mathsf{S}_n}$.

[5] Nous verrons plus tard les ***multi-ensembles*** qui permettent de tenir compte des éventuelles multiplicités.

[6] Toutefois, lorsque que l'on fait de l'algèbre avancée, on aime bien qu'un polynôme de degré n ait exactement n racines, même le monôme X^n (qui ne s'annule qu'en 0). Les *schémas* sont un outil permettant de tenir compte de cette différence entre l'"ensemble" des racines de X et celui de celles de X^2. Alexandre Grotendieck, en créant les schémas autour de 1960, a révolutionné la *géométrie algébrique*.

[7] On pourrait tiquer d'invoquer un h-théorème dans une (pas de h)-preuve – mais nous n'en n'utilisons qu'une *règle*.

7.5 Réunion d'un nombre usuel d'ensembles

Ensuite, on définit la ***réunion*** (ou l'***union***) de deux ensembles :

$$\forall A, B,\ \exists (A \cup B),\ [x \in A \cup B] \iff [x \in A \text{ ou } x \in B].$$

Il suffit de poser $A \cup B := \cup \{\{A\}, \{B\}\}$. On récupère donc les éléments de A, les éléments de B, et on les met ensemble. On a

$$\forall x,\ [x \in A \cup B] \iff [(x \in A) \vee (x \in B)].$$

De même, on définirait $A \cup B \cup \cdots \cup Z := \cup \{\{A\}, \{B\}, ..., \{Z\}\}$ qui est caractérisé par

$$\forall x,\ [x \in A \cup B \cup \cdots \cup Z] \iff [(x \in A) \vee (x \in B) \vee \cdots \vee (x \in Z)].$$

(noter la ressemblance graphique entre les symboles $\cup$ et $\vee$).

On pourrait appeler $\{a, b, c\}$ un ***trio***, $\{a, b, c, d\}$ un ***quatuor***... (mais que dire d'un ***duo*** ?)

8 Axiomes des parties

pas prouvable par les autres :

il a été démontré que la théorie ZF privée de l'axiome de l'ensemble des parties admet une interprétation dans la théorie Z privée de cet axiome (source *http ://fr.wikipedia.org/wiki/Axiome_de_l%27ensemble_des_parties*, plus précisément *V. G. Kanovei, Matematicheskie Zametki, Vol. 30, N° 3, pp. 407-419, septembre 1981 ; publi en anglais par Springer*)

EXO *les ensembles Adont la cloture transitive* $\bigcup_{n \in \mathbf{N}} \cup^{\circ n} A$ *est bornée par un cardinal infini* (eg les esebmels héréditairement au plus dénombrable) *sont modèles de ZFC privé de partie* ; donc équiconsistant

C'est un axiome de *compréension* non borné !

Parie est un axiome de *création externe*, qui augement brutlamenet la taille (comme on le voit sur les ensmble finis où n devient 2^n). On pourrait parler de création *verticale* (ascendante).

Contrairement à union, pas de limitation à l'ascension verticale. Au contraire, on pourra se donner des "palliers" avec les axiomes de l'infini & grands cardinaux.

8.1 Ensemble des parties (d'un ensemble donné)

Étant donné un ensemble, on peut mettre ses parties dans un même sac :

$$\forall A,\ \exists \mathfrak{P}(A),\ [P \in \mathfrak{P}(A) \iff P \subset A].$$

$\mathfrak{P}(A)$ est appelé ***ensemble des parties*** de A. Par exemple :

$$\begin{aligned} \mathfrak{P}(\emptyset) &= \{\emptyset\} \\ \mathfrak{P}(\{a, b\}) &= \{\emptyset, \{a\}, \{b\}, \{a, b\}\}. \end{aligned}$$

En d'autres termes, *la classe des parties d'un ensemble donné est un ensemble.*

8.2 Le paradoxe de Rusell

Parties et séparation permettent de faire tomber le ***paradoxe de Russell*** : il n'y a pas d'ensemble de tous les ensembles. Sinon, on peut définir une surjection $\Omega \twoheadrightarrow P(\Omega)$ par l'identité sur $P(\Omega)$ et Ω ailleurs, mais alors la partie $A = \{\omega \in \Omega,\ \omega \notin s(\omega)\}$ est fixé par s et on a les équivalences $A \in A \iff A \notin s(A) = A$, ce qui est problématique...

(L'idée est que prendre l'ensemble des parties grossit beaucoup beacoup un ensemble (on montrera que $|P(A)| = 2^{|A|}$). Ainsi, si Ω convient, il doit contenir ses parties, d'où une injection de $P(\Omega)$ dans Ω, ce qui fournit en retour un surjection s de Ω sur $P(\Omega)$)[8]

EXO : *mq P ne fixe personne.* Si $A = \mathfrak{P}(A)$, alors (séparation) la partie $@ := \{a \in A\ ;\ a \notin a\}$ vérifie $\forall a \in A,\ a \in @ \iff a \notin a$, d'où contradc en spécialisant $a \leftarrow @$.

[8] pour l'histoire, le moines qui recensait les livres ne se mentionnant pas –> livre pas comme les autres ...

8.3 Union et parties sont dans un bateau

Noter que $\mathfrak{P}$ et $\cup$ agissent d'une certaine manière en sens contraire. $\mathfrak{P}$ « monte » en rajoutant une accolade tandis que $\cup$ « descend » en retirant une accolade. On a en particulier pour chaque ensemble A

$$\cup\mathfrak{P}(A) = A \subset \mathfrak{P}(\cup A)$$

avec $=$ dans l'inclusion de droite ssi A peut s'écrire $\mathfrak{P}(E)$ pour un ensemble E (pourquoi ?)

EXO *: montrer que sont distincts les ensmbles* $\emptyset$, $\mathfrak{P}(\emptyset)$, $\mathfrak{P}\mathfrak{P}(\emptyset)$, $\mathfrak{P}\mathfrak{P}\mathfrak{P}(\emptyset)$, $\mathfrak{P}\mathfrak{P}\mathfrak{P}\mathfrak{P}(\emptyset)$...

DEM : suppo $\mathfrak{P}^n(\emptyset) = \emptyset$. Si $n > 0$, alors $\mathfrak{P}^n(\emptyset)$ est de laforme $\mathfrak{P}(?)$ donc contient au moins un élment, ce qui est absurde. Supp à présent $\mathfrak{P}^a(\emptyset) = \mathfrak{P}^b(\emptyset)$ avec $a \leq b$. Appliquer $\cup^a$ donne $\emptyset = \mathfrak{P}^{b-a}(\emptyset)$, d'où $a = b$.

EXO : *mq* $\mathfrak{P}^a(E) = \mathfrak{P}^b(F) \iff \binom{E}{a} = \binom{F}{b}$

8.4 Paire, parties et fonctions

codage d'application par couples $\langle a, b\rangle \subset \mathfrak{P}\mathfrak{P}(\{a, b\}) \subset \mathfrak{P}^3(a \cup b)$, graphes $G \subset A * B \in \mathfrak{P}^3(A \cup B)$, d'où $\left\langle {}^{\langle A,B\rangle}_{G} \right\rangle \subset \mathfrak{P}^3(\langle A, B\rangle \cup G) \subset \mathfrak{P}^6(\langle\langle A, B\rangle \cup G\rangle)$ et $B^A \subset \mathfrak{P}^8(A \cup B)$. Interprétation : parties et séparation permettent de récupérer dans $\mathfrak{P}^8(A \cup B)$ les fonctions de A vers B. Puisque partie revient à se donner 2^E,

la morale de l'histoire est que les fonctions sont "engendrées" par les fonctions caractérisqtique.

Formalisons dans exo suivant.

EXO *: montrons que l'axiome partie/fonctionnel suivant (où on représente une partie par son graphe) implique l'axiome plus général*

$$\begin{aligned} \forall A,\ \exists 2^A,\ G \ \in\ 2^A &\iff [(c \in G) \iff (\exists a \in A,\ c = \langle a, 0\rangle \text{ ou } c = \langle a, 1\rangle)] \\ \forall A, B,\ \exists B^A,\ G \ \in\ B^A &\iff [(c \in G) \iff (\exists a \in A,\ \exists b \in B,\ c = \langle a, b\rangle)] \end{aligned}$$

Un tel 2^A est donc unique. A un tel G on associe par séparation

$$P_G := \{a \in A, \langle a, 1\rangle \in G\}.$$

REmplacement donnc un $P(A) = \{P_G\}_{G \in 2^A}$. Montrons que $P(A)$ satisfait axiome parties.

Clair que $P \in P(A) \implies P \subset A$. Soit réciproqmuet $O \subset A$. On associe à $a \in A$ le couple $\langle a, 1\rangle$ si $a \in A$ et $\langle a, 0\rangle$ sinon. Alors remplacement nous donne un grphe G_P tel que

$$c \in G_P \iff \exists a \in A,\ (c = \langle a, 1\rangle \,\text{et} a \in P)\, ou\, (c = \langle a, 0\rangle \,\text{et} a \notin P).$$

Montrons $P = P_{G_P}$. Soit $p \in A$. Alors $p \in P_{G_P}$ ssi $\langle p, 1\rangle \in G_P$ ssi[9] $\exists a \in A,\ (\langle p, 1\rangle = \langle a, 1\rangle \,\text{et} a \in P)$ ssi $\exists a \in A,\ (p = a \text{et} a \in P)$ ssi $p \in P$, CQFD.

9 Axiome de l'infini

Jusqu'alors, on ne peut pas modéliser des éléments infini (car on a un modèle $\mathbb{N}$, cf plus loin ; ou encore V_ω). On va rajouter un axiome pour ça, d'où système de Zermelo Z (sans infin, on notera Z_*)

Zermelo l'appelait *axiome de Dedekind* (source : *La création des nombres* H. Sinaceur, Vrin)

Idée : entiers code notre *action*. Selon cette optique, on choisit de coder chaque entier usuel n par le n-itéré d'une fonctinnelle σ appliquée sur un objet o de départ : $\sigma(o)$ code 1, $\sigma(\sigma(o))$ code 2, $\sigma(\sigma(\sigma(o)))$ code 3, ... $\sigma^n(o)$ code n, o code 0. La notation σ vient de **s***uccesseur* : $\sigma(\widetilde{n})$ code l'entier suivant n. Afin que le codage soit *fidèle*, il faut éviter les boucles, donc agréable que σ soit injective et n'atteint pas o (vérif alors que $\sigma^a(o) = \sigma^b(o) \overset{\text{inj}}{\Longrightarrow} o = \sigma^{b-a}(o) \overset{o \notin \text{Im}\,\sigma}{\Longrightarrow} a = b$ pour tous h-entiers a et b). Pour continuer aussi loin que voulu, il est sympa que σ soit PARTOUT DEFENIE.

Même si aussi loin q voulu, action limitée : on a un ensemble $\left\{\widetilde{0}, \widetilde{1}, \widetilde{2}, ..., \widetilde{n}\right\}$ qui code une action limitée à l'avance, jusqu'à chaque hnaturel n.

[9] on a nié ici l'égalité $\langle a, 0\rangle = \langle a, 1\rangle$, pour le faire proprement OPS $a \neq 0$, ainsi $\{a, 0\} \not\subset \{a\}$ donc de l'appartenance $\{a, 0\} \in \langle a, 1\rangle$ on déduit $0 \in \{a, 0\} = \{a, 1\}$ abusrde.

Pb action illimité <–> pas d'obstcle à l'action <-> on peut toujours agir. Toujours selon cette optique, on code l'infini par un ensemble stable par σ (et contenant o) :

$$\exists I,\ [o \in I] \text{ et } [i \in I \implies s(i) \in I]$$

Voir DM pour disctuer du choix de l'action : l'axiome usuel (à venir) rend techniquement plus agréable la voie vers les ordinaux (l'ordre d'exprime direcement dans le langage ensembliste) mais vaut autant que les autres pour ce qui est de modéliser l'infini.

Autre idée : **axiomeS d'itération** –> se donner un plus petit ensemble stabme contenant un départ, à savoir (cf Frege pour qui **N** est lensemble des objets tombant sous chaque propriété héréditaire) l'ensemble des n appartenant à tous les S contnent o et stables par σ (en fait, c'est directement écrire l'intersection des "infinis" lâches !) :

$$\begin{aligned} Itérat_o^\sigma &: \equiv \maltese_n \left[\forall S, \left\{ \begin{array}{c} o \in S \\ \forall s \in S,\ s' \in S \end{array} \right. \implies n \in S\right] \\ Itérat^\sigma &: \equiv \forall o,\ Itérat_o^\sigma \,?\,?\,?\,?\,? \end{aligned}$$

AxiomeS de l'infini :

$$\forall o, \left\{ \begin{array}{l} \sigma \text{ "injective"} \\ \nexists a,\ o = \sigma(a) \end{array} \right. \implies Itérat_o^\sigma$$

9.1 Successeur (d'un ensemble donné)

Exemple de $\sigma : a \mapsto \{a\}$: On a vu comment engendrer avec la paire une suite d'ensembles, chacun étant le singleton contenant le précédent, composée d'un nombre usuel d'objets aussi grand que voulu (grace à fondation). Pour des raisons de commodité technique, on code la montée vers l'infini en rajoutant à chaque étape, au lieu d'une paire d'accolade (comme pour $a \mapsto \{a\}$), un élément. Après un ensemlbe a vient donc quelque chose de la forme $a \cup \{?\}$. Pour s'assurer que ce dernier un ensemble *différent* de a, on choisit un élément $? \notin a$, par exemple $? = a$ (l'axiome de fondation assurera que $a \notin a$). Cela motive la définiton suivante.

On définit le ***successeur*** d'un ensemble par

$$s(a) := a \cup \{a\}$$

et on note $\widetilde{n} := s^n(\emptyset)$ avec la convention $\widetilde{0} = \emptyset$ pour chaque entier usuel n. On observera sur les premiers entiers la relation[10]

$$\widetilde{n+1} = \left\{\widetilde{0}, \widetilde{1}, ..., \widetilde{n}\right\}.$$

On a envie de considérer l'ensemble de ces entiers (qui ensemblistement serait leur réunion au vu de l'égalité ci-dessus), mais rien de garantit son existence.

9.2 Le "plus petit" ensemble infini $\mathbb{N}$, de départ $\emptyset$ et successeur s

D'où l'axiome

$$\exists S,\ [\emptyset \in S] \text{ et } [a \in S \implies s(a) \in S].$$

garantissant l'existence d'un ensemble S stable par sucesseur. En en prenant un minimal (il suffira de prendre l'intersection de ces tels ensembles dans l'un d'entre eux), on obtient l'ensemble $\mathbb{N}$ des entiers naturels. Ce dernier contient fidèlement chaque entier usuel : rien ne assure qu'il n'y rien d'autre.

Rq : l'idée de infini est : entiers code notre *action*. Action illimité <–> pas d'obstcle à l'action <-> on peut toujours agir. On code donc l'infini par un ensemble stable par une action (et contenant un point de départ).

De ce point de vue, le point de départ $\emptyset$ et l'action s ne jouent aucun rôle particulier : on aurait pu prendre n'importe quel point de départ o et n'importe quelle fonctionnelle σ, pourvu qu'elle atteigne pas o (pour éviter un cercle) et soit injective (pour éviter une boucle après o). On retrouve le th de réc, les segments finis, les suites récurrentes, l'addition, l'ordre...

cf DM

Cette construction rend quasi-tautologque le principe de récurrence ; en d'autres termes, le principe de récurrence *définit* les entiers naturels.

[10] Relation qui ne peut s'écrire à l'aide d'un $\forall n \in \mathbb{N}$ puisque le $\mathbb{N}$ en question n'est pas encore défini.

9.3 La récurrence : induction par successeur partant de 0

Théorème (réccurence).
Pour chaque 1-prédicat P, on a le théorème

$$(P(0) \wedge [\forall n \in \mathbb{N},\ P(n) \implies P(s(n))]) \implies (\forall n \in \mathbb{N},\ P(n)).$$

Démonstration.
On sépare la partie $\{n \in \mathbb{N}\ ;\ P(n)\}$. Il contient 0 et est stable par successeur, donc il contient $\mathbb{N}$, donc lui est égal.

Autre formulation, dite récurrence forte (mais parfaitement équivalente)

$$(P(0) \wedge [\forall n \in \mathbb{N},\ (\forall k < n, P(k)) \implies P(n)]) \implies (\forall n \in \mathbb{N},\ P(n))$$

(les hypothèses et conclusions sont plus fortes, d'où plus d'hytpohèse à dispositin mais plus de choses à montrer)

heursitique : si existait un prédicat "être un h-entier" (mais alors on ne s'em...erait pas avec l'infini), on motnrerait alors par rec que chaque entier code bien un (unique) h-entier. Cela peut rassurer qu'on l'a bien rien d'autre que les h-entiers imiginables.

Mais pb techinque : considérons un entier a non primtif, esayons de le retirer : $N \setminus \{a\}$ contient bien 0 (car a n'est pas primiitf) mais est $s$stable ssi a n'est pas sucesseur. Il faudrait alors retirer les prédécesseurs de a, ce qui fournirait une partie $S \ni a$ stable par σ^{-1} : comment en exhiber une ? L'"axiome" de l'infini de départ a et fonctionnelle σ^{-1} en donnerait-elle une (même si elle boucle) ? Non car σ^{-1} pas définie partout... (imaginer même démo en remplaçant a par un h-nombre codé) ; poursuivons quand même. Soit S_a conenvant. Alors $N \setminus S$ est σstable et $\subsetneq N$, donc ne contient pas 0, donc on ne peut récurrer...

9.4 L'itération : caractérise l'infini

th 126, cf DM, dire que équivalent à itération + platitude

9.5 Le transfini : induction par successeur et récurrence (à partir de 0)

L'opération << successeur >> est plus que naturelle pour explorer le fini (au suivant !) (bien sûr le codage est discutable)

L'opératin << passer à la limite >> (permise par l'axiome de l'infini) est nécessaire si l'on veut pouvoir réaliser un premier infini ω. Que permet-elle de plus ?

Ensemble, ces deux opérations permettent de décrire inductivement la colonne vertébrale ordinale $\widetilde{\mathbb{O}}$:

$$0, 1, 2, ...\omega, \omega+1, \omega+2, ..., 2\omega, 2\omega+1, ..., 3\omega, 4\omega, ..., \omega^2, \omega^3, ..., \omega^\omega,\ \omega^{\omega^\omega}, ..., \omega^{\omega^{\omega^{\omega^{\cdots}}}} =: \varepsilon_0...$$

On peut décrire les ordinaux de manière directe par les ensembles bien ordonnés par $\in$ dont tous les éléments vallent leur segment initial strict associé. Un ordinal est ou bien nul, ou bien successeur, ou bien (par définition) ***limite***.

Les deux opérations permettent une induction transfinie lorsque le prédicat (initialisé en le premier ordinal 0) passe : d'une part au sucesseur (récurrence classique) d'autre part à la limite (passage à l'infini) :

$$(P(0) \wedge [\forall \alpha \text{ordinal},\ P(\alpha) \implies P(s(\alpha))] \wedge [\forall \lambda \text{ordinal limite},\ (\forall \alpha < \lambda, P(\lambda)) \implies P(\alpha)]) \implies (\forall \alpha \text{ordinal}, P(\alpha))$$

ce qui peut se réécrire (induction transfinie "forte") en

$$(P(0) \wedge [\forall \alpha \text{ordinal},\ (\forall o < \alpha, P(o)) \implies P(\alpha)]) \implies (\forall \alpha \text{ordinal}, P(\alpha)).$$

Nous insistons sur le cararctère naturel des ordinaux comme prolongement de la récurrence mettant en jeu le passage à l'infini (et rien d'autre !). Eg histoirique Cantor ? Eg colle fonction loc polynomiale ?

Bref, les ordinaux, c'est **bien**. Dans le même genre, pour faire de la topologie ensembliste, plutôt que de se faire ch*** à manipuler des filtres pour la convergence (« un espace topologique X est compact si et seulement si chaque ultrafiltre sur X a une limite [unique] »), il est largement plus clair de procéder avec des séquences ordinales **(« un espace topologique X est compact si et seulement si chaque séquence de points de X indexée par un ordinal limite** (ou, ce qui revient au même pour cette définition, par un cardinal régulier) **admet une valeur d'adhérence** »), ce qui se conforme plus à l'intuition qu'on se fait sur les espaces métriques. (De même, **une partie F d'un espace topologique E est fermée si et seulement si chaque séquence de points de F, indexée par un ordinal limite** (cardinal régulier)**, qui converge dans E, converge dans F**.).

(gros-tsen, 28 10 2001, 11H15)

En fait, *la défintion des fermés est fausse* :-) une partie F d'un espace topologique E est fermée si et seulement si chaque valeur d'adhérence dans E d'une séquence indicée par un ordinal limite (ou, ce qui revient au même dans le contexte, un cardinal régulier) de points de F, est dans F.

9.6 Des h-entiers vers les entiers naturels

Comment déduire les propositions énoncées précédemment sur les h-entiers (l'extension, la réunion, et l'intersection) ? deux pb :

1. sur quoi quantifier
2. comment prédiquer.

Pour faire proprement, on aimerait dire

$$\forall n,\ \forall \text{ "suite" de "taille" } n,\ \exists X,\ x \in X \iff (???)\,.$$

Pour la "suite", on peut dire "*a*suite de taile n" ssi "il y a un ensemble A tq $a \in A^{\underline{n}}$".

Mais alors le prédicat pose problème car comment donner sens à $(x = a_1) \vee (x = a_2) \vee ... \vee (x = a_n)$ lorque la strucutre me^me de la phrase logique (qui est censée être indépendante des symboles en jeu) dépend de l'entier n ? On contourne en disant $\exists i \in \underline{n},\ x = a_i$. Et on déjà vérifié que pour $a, b, ..., z$, la proposition $\exists i \in \{a, b...z\}, P(i)$ signifie bien $P(a) \vee P(b) \vee ... \vee P(z)$

10 Axiome de fondation

Prenons un ensemble A non vide. On peut y prendre un élément a. Si a est non vide, on peut regarder un élément α de a. Puis on peut recommencer tant que l'on atteint pas $\emptyset$. L'axiome de fondation affirme que ce procédé s'arrête toujours au bout d'un nombre fini d'étapes, *i.e.* qu'en zoomant successivement sur les éléments des éléments des éléments des..., on tombera toujours sur l'ensemble vide. En d'autres termes, lorsqu'on « creuse » dans un ensemble, on finit toujours par tomber sur une « fondation » (l'ensemble vide).

Fondation borne donc la création verticale *descendante* de union.

Fondation ne créé rien, il décrit : c'est juste un choix d'ensemble qu'on regarde.

Déjà, pour qu'on soit bien d'accord, l'« ***univers régulier*** » c'est la classe des éléments construite à partir du vide par itération transfinie (sur la classe des ordinaux) de l'ensemble des parties : i.e., un ensemble est ***régulier*** ssi il existe un ordinal α tel que $x \in \mathfrak{P}^{\alpha}(\emptyset)$. L'axiome de fondation dit exactement que (*l'univers régulier est l'univers*, i.e.) *chaque ensemble est régulier*.

Ensuite, ce que j'affirme c'est que chaque théorème de ZFC avec fondation est équivalent au même énoncé dans ZFC sans fondation en remplaçant tous les quantificateurs « $\forall x$ » et « $\exists x$ » (il suffit de le faire pour les quantificateurs non restreints) par les quantificateurs restreints à l'univers régulier : i.e., « $\forall x$ régulier » et « $\exists x$ régulier ». Bref, **poser l'axiome de fondation (=régularité) revient tout bêtement à dire « je ne m'intéresse qu'aux ensembles réguliers, les autres ne m'intéressent pas ».**

!!!! c'est le cas pour tous les axiomes !!! car tous sont de la forme $\forall a,\ P(a)$ où P est un enénoncé existentiel (de création, d'accord, par d'ordinaux déjà créés)

Enoncé propre : Soit $\mathcal{C}$ une classe. Si E est un énoncé ensembliste, on définit $E^{\mathcal{C}}$ par récurrence sur le nombre de quantif dans E, où l'on remplace Qa par $Qa \in \mathcal{C}$. EG : si E est $\forall a,\ a \in \mathcal{C}$, alors $E^{\mathcal{C}}$ est $\forall a \in \mathcal{C},\ a \in \mathcal{C}$, ce qui est vrai. Alors supposer $\forall a,\ a \in \mathcal{C}$ revient à supposer $E \iff E^{\mathcal{C}}$ pour chaque énoncé. => clair ; <= prendre pour E l'EG

10.1 La relation $\in$ est "bien fondée"

On le formule de manière indirecte :

$$\forall A \neq \emptyset,\ \exists a \in A,\ A \cap a = \emptyset.$$

On en déduit en particulier (prendre $A = \{x\}$)

$$\forall x,\ x \notin x.$$

(Plus généralement, pas de suites u décroissantes pour $\in$ (prendre $A = \operatorname{Im} u$), ni donc de $\in$-cycles). Cela résoud le paradoxe de Russel d'une manière plus directe : il n'y a pas d'ensemble de tous les ensembles, sinon ce dernier devrait s'appartenir (bon, on peut se passer de fondation pour résoudre Russel, hein, un séparation suffit...).

Montrons la réciproque (avec AC). Soit $A \neq \emptyset$ tel que $\forall a \in A,\ \exists x \in A \cap a$. AC nous donne une application $f : A \longrightarrow A$ telle que $\forall a \in A,\ f(a) \in a$. Soit $\alpha \in A$. Alors la suite $n \mapsto f^{\circ n}(\alpha)$ décroît strictement pour $\in$.

10.2 Univers de Von Neumann & axiome de régularité

L'axiome de fondation permet de montrer que chaque ensemble peut s'obtenir de la manière suivante. On part de l'ensemble vide $\emptyset$, que nous noterons V_0, puis on prend son ensemble des parties $\{\emptyset\}$, noté V_1, puis on pose de proche en proche $V_{n+1} = \mathfrak{P}(V_n)$. Pour continuer, en notant ω l'ensemble $\mathbb{N}$ des entiers naturels, on pose $V_\omega = \bigcup_{n\in\omega} V_n$ puis de proche en proche $V_{\omega+n+1} = \mathfrak{P}(V_{\omega+n})$. Et ainsi de suite. La théorie des ordinaux (donc nous ne parlerons pas ici) permet d'assurer l'existence d'une telle suite (V_α) où α décrit les ordinaux, et l'axiome de fondation peut alors s'écrire

$$\forall x,\ \exists \alpha \text{ ordinal},\ x \in V_\alpha.$$

(axiome du à Von Neumann, quand il travaillait sur les ordinaux, d'où la lettre V)

application rigolote (mouais, en fait c'est juste dire que chaque $\in$ordre est toujours *bon* ordre) de fondation : *Montrons que chaque partie non vide de N admet un min* Soit A une telle partie (définissable au premier ordre). Intuitivement, il s'agit de prendre le plus petit entier de A, donc celui qui est le moins sophistiqué niveau construction. L'axiome de fondation (appliqué à $A \neq \emptyset$) nous donne un tel $a_0 \in A$ vérifiant plus précisément $A \cap a_0 = \emptyset$. Montrons que $a_0 = \min A$. Soit par l'absurde un élément $a \in A$ tel que $a < a_0$, *i. e.* $a \in a_0$, ce qui impose $a \in A \cap a_0$, *absurde.*

11 Axiomes de remplacement

(on dit aussi ***axiomes de substitution***)

On appelle ***relation fonctionnelle*** sur un ensemble A un 2-prédicat f tel que

$$\forall a \in A,\ \forall b, b',\ [f(a,b) \text{ et } f(a,b')] \implies (b = b').$$

La notation $f(a,b)$ est à comprendre intuitivement comme « b est l'image de a par une fonction f ».

Résumé :remplacement <=> existence $\{A_i\}$ <=> existence (A_i) <=> exsitence $\prod A_i$,

11.1 Remplacement des éléments du domaine d'une fonctionnelle par leur image

Pour chaque relation fonctionnelle f sur un ensemble A :

$$\exists B,\ \forall b,\ [b \in B \iff \exists a \in A,\ f(a,b)]\,.$$

En d'autres termes, la classe des b tels que $[\exists a \in A,\ f(a,b)]$ est un ensemble.

B est intuitivement l'ensemble des images (quand elles existent) des $a \in A$ par f. On peut d'ailleurs définir une fonction de A vers B qui à un $a \in A$ associe l'unique $b \in B$ (s'il existe) tel que $f(a,b)$. Une telle fonction f est unique en vertu de l'équivalence

$$f(a,b) \iff f(a) = b.$$

Les axiomes de remplacement disent donc que l'image d'un ensemble par une « fonction » est encore un ensemble :

$$\left[\forall a \in A,\ \exists^{\leq 1} b,\ f(a,b)\right] \implies (\exists B,\ \forall b,\ [b \in B \iff \exists a \in A,\ f(a,b)])\,.$$

On en déduit une *fonction* $F : \left\{ \begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & \text{le } b \text{ tel que } f(a,b) \end{array} \right|$. En d'autres termes, en *remplaçant* dans A chaque élément par son image, on obtient encore un ensemble.

C'est donc un aximoe de *création* à l'aide de fonctionnelles. Il n'aument pas la taille, donc on pourarit aprler de création *horizatale*.

Remplacement est *création horizontale*. Visualier une figure dans le plan (=ensemble), on lui appliquer une translation (=fonctionnell), on obtient une autre figure dans le mêem plan.

Couplé à union et partie, il devient *création verticale* monstrueuse : EG $\bigcup_{n\in\mathbf{N}} \mathfrak{P}^n(\emptyset)$ et plus générlaemnet les V_α.

RQ : $V_{\omega+\omega}$ est modèle de ZF sans remplacment, donc on a besoin de remplcament pour grimpsr dans les V_α (sinon on bloque pour considérer $\bigcup_{n\in\mathbf{N}} V_{\omega+n}$)

introduit par Fraenkel (d'où le Z dans ZFC) & Skolem (indépendamment), c'est surtout VN qui en a remarqué l'intérêt dans la théorie des ordinaux (citer Michael Halett *Cantorian set theory dans limitations of size*)

À part pour un détail technique dans le théorème de comparaison des ordinaux, on ne l'utilsera cependant guère.

Vraie résultat mathématique usilisnt remplacment : le theoreme de Martin affirmant que chaque sous-ensemble borelien de $\mathbf{R}$ est determiné, ce qui veut dire que certains jeux (de complexite borelienne) ont des strategies gagnantes : la, on sait montrer que, sans remplacement, le resultat ne peut pas etre demontré (et pas seulement qu'on ne sait pas le demontrer, mais qu'on saura peut-etre un jour).

11.2 Remplacement, séparation, extensionalité

TRES PUISSANT car il implique d'autres axiomes (mais n'augement pas la taille, contrairement à parties ou union).

rempl=> sépartatoin : (morale : on prend une fonction sur A de deomaine A' agisant comme l'identité) si $P(x)$ proposition, considérons la fonctionnelle $f(x,y) \iff ((x = y) \wedge P(x))$. Alors, étant donné un ensmble A, il y a un ensemle $B = \{b\ ;\ \exists a \in A,\ f(a,b)\} = \{a \in A\ ;\ P(a)\}$.

rempl+partie=> paire : (résumé : partie augement la taille jusqu'à ≥ 2, puis on peut remplacer deux élémetsn arbitraire par deux quelcoques) d'après paire, il y a un ensemble ni vide ni singleton, eg $X = \mathfrak{P}(\emptyset)$, dont qui contient deux éléments $i \neq j$, d'où la paire $\{i,j\} =: I := \{x \in X;\ x = i \vee x = j\}$, et on peut alors former n'importe quelle paire $\{a,b\}$: on définit $f(i,x) \iff x = a$ et $f(j,x) \iff y = b$. Alors $\forall i \in I,\ \exists! x,\ f(i,x)$, d'où un $\{a,b\}$

de même **rempl+parties => extens finie**

EXO : *montrer que remplacmeent équivaut à sépartion conjoint au même énoncé en remplacat* $\exists!$ *par* $\exists$

<= trivial

=> Soit A et f fonctionelle desus. On sépare le domaine de la relation $A' := \{a \in A\ ;\ \exists b,\ f(a,b)\}$. Alors on peut appliquer remalcement à A' : $\exists B,\ \forall b,\ [b \in B \iff \exists a \in A',\ f(a,b)]$. Or, à b fixé, il est équivalent de dire $\exists a \in A',\ f(a,b)$ ou $\exists a \in A,\ f(a,b)$, ce qui conclut.

EXO (**variante**) : *avec union&paire, mq remplacemet équiavaut à (pour chaque f relation fonctionnelle et chaque A ensemble)*

1. $\exists G$ *tel que* $\forall a \in A,\ \forall b,\ \langle a,b\rangle \in G$ *ssi* $f(a,b)$
2. $\exists F$fonction telle que $F(a) = b \iff f(a,b)$

DEM :
REP=>1 on définit une relation

$$C(a,c) \quad \overset{\text{def}}{\iff} \quad \exists b, c = \langle a,b\rangle \,\text{et} f(a,b)\,.$$

C'est fonctionnel (si $C(a,c)$ et $C(a,c')$, alors il y a b et b' tel que $f(a,b)$ et $f(a,b')$ d'où $b = b'$ et $c = \langle a,b\rangle = c'$), donc remplacement donnc un G tel que $c \in G$ ssi $\exists a \in A,\ C(a,c)$. Ainsi, si un couple $\langle x,y\rangle$ est dans G, il y a un $a \in A$ et un b tq $c = \langle a,b\rangle$ (d'où $a = x$ et $b = y$) et $f(a,b)$, d'où $f(x,y)$. Réciproque claire.

1=>2 on sépare dans $\cup\cup G$ les b tq $\exists a \in A, \langle a,b\rangle \in G$ puis on pose $F := \langle\langle A,B\rangle, G\rangle$, qui vérifie $F(a) = b$ssi $\langle a,b\rangle \in G$ ssi $f(a,b)$ CQFD

2=>REP On sépare l'image de l'application.

11.3 Remplacement et union

Hyper intuitif : il s'agit, à partir de $i \mapsto A_i$, de considérer la réunion $\bigcup_{i\in I} A_i$

EXO (**généralisation**) (l'appler l'axiome de *collecte/récolte* ? ? ?)
version **bourbaki** : pour chaque 2prédicat P

$$\forall A, \quad \begin{array}{c} \forall a \in A,\ \exists B,\ \forall b,\ (b \in B \iff P(a,b)) \\ \Longrightarrow \exists B,\ \forall b,\ (b \in B \iff \exists a \in A,\ P(a,b)) \end{array}$$

Lorsque P est univoque, on retrouve remplacement (d'où paire)
Lorsque P est $\ni$, spécialiser B en a donne union
R2ciproque : supposons union et rempl. Soit A tel que $\forall a \in A,\ \exists B,\ \forall b,\ (b \in B \iff P(a,b))$. On a donc une correcpondance unvooque $a \mapsto B_a$, d'où (rempl) un ensmble $\{B_a\ ;\ a \in A\}$, d'où (union) un $B := \bigcup_{a\in A} B_a$.

11.4 Remplacmenet et produit cartésien

Application. Si l'on dispose pour chaque indice $i \in I$ d'un ensemble a_i uniquement défini par une propriété $f(i,a_i)$, l'axiome de remplacement nous donne un ensemble $\{a_i\}_{i\in I}$, d'où l'on tire une famille (a_i).
Eg : si A ensemble, on peut considérer la réunion et la produit cartésien des A^n. (en fait, pour la réunion, pas besoin, il suffit de séparer dans $\text{Fonc}(\mathbb{N}, A)$ les fonctions dont le domaine est fini)
CP : pour $I \subset \mathbb{N}$ fini, on retrouve l'extendsionalité (ce qui est cohérent).

Réciproque (Remplcameent et produit cartésein) Soit A fonctionnelle et I un ensemble. Montrer que remplcament pour $\{A_i\}_{i\in I}$ équivaut à $\maltese_f (\forall c \in f,\ \exists i \in I,\ \exists a \in A_i,\ c = \langle i,a\rangle)$:

$$\exists P,\ \forall f,\ [f \in P \iff (\forall c \in f,\ \exists i \in I,\ \exists a \in A_i,\ c = \langle i,a\rangle)]$$

=> poser $P := \bigcup_{J\subset I} \prod_{j\in J} A_J$ (fonctions partielle sur $\prod_{i\in I} A_i$)
<= soit un tel P. Montrer que l'"ensemble des A_i" est

$$\mathcal{A} := \{A \in \mathfrak{P}(\cup\cup\cup P)\ ;\ \exists i \in I,\ \forall a,\ [a \in A \iff (\exists f \in P,\ \langle i,a\rangle \in f)]\}\,.$$

On montre donc $\forall A,\ [A \in \mathcal{A} \iff (\exists i \in I,\ A = A_i)]$.
=> Soit $A \in \mathcal{A}$. Soit $i \in I$ tq... Mq $A = A_i$
$\subset$ soit $a \in A$. Soit $f \in P$ tq $c := \langle i,a\rangle \in f$. Par déf de P, soit un $(j,b) \in I \times A_j$ tq $c = \langle j,b\rangle$. On en déduit $i = j$ d'où $a = b \in A_j = A_i$.
$\supset$ soit $a \in A_i$. Alors (par déf de P) on a $\{\langle i,a\rangle\} \in P$, donc (par déf de A) on a $a \in A$.
<= Soit $i \in I$. Mq $A_i \in \mathcal{A}$. Soit a. ON veut l'équivalence $a \in A_i \iff (\exists f \in P,\ \langle i,a\rangle \in f)$. Le sens => est clair car $\langle i,a\rangle \in P$. Pour <=, on part de $\exists f \in P,\ \langle i,a\rangle \in f$, çàd de $\exists f \ni \langle i,a\rangle$, $(\forall c \in f,\ \exists j \in I,\ \exists b \in A_j,\ c = \langle j,b\rangle)$ .Soit donc un tel f. Notons $c := \langle i,a\rangle$. Soient j,b tq $c = \langle j,b\rangle$. Alors $i = j$ et $a = b \in A_j = A_i$.

morale :
remplacement <=> exsitence $\prod A_i$,
AC <=> non vacuité $\prod$

11.5 Transition vers AC

Remplacement se formule $\left[\forall a \in A,\ \exists^{\leq 1} b,\ P(a,b)\right] \implies [\exists B, ...]$, d'où une fonction $\left\{ \begin{array}{ccc} A & \longmapsto & B \\ a & \longrightarrow & \text{un } b \text{ tq } P(a,b) \end{array} \right.$
(le "un" est un "le")

Question : on se donne un ensembble B, mais on remplace le "au plus" par un "au moin" dans lénoncé

$$\forall a \in A,\ \exists^{\geq 1} b \in B,\ P(a,b)\,.$$

Y a-til au moins une vraie application $\begin{array}{ccc} A & \longrightarrow & B \\ a & \longmapsto & \text{un } b \text{ tel que } P(a,b) \end{array}$? Une telle application est exactement un processus de *choix* d'un b tq... –> AC

12 Axiome du choix

L'axiome qui suit, controversé pour des raisons légitimes, peut venir se rajouter à ZF pour former ZFC (C comme choix).

hyper naturel : passer de "$\forall a \in A,\ \exists b,\ P_a^b$" à "$\exists$ **fonction** $f \in ?^A, \forall a,\ P_a^{f(a)}$" (d'ailleurs vision fonctionnelle amène changement logique –> hintikka, quantif indépendant...)

deux pb :
existance de l'*ensemble d'arriéve* (ce n'est pas le but de AC, mais remplacement aura un mot à jouer)
existence d'une *application* (voyons l'exmeple du dévelopement)

Pour développer $\bigwedge_{i\in I} \bigvee_{a\in A} P_i^a$ (où I et A **h-finis**) on choisi dans chaque disjonction (çàd pour chaque i) un P_i^a (çàd un a), on les conjoint et on disjoint sur tous les choix possibles (d'où $\bigvee_{a\in A^I} \bigwedge_{i\in I} P_i^{a_i}$)
AC va généraliser.

12.1 AC et interversion $\forall\exists$ (ou distrib généralisée $\wedge$ sur $\vee$)

Commment passer de « pour chaque tiroir, j'ai une chaussettes » à « j'ai une famille de chaussettes dont chacune appartient à un tiroir donné » ? Comment regrouper les chaussettes, les rasembler en une famille ?
En d'autres termes, les deux énoncés suivants sont-ils équivalents :

$$\begin{array}{rcl} \forall i & \in & I,\ \exists a \in A,\ P_i^a \\ \exists a & \in & A^I,\ \forall i \in I,\ P_i^{a_i} \end{array}$$

Naîvement, on ne fait que du fini, au mieux dénombralbe. VOICI AC!!!

AC n'est pas un axiome de création d'ensemble "*externe*" (comme remplacement) : il crée un ensemble dans un truc déjà créé (le produit cartésien), donc ne peut pas créer de la taille.

RQ (non AC) Quand on dit « il existe », tu n'as pas besoin de l'axiome du choix pour choisir l'objet. C'est une erreur assez commune. C'est juste un principe de logique : si $P(a) \implies Q$pour un certain a alors $\exists x, P(x) \implies Q$, c'est-à-dire que dès que tu as « $\exists x$» tu peux donner un nom, a, à l'objet en question

12.2 AC et remplacement

EXO (choix-remplacement) *Sous fondation&sepération, montrer que AC + REMP équivaut à*

$$\forall A,\ \left\{\begin{array}{l}\forall a\in A,\ \exists b,\ P_a^b \Longrightarrow\\ \exists b\in ?^A,\ \forall a\in A,\ P_a^{b_a}\end{array}\right.$$

=> Soit $a\in A$. Def α le plus petit ordainal tq V_α contienne un b tq $P(a,b)$. Remplacement nous donne alors la rénion de ces α_a, qui est un ordainl ; notons-le α. On a donc $\forall a\in A,\ \exists b\in V_\alpha,\ P(a,b)$, d'où (par AC) une fonction comme voulu.

<= Pour AC, def $Q(a,b)\Longleftrightarrow P(a,b)\wedge(b\in B)$.

Pour remplacement, suffit mq version $\exists!$ (car sépérat). Supp $\forall a\in A,\exists! b,\ P_a^b$, soit B et $b\in B^A$ tq $\forall a\in A,\ P_a^{b_a}$. Alors $\operatorname{Im} b$ (sensée par séprar) convient.

PB : de $\forall a\in A,\ \exists^{\geq 1}b,\ P(a,b)$, peut-on appliquer remplacement/AC pour avoir une image ? ? ? (sans fondation)

EXO : *mq, sous séparation/fondation, l'axiome suivant équivaut à REMP UNION AC :*

$$\forall A,\ \begin{array}{c}\forall a\in A,\quad \exists E,\quad P_a^E\\ \Longrightarrow \exists ?,\ \exists E\in\mathfrak{P}(?)^A,\ \forall a\in A,\ P_a^{E(a)}\end{array}$$

=> remp/AC (fondation) donne un $\mathcal{F}$ et un $E\in\mathcal{F}^A$ tq... Def $F:=\cup\mathcal{F}$. Alors $\mathcal{F}\subset\mathfrak{P}(F)$, d'où $\mathcal{F}^A\subset\mathfrak{P}(F)^A$.

<= mq UNION. Soit A. On applique en remplaàant E par a et en prenant pour prédicat P l'égalité. On sépare alors $U:=\left\{x\in F\ ;\ \exists a\begin{array}{l}\in A\\ \ni x\end{array}\right\}$. Puisque $a=E_a\subset F$, on a l'éq $x\in a\Longleftrightarrow\begin{array}{l}x\in a\\ x\in F\end{array}$, donc appartenir à U signifnie bien " $\exists a\begin{array}{l}\in A\\ \ni x\end{array}$ "

Mq REMP. On sépare dans A les a ayant une image. Soit $E\in P(F)$ tq... Alors $\operatorname{Im} E$ répond à la question.

Mq AC. Soit (E_i) non vides : $\forall i\in I,\ \exists x,\ x\in E_i$. Soit ? et un $x\in P(?)^I$ tq $\forall i\in I,\ x_i\in E_i$. Alors x induit un élément de $\prod E_i$.

rq exo ad hoc, énoncé ni joli, ni naturel, contrairement à AC+REMP

12.3 AC et produit cartésien

Soit I, soit $i\mapsto A_i$ une fonctionnelle. Notons A la réunion des A_i (ok par remplcament). Rappelos que $\prod A_i=\left\{a\in A^I\ ;\ \forall i\in I,\ a(i)\in A_i\right\}$

Mq que, sous remplacement, AC équivaut à "

$$\prod A_i=0 \text{ ssi } \exists i,\ A_i=0$$

(ce qui amena Russell à le baptiser ***"multiplicative axiom"***).

DEM

=> Suppo $\forall i\in I,\ A_i\neq\emptyset$, çàd $\forall i\in I,\ \exists a\in A,\ P(i,a)$ où $P(x,y)\Longleftrightarrow y\in A_x$. On a donc un $a\in A^I,\ \forall i\in I,\ P(i,a(i))$, çàd $a(i)\in A_i$, d'où $a\in\prod A_i$

<= Supp $\forall i\in I,\ \exists a\in A,\ P(i,a)$. Notons $A_i:=\{a\in A\ ;\ P(i,a)\}$. On a une fonctionnelle $i\mapsto A_i\neq\emptyset$, d'où une app $a\in\prod A_i$, çàd un $a\in A^I$ tq $\forall i\in I,\ a(i)\in A_i$, çàd tq $\forall i\in I,\ P(i,a(i))$ cqfd.

12.4 AC et fonction de choix

Tout le pb est sur le choix des images, plus précisément sur l'existence d'un *processus* de choix *global* (pas juste point par point). Le terme intuitif "processus global de choix des images" se formalise en *application*. D'où la reformulation :

EXO : mq éq ∃ fonction de choix :

$$\forall E,\ \forall \mathcal{A} \subset \mathfrak{P}(E) \setminus \{\emptyset\}\ ,\ \exists c \in E^{\mathcal{A}},\ \forall A \in \mathcal{A},\ c(A) \in A$$

DEM

$\Longrightarrow$ SOit E, soit $\mathcal{A}$ tq... Soit $A \in \mathcal{A}$: puisque $A \neq \emptyset$, on sait $\exists a \in A$, çàd $\exists a \in E,\ a \in A$. On a dcon $\forall A \in \mathcal{A},\ \exists a \in E,\ P(A,a)$ où P est $\ni$, d'où (AC) $\exists a \in E^{\mathcal{A}},\ \forall A \in \mathcal{A},\ P(A, a(A))$, CQFD

$<=$ SUpo $\forall x, \exists a$.... Notons $A_x := \{a \in A\ ;\ P(x,a)\}$ (qui est non vide) et $\mathcal{A} := \{A_x\ ;\ x \in X\} \subset \mathfrak{P}(A)$. SOit $c : \mathcal{A} \longrightarrow A$ une fonctoi de choix. Nontons $a : x \mapsto c(A_x)$. SOit $x \in X$. On a $c(A_x) \in A_x$, çàd $a_x \in A_x$, d'où $P(x, a_x)$.

12.5 AC et minima

EG : tous les ensmbles bien ordonnés ont une fonction de choix : le min.

EG : ensemble fini, **N**. Cela se propage : rationnel sont dénomb, donc il y a un bon ordre venant de celui de $\mathbb{N}$. (exo cor : il y a fonction de choix sur intervalles réels[11])

On peut montrer la $<=$ (cf DM ordinaux) : *A bien ordonnable ssi il ya une fonction de choix sur A.*

En d'autres termes, *un fonction de choix peut toujours être vue comme un min.*

12.6 AC et maximaux

De nombreux problèmes demandent des éléments maximaux pour un certain ordre : bases ev (libres max), idéal max (inclusion), prolongement de fonction (ordre est inclusion des domaines et restrcition), cloture algébrique, ultrafiltre... Très intuitif via les ordinaux : induction transfinie, aussi constructif que remplacer "il y a un plus petit stable par successeur" par "on récurre" (on rajoute juste l'étape ordinal limite).

Equivalence avec Zorn : passer par les ordinaux, c'est naturel !

Soit P un ensemble ordonné dans lequel chaque chaîne (partie totalement ordonnée) T admet un majorant. L'axiome du choix nous permet de choisir une fois pour toutes, pour chaque chaîne T dans P un majorant $M(T)$; et pour chaque élément x de P qui n'est pas un élément maximal, un élément $s(x)$ strictement plus grand. On veut construire un élément maximal de P. Par induction sur l'ordinal α, on va construire un élément x_α de P, de sorte que si $\beta < \alpha$ alors $x_\beta < x_\alpha$.

Supposons donc x_β construit pour chaque $\beta < \alpha$. Alors l'ensemble T des x_β pour $\beta < \alpha$ forme manifestement une chaîne dans P. Considérons $M(T)$: soit il est maximal dans P et on a fini, soit on pose $x_\alpha = s(M(T))$, et on a bien $x_\beta < x_\alpha$ pour chaque $\beta < \alpha$. Or on ne peut pas injecter les ordinaux dans P, donc le processus doit finir par s'arrêter (c'est-à-dire qu'on trouve un élément maximal de P)

(cf sinon EXOS pour démo "à la main")

12.7 AC plus faibles

AC dénom : on se restrieint à un domaine dénombrable (**N**)

AC dép : suite de choix successifs

Mq AC=>$\mathrm{AC}_{\mathrm{dép}}$=>$\mathrm{AC}_{\mathrm{dén}}$

(culture : implications *strictes*.

Solovay a construit des modèles de ZF + $\mathrm{AC}_{\mathrm{dép}}$ où chaque partie de R est mesurable, ce qui est faux avec AC

et la 2e ? ? ? ?)

[11] on a aussi un formule explicite entre deux réels : $\frac{\left\lceil a \left\lceil \frac{1}{b-a} \right\rceil \right\rceil}{\left\lceil \frac{1}{b-a} \right\rceil}$ est toujours dans $]a,b[$ (mais le choix est caché dans les "coins" qui cachent des min)

12.8 culture

Il faut l'axiome du choix pour démontrer qu'une union dénombrable d'ensembles dénombrables est dénombrable (pour choisir un dénombrement de chacun des ensembles : ici, avec les notations ci-dessus, D = les ensembles en question, $E(x)$ = les fonctions de $\mathbb{N}$ vers x, blah(x,y) = y est une bijection).

(Et il faut l'axiome du choix pour montrer que chaque suite croissante d'ordinaux dénombrables est majorée par un ordinal dénombrable.)

Mais l'axiome du choix n'est pas nécessaire pour travailler avec un ou un nombre fini d'ensembles dénombrables.

12.9 Pathologies

objets "intangibles"... Base de Hamel, parties non mesurables, ultrafiltre non principal

Mettre Banach-Tarski sur le compte de l'axiome du choix, c'est incroyablement hypocrite : ce qui pose problème dans Banach-Tarski, si quelque chose pose problème, c'est l'inexistence d'une mesure finiment additive sur les parties de $\mathbb{R}^3$ qui soit préservée par les isométries. L'axiome du choix, il n'y est pas pour grand-chose là-dedans, le pauvre : c'est le fait qu'on arrive à trouver un groupe libre dans les rotations de l'espace qui fait chier.

L'axiome du choix fait qu'on peut trouver une décomposition paradoxale de la boule, ce qui met le problème en lumière, certes, mais si on cherche à éviter cette décomposition, on se trouve dans une situation encore plus grotesque, où il n'y a pas de telle décomposition, mais pas non plus de mesure qui l'interdit ! L'axiome du choix n'y est pour **rien** dans le côté désagréable de Banach-Tarski.

d'ailleurs, le paradoxe de Dougherty et Foreman est encore pire !

12.10 Lectures

"*The Axiom of Choice is necessary to select a set from an infinite number of socks, but not an infinite number of shoes.*" — Bertrand Russell The observation here is that one can define a function to select from an infinite number of pairs of shoes by stating for example, to choose the left shoe. Without the axiom of choice, one cannot assert that such a function exists for pairs of socks, because left and right socks are (presumably) indistinguishable from each other.

(en parlant de l'idempotence des cardinaux infinis, *Introduction to Mathematical Philosophy*, 125-126). *But this, though we can prove that it is sometimes the case, cannot be proved to happen always unless we assume the multiplicative axiom. This is illustrated by the millionaire who bought a pair of socks whenever he bought a pair of boots, and never at any other time, and who had such a passion for buying both that at last he had $\aleph_0$ pairs of boots and $\aleph_0$ pairs of socks. The problem is : how many boots had he, and how many socks ? One would naturally suppose that he had twice as many boots and twice as many socks as he had pairs of each, and that therefore he had $\aleph_0$ of each, since that number is not increased by doubling. But this is an instance of the difficulty, already noted, of connecting the sum of ν classes each having μ terms with $\mu \times \nu$. Sometimes this can be done, sometimes it cannot. In our case it can be done with the boots, but not with the socks, except by some very artificial device. The reason for the differences is this : Among boots we can distinguish right and left, and therefore we can make a selection of one out of each pair, namely, we can choose all the right boots or all the left boots ; but with socks no such principle of selection suggests itself, and we cannot be sure, unless we assume the multiplicative axiom, that there is any class consisting of one sock out of each pair. Hence the problem.*

triangle de pensées, pages 29-30, Alain Connes (je mets en gras)

en logique, lorsqu'on construit un modèle non standard, par exemple des entiers, ou de la droite réelle, on utilise sans le dire l'axiome du choix. Il est appliqué dans une situation non dénombrable. L'axiome du choix, pour autant qu'il paraisse évident lorsqu'on l'énoncé puisqu'il s'agit de choisir un élément dans un ensemble non vide, n'est en fait pas du tout évident dans le domaine du non dénombrable. [...] Il est très facile de donner des exemples des difficultés que cela entraîne. Un exemple frappant est celui des pavages de Robinson-Penrose. Il s'agit de tous les puzzles que l'on obtient dans le plan à l'aide de deux petits motifs qui sont des triangles

de formes différentes liées au nombre d'or. On peut paver le plan d'une infinité de manières par ces motifs, d'un infinité de manière qui sont non congruentes, c'est-à-dire non isométriques les unes avec les autres. Or, précisément, il n'est pas possible de nommer dans chaque classe de pavages, à équivalence isométrique près, un pavage et un seul. Le fait est qu'il est impossible de choisir dans chaque classe de pavage un représentant et un seul. Cela n'est pas possible, sans précisément utiliser l'axiome du choix non dénombrable, donc ce n'est jamais possible de manière effective.

[...]

Une des propriétés surprenantes des pavages de Penrose est la suivante. Pensons à un univers de Penrose, c'est-à-dire à un pavage infini avec ces deux petits motifs, ces deux petits triangles. Deux univers sont différents si on ne peut pas les appliquer l'un sur l'autre par une isométrie. Il y a néanmoins un fait incroyable : ***quelle que soit la configuration finie dans un univers donné, on va pouvoir la retrouver exactement dans identique dans tout autre univers****. Cela veut dire qu'il est impossible de distinguer un univers de Penrose d'un autre par une portion finie.*

[...]

C'est quand même quelque chose d'étonnant car on peut distinguer entre deux nombres réels en allant suffisamment loin dans leur développement décimal.

Henri Lombardi, *Épistémologie mathématique* (p. 143)

l'argument selon lequel l'axiome du choix devrait être vrai par extrapolation du fini à l'infini est en soi un argument très faible. Car l'infinie actuel a justement été créé par le coup de force consistant à dire que désormais on considérerait comme irrémédiablement fausse la propriété, vraie dans le domaine des collections finies, selon laquelle il ne peut y avoir d'application bijective d'une partie stricte de E sur E lui-même (le tout est plus grand que la partie.

13 Cardinaux innaccssibles

$$\exists \kappa,\ \forall E \not\twoheadrightarrow \kappa,\ \mathfrak{P}(E) \hookrightarrow \kappa.$$

Mq alors li y a un ensmble stable par $\mathfrak{P}$:

$$\exists \kappa,\ \forall E \in \kappa,\ \mathfrak{P}(E) \in \kappa$$

Soit un tel κ. Def une fonctionelle sur $\mathfrak{P}(\kappa)$ qui à un P associe P si P est l'image diecte dans κ d'un $\mathfrak{P}(E)$ avec $E \not\twoheadrightarrow \kappa$ (et rien sinon) :

$$P(a,b) :\equiv \exists E \not\twoheadrightarrow \kappa,\ a = \mathfrak{P}(E) = b.$$

. Soit K lim'age de cette fonctionne (ok par remplcament). Mq K est $\mathfrak{P}$-stable. Soit $p \in K$. Mq $\mathfrak{P}(p) \not\twoheadrightarrow \kappa ? ? ? ?$ Aliors $\mathfrak{P}(p) \hookrightarrow \kappa$, donc κ contient une iamge directe d'un $\mathfrak{P}(p)$, donc contient $\mathfrak{P}(p)$, cqfd.

ZF + « il existe un cardinal inaccessible » prouve (ZF+)Consis(ZF). Et ZF + « il existe deux cardinaux inaccessibles » prouve la consistance de ZF + « il existe un cardinal inaccessible », etc. Presque tout le monde est intimement persuadé que tous ces systèmes sont consistants (et même avec de bien plus gros cardinaux).

s'il est difficile d'affirmer que l'intuition recommande a priori d'adopter les axiomes de grands cardinaux, il existe néanmoins à l'heure actuelle un consensus parmi les spécialistes pour le faire—ou, tout au moins, pour rejeter tout axiome qui contredirait l'existence de grands cardinaux. Au moins trois principes justifient cette position :

1 l'un est que le passage à l'infini est l'opération clé de la théorie des ensembles et qu'il serait illogique de refuser de l'itérer ;

2 le second est que les théories sans grands cardinaux apparaissent comme des sous-théories des théories avec grands cardinaux, de sorte que ces dernières sont le cadre global le plus adapté pour le calcul ensembliste — à la facon dont les corps algébriquement clos fournissent un cadre adapté pour le calcul algébrique ;

3 surtout, le troisième point est que les axiomes de grands cardinaux mènent à une théorie si riche et satisfaisante qu'elle emporte *a posteriori* l'adhésion des spécialistes — on y reviendra plus loin.

2de ordre cool Les modèles de ZFC du second ordre sont tous de la forme V_κ, et V_κ est un modèle de ZFC du second ordre ssi κ est un cardinal inaccessible.

Rq : grnds cardinaux <=> axiome des univers de Grothendieck (écrit pour formaliser catégories dans ZF)

14 Divers

AF est independant des autres axiomes ZF ou ZFC,

Sur les énoncés arithmétiques, ZF et ZFC prouvent exactement les mêmes choses.
On a même mieux : sur les énoncés arithmétiques, ZF et ZFC+GCH (hyp du continu généralisé) prouvent exactement les mêmes choses.

Croire en fondation, choix, c'est juste choisir sur quels ensembles on travaille.
En revanche, remplacement a une conséquence arithmétique (via les ordinuax) : il permet de montrer la consistance de Zermelo moins fondation. :-p

14.1 ZF avec atomes

14.2 théorie alternative à ZFC : von Neumann–Bernays–Gödel (NBG)

formaliser le langage naïf des classes : écrire $a \in C$, abréger $a = C$ si les deux ont même éléments, interdire $C \in ....$ La théorie obtenue (avec quasiément les mêmes axiomes que ZF) montre les même théorèmes que ZFC.
Si l'on autorise, dans séparation, des énoncés avec des variables libres portant sur des **classes** (exclu dans NBG), alors on tombe sur Morse-Kelley, strictement plus forte (sa consistance entraine celles de ZFC et NBG, mais est entrainée par ZFC+IC)

14.3 De l'art de conceptualiser : des sacs aux ensembles

$\mathbb{N}$ n'est pas aussi "réel" qu'on voudrait qu'il le soit. Je m'explique.
Nous avons l'habitude de manipuler un concept d'entier naturel, plus petit que $10!^{10!}$(par exemple). En quoi ces entiers *habituels* en deviennent *réels* ?
Par ailleurs, il y a déjà un saut conceptuel pour atteindre d'autres entiers plus grands, le "aussi grand que l'on souahite". Et un de plus pour atteindre le concept de l'ordinal oméga, à savoir de pouvoir mettre *tous* les entiers.

De même pour les ensembles : à l'origine, on met des objets dans des sacs, et basta, pas moins concrêt que les entiers habituels. On peut même mettre des sacs dans d'autres sacs, cela reste accessible.
Le premier pas selon moi à franchir est de se dire que l'on peut remplir des sacs *par la pensée* : je peux mettre cette bettrave et cette enclume ensemble, je peux regrouper ce verre à pied, ce bandeau, et cette enclume.
Apparaît dans l'exemple ci-dessus un autre pas : s'autoriser à dupliquer par la pensée un objet en vue de différentes utilisations : par exemple, en utilisant plusieurs fois l'exemplaire unique de vase Ming que j'ai sous les yeux pour différents sacs.
Une petite convention apparaît alors : il n'est pas nécesaire de répéter un même objet au sein d'un même sac. Ce n'est pas un saut conceptuel, et c'est justifié pour les raisons que l'on connaît (possibilité de coder la répétition).
De cette convention naît cependant un autre saut, vraiment important car il amène à la définition de l'égalité ensembliste. La question que l'on se pose lorqu'on a un sac devant nous, c'est est-ce que tel objet est dedans ou pas. Et la réponse à ces questions détermine entièrement notre sac : on se fiche si l'enveloppe est en peau de vache ou de crocrodile, tout ce qui nous intéresse, c'est ce qu'il contient.
Ensuite, je ne vais pas parler des axiomes constructifs (union, partie, séparation), car ils sont naturels et ne nécessitent aucun effort pour les sacs habituels – comprendre : qui ne contiennent qu'un nombre *usuel* d'éléments.
Je passe donc tout de suite au saut de l'infini : accepter que l'on puisse mettre plein d'objets, *autant* d'objets que souhaité, dans un même sac. Ca c'est vraiment fort, déjà ca casse les limites physiques immaginables, et on passe de l'infini potentiel à l'infini actuel.
Je peux maintenant revenir sur les axiomes consctructifs (en rajoutant même AC). Je vois l'union comme : mon coffre de voiture est rempli de sacs de courses, je vide mes courses sur la table avant de les ranger. Il y a donc croissance du cardinal (qui peut être violente dans le cas fini), ce qui pose un saut conceptuel du même

ordre que pour infini (même si on descend d'un type, mais ca ne veut rien dire sans fondation derrière). Même discours pour partie. Séparation m'a l'air très acceptable, car il s'agit jsute de séparer un ensemble en deux (mais avec les problèmes que l'on connaît pour la formulation du critère de séparation).

Pour choix, c'est un autre saut conceptuel venant de la représentation d'un procédé de choix à l'aide de sacs. Déjà, ca fait bizarre... Mais le cas fini et le codage d'un choix avec un graphe (sacs de couples) est parfaitement accessible. Déjà il y a un saut pour $AC_{dén}$ (pour moi le même que pour infini), et de vraiment tout autre nature pour les formes plus fortes de AC.

Pour fondation, il s'agit essentiellement de croire que tout se construit par les ordinaux, ce qui supppose le saut conceptuel adéquat (et donc de discuter de la vérité de remplacement, ou au moins de son application dans la construction des ordinaux). Pour ma part, comme l'opération successeur est "naturelle" et que l'opération réunion est un analogue de l'infini, les ordinaux ne posent pas de problèmes si je fais le pas jusqu'à infini (modulo l'application de remplacament là où il faut)

Dans tous les cas, un point me semble fondamental : si l'on accepte les fondements actuels logiques des maths, une fois les axiomes d'une théorie posée (dont on aura longuement discuté de la "vérité" comme ci-dessus), tout le reste *doit* suivre et être accepté (puiqu'il s'agit de mettre des propositions bout à bout pour écrire des preuves).

J'aime souvent à parler de l'analogue physique : on modélise un phénomène physique par un modèle mathématique. Si on croit en notre modèle, on doit en accepter toutes les conséquences physiques correspondant aux conséquences mathématiques. Ce qui donne généralement des choses rigolotes :-P

14.4 Pourquoi les indécisables ne le sont pas autant que ça, notion de vérité

S´eminaire BOURBAKI Mars 2003+
55‘eme ann´ee, 2002-2003, no 915
PROGR‘ES R´ECENTS SUR L'HYPOTH‘ESE DU CONTINU
[d'apr‘es Woodin]
par Patrick DEHORNOY

Il peut être tentant de retenir que le problème du continu ne peut être résolu et qu'à défaut d'être fermé, il est du moins sans intérêt, tout nouvel effort étant voué à l'échec.

Cette conclusion est erronée. On peut certes juger le problème inopportun si on accorde peu d'intérêt aux objets qu'il met en jeu : sous-ensembles compliqués de $\mathbb{R}$, bons ordres dont l'existence relève de l'axiome du choix1. Par contre, on doit voir que la question, si elle n'est pas écartée a priori, n'est pas fermée mais ouverte par les résultats de Gödel et Cohen : ainsi que le démontre le corpus accumulé, le système ZFC n'épuise pas notre intuition des ensembles, et la conclusion ne doit pas être que l'hypothèse du Continu n'est ni vraie, ni fausse2, mais, simplement, que le système ZFC est incomplet, et qu'il s'agit de le compléter.

Des analogies sont évidentes : que l'axiome des parallèles ne soit pas conséquence des autres axiomes d'Euclide n'a pas clos la géométrie, mais, au contraire, a permis l'émergence des géométries non euclidiennes, et a ouvert la question de reconna■tre, parmi toutes les géométries possibles, la plus pertinente pour décrire le monde physique. De même, les résultats de Gödel et de Cohen montrent que plusieurs univers sont possibles à partir de ZFC, et ouvrent donc l'étude des divers univers possibles — c'est-à-dire, de fa¸con équivalente, des divers systèmes axiomatiques complétant ZFC — et la question de reconna■tre, parmi ceux-ci, le(s) plus pertinent(s) pour décrire le monde mathématique.

K. G¨odel, What is Cantor's Continuum Problem ?, Amer. Math. Monthly 54 (1947) 515–545.

There might exist axioms so abundant in their verifiable consequences, shedding so much light upon a whole discipline, and furnishing such powerful methods for solving given problems (and even solving them, as far as possible, in a constructivistic way) that quite irrespective of their intrinsic necessity they would have to be assumed at least in the same sense as any established physical theory.»

14.5 Discussion David D après *braquage à l'anglaise*

Sur l'égalité ensembliste : avec fondation, c'est une définitino récursive, on creuse jusqu'au vide. Si on avait deux vides différents, on serait bien embetés...

Les êtres mathématiques (dont les ensembles) sont uniques. On peut toutefois en capter un exemplaire et l'enfermer dans un ensemble.

14.6 Une idée pour se rassurer d'utiliser ZF

Mais si tu veux te convaincre intuitivement de la consistance de ZF **dans** ZF, tu peux toujours faire ceci : il est un théorème de ZF (connu sous le nom de principe de réflexion) que chaque sous-ensemble fini des axiomes de ZF (ou même : ZF avec le schéma de remplacement limité aux formules Σ_n pour n'importe quel entier naturel n fixé) admet un modèle. Or dans une démonstration donnée tu n'utiliseras jamais qu'un nombre fini d'axiomes de ZF, et je viens de dire que ZF prouve leur consistance. L'arnaque, bien sûr, c'est que ZF ne prouve pas ça de façon **uniforme** sur l'ensemble d'axiomes / le n dans Σ_n. Mais si tu prends tous les axiomes jamais utilisés en maths, ils sont bien limités par un certain n et tu peux alors pondre la démonstration de « consistance du sous-système qu'on a utilisé jusqu'en 2007 (cet article-ci exclu :-) ». Ça ne vaut pas plus que l'argument platonique « je suis convaincu que ZF est vrai, donc il est certainement consistant », mais c'est toujours rassurant.

14.7 Kripke-Platek : un ZF sans partie

Il y a une théorie des ensembles appelée Kripke-Platek, qui est constituée des axiomes d'extension, vide, paire, union, infini, sélection limitée aux prédicats Δ_0 (i.e., à quantificateurs bornés comme je viens de le définir) et remplacement limité aux prédicats Σ_1 (i.e., admettant des quantificateurs existentiels uniquement devant un prédicat Δ_0) ou quelque chose de ce genre (Δ_0-collection). Il manque donc : ensemble des parties et les formes complètes de sélection et remplacement. Il s'avère que

(1) cette théorie est très intéressante de beaucoup de points de vue (notamment, elle a des liens très forts avec la théorie de la calculabilité et des ensembles hyperarithmétiques : par exemple, le plus petit ordinal dont elle ne prouve pas l'existence est le ω_1 de Church-Kleene),

(2) qu'on sait l'analyser du point de vue de la théorie de la preuve (son ordinal de preuve est exactement l'ordinal de Bachmann-Howard)

(3) qu'elle suffit vraisemblablement, modulo un peu de codage[#], à faire toutes les mathématiques « usuelles ».

Il est pertinent, en vertu des remarques (1) et (2), de prendre le soin de vérifier dans quelle mesure la (3) est vraie.

[#] Évidemment, il faut ruser, parce que Kripke-Platek ne prouve pas l'existence de $\mathbb{R}$ (il n'y a pas d'axiome d'ensemble des parties). Cependant, il prouve l'existence de l'ensemble-des-réels-récursifs, par exemple, ou de l'ensemble-des-réels-arithmétique[ment-définissable]s, et quitte à ajouter des classes (prédicativement définies) dans la théorie on peut faire largement comme si $\mathbb{R}$ existait (ce sera en pratique l'ensemble des réels hyperarithmétiques, mais aucun mathématicien non ensembliste n'a jamais besoin d'un réel non hyperarithmétique).