La théorie des ensembles cinquante ans après Cohen

Patrick Dehornoy

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

Grenoble, avril 2018

- Les résultats de Cohen ne sont pas la fin de l'Histoire.
- Aujourd'hui, on en sait (bien) plus sur (les ensembles et) l'infini,
  et il existe un espoir raisonnable que le problème du continu soit résolu.
- De nouveaux types d'applications de la théorie des ensembles apparaissent.

Plan:

- I. Le problème du continu jusqu'à Cohen
- II. Que signifie découvrir de nouveaux axiomes vrais ?
- III. Une application d'un type nouveau: les tables de Laver

Plan:

- I. Le problème du continu jusqu'à Cohen
- II. Que signifie découvrir de nouveaux axiomes vrais ?
- III. Une application d'un type nouveau: les tables de Laver

- Théorème (Cantor, 1873) : *Il existe*
  au moins deux infinis non équivalents.

- Théorème (Cantor, 1880's) : *Il existe*
  une infinité d'infinis non équivalents,
  qui s'organisent en une suite bien ordonnée

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \cdots.$$

- Faits. - $\mathrm{card}(\mathbb{N}) = \aleph_0$,
  - $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathfrak{P}(\mathbb{N})) = 2^{\aleph_0} > \mathrm{card}(\mathbb{N})$.

- Question (problème du continu) : Pour quel ordinal α a-t-on $\mathrm{card}(\mathbb{R}) = \aleph_\alpha$?

- Conjecture (hypothèse du continu, Cantor, 1879) : $\mathrm{card}(\mathbb{R}) = \aleph_1$.
  - Équivaut à : tout ensemble non dénombrable de réels est en bijection avec $\mathbb{R}$.

- Théorème (Cantor–Bendixson, 1883) : *Les fermés vérifient HC.*

Tout fermé non dénombrable est en bijection avec $\mathbb{R}$.

- Théorème (Alexandroff, 1916) : *Les boréliens vérifient HC.*

... et puis plus aucun progrès pendant 70 ans.

- Entre-temps, formalisation de la logique du premier ordre (Frege, Russell, ...) et axiomatisation de la théorie des ensembles (Zermelo, puis Fraenkel, ZF)
  - Consensus : « *Nous sommes d'accord que ces propriétés traduisent notre vision actuelle des ensembles* (*mais cela peut changer dans le futur...*)».

- Première question : HC est-elle prouvable ou réfutable à partir de ZF ?

- <u>Théorème</u> (Gödel, 1938) : *Sauf si ZF est contradictoire, HC n'est pas réfutable à partir de ZF.*

- <u>Théorème</u> (Cohen, 1963) : *Sauf si ZF est contradictoire, HC n'est pas prouvable à partir de ZF.*

- Conclusion : ZF est incomplet.
  - Découvrir plus de propriétés de l'infini, et adopter plus d'axiomes !
  - Comment reconnaître qu'un axiome est vrai? (Qu'est-ce que cela signifie ?)

Exemple: On <u>peut</u> prendre HC comme axiome, mais ce n'est <u>pas</u> une bonne idée...

Plan:

- Quels nouveaux axiomes ?

- Depuis les années 1930, axiomes de grand cardinal (GC):
  - diverses solutions à l'équation

$$\frac{\text{super-infini}}{\text{infini}} = \frac{\text{infini}}{\text{fini}}$$

  - cardinaux inaccessibles, measurables, etc.
  - axiomes «il existe tel ou tel grand cardinal»...

- Principe: «autosimilaire implique grand»
  - X infini: $\exists j : X \to X$ (j injective non bijective)
  - X super-infini: $\exists j : X \to X$ (j inj. non bij. préservant toute notion $\in$-definissable)

    un plongement (élémentaire) sur X
  - Exemple: Il ne peut exister aucun plongement sur $\mathbb{N}$, donc $\mathbb{N}$ n'est pas super-infini.

- Les axiomes GC sont naturels (itération de l'existence d'un ensemble infini), mais aucune évidence qu'ils soient vrais, ou simplement utiles (pas de lien avec les objets usuels).

• Définition : Pour $A \subseteq \mathbb{R}$, on considère le jeu G_A où deux joueurs I et II jouent 0 ou 1

I	a_1		a_3		...		
II		a_2		a_4		...	

et où I est déclaré gagnant si le réel $[0, a_1 a_2 \ldots]_2$ est dans A.
Alors A est dit déterminé si un des deux joueurs a une stratégie gagnante dans G_A.

• Un énoncé infini d'un type spécial:

$$\exists a_1 \forall a_2 \exists a_3 \ldots ([0, a_1 a_2 \ldots]_2 \in A) \ \underline{\text{ou}} \ \forall a_1 \exists a_2 \forall a_3 \ldots ([0, a_1 a_2 \ldots]_2 \notin A),$$

et un modèle pour de nombreuses propriétés: il existe $C_{\mathcal{L}}, C_{\mathcal{B}} : \mathfrak{P}(\mathbb{R}) \to \mathfrak{P}(\mathbb{R})$ t.q.

A est Lebesgue mesurable ssi $C_{\mathcal{L}}(A)$ est déterminé,

A a la propriété de Baire ssi $C_{\mathcal{B}}(A)$ est déterminé, etc.

• Toujours vrai pour les ensembles simples, et (faux) pour les ensembles compliqués:

- Tous les ouverts sont déterminés (Gale–Stewart, 1962),
- Tous les boréliens sont déterminés (Martin, 1975).
- «Tous les ensembles sont déterminés» contredit AC (Mycielski–Steinhaus, 1962),
- «Tous les projectifs sont déterminés» non prouvable à partir de ZF ($\approx$ Gödel, 1938).

$\uparrow$ clôture des boréliens par projection et complément

- Définition : Axiome de détermination projective (DP) :
  "Tout ensemble projectif de réels est déterminé".

- Propositions (Moschovakis, Kechris, ..., 1970s) : *Ajouté à ZF,*
  DP *fournit une description «complète» et satisfaisante des ensembles projectifs.*

  heuristiquement complète pas de pathologie : Lebesgue mesurable, etc.

  - Exemple: Sous ZF+DP, les ensembles projectifs vérifient HC.

- L'axiome DP est utile (améliore la description des ensembles usuels),
  mais pas naturel (pourquoi le considérer ?)
  — contrairement aux axiomes de grand cardinal, naturels mais non utiles.

- Théorème (Martin–Steel 1985, Woodin, 1987) : DP *est un axiome de grand cardinal.*

une infinité de cardinaux de Woodin entraîne DP

DP (entraîne) une infinité de cardinaux de Woodin

- Corollaire (Woodin) : DP *est vrai.*

«Démonstration» : DP est à la fois naturel (comme axiome de grand cardinal), et utile (comme axiome de détermination). □

- Pourquoi «vrai» ?
  - Comparer avec l'axiome d'infini : évidence = (?) intériorisation d'une longue familiarité et d'une efficacité pratique.
  - (Woodin) «*The statement that DP is consistent is a new mathematical truth. It predicts facts about our world, for instance that in the next 1000 years there will be no contradiction discovered from PD by any means.*»

- Nouveau consensus :

Le système de référence pour la théorie des ensembles n'est plus ZF, mais ZF+DP.

- Fait: Ni HC ni $\neg$HC ne sont prouvables à partir de ZF+DP : rien n'est réglé...
  - avec ZF : description «complète» des ensembles finis (= cardinal$<\aleph_0$);
  - avec ZF+DP : description «complète» des ensembles finis ou dénombrables (= cardinal$<\aleph_1$);
  - étape suivante : description «complète» des ensembles de cardinal$<\aleph_2$?
    ... inclura forcément une solution de HC.

- Deux types d'approche (et pas encore de consensus...)

- Approche maximaliste : axiomes de forcing (par ex. «axiome de Martin maximal»)
  - $\approx$ principes de clôture algébrique (tout ce qui n'est pas exclu existe...) ;
  - compatibles avec les grands cardinaux.

- Théorème (Woodin, 2003) : *Si la Ω-conjecture forte est vraie, tout axiome de forcing décrivant «complètement» les ensembles de cardinal $<\aleph_2$ implique $\neg$HC.*

  - mais seulement envisageable pour le cas de $\aleph_2$, pas au-delà.

- Approche minimaliste : identifier un plus petit modèle de référence (n'existe que ce qui doit exister... ; par ex. l'univers L des ensembles constructibles) ;
  - mais L non compatible avec les grands cardinaux : développer des analogues à L ?
  - univers $L[U]$ (Kunen, 1971) : compatible avec les cardinaux mesurables ;
  - univers $L[E]$ (Mitchell–Steel, 1980-90s) : compat. avec les card. de Woodin (DP) ;
  - mais : comment espérer compléter le programme avec une hiérarchie sans fin ?

- Théorème (Woodin, 2006) : *Si un univers de type $L[X]$ est compatible avec un cardinal supercompact, il est automatiquement compatible avec tous les grands cardinaux.*

  - $L^{\mathrm{ultime}} :=$ univers $L[X]$ (encore hypothétique...) pour un cardinal supercompact.

- Conjecture (Woodin, 2010) : $\mathrm{ZF}+\mathrm{DP}+V=L^{\mathrm{ultime}}$ *est vrai.*

  - signifie(rait) que $V=L^{\mathrm{ultime}}$ est devenu naturel (jugement esthétique fondé sur une accumulation de théorèmes) et fournit une description exempte de pathologie.
  - (comme pour tout univers $L[X]$) $V=L^{\mathrm{ultime}}$ entraîne HC (et même HCG).

- Si (un jour) $\mathrm{ZF}+\mathrm{DP}+V=L^{\mathrm{ultime}}$ — ou ZF+DP+un axiome de forcing — est adopté comme système de référence, alors le problème du continu aura été résolu.

Plan:

- I. Le problème du continu jusqu'à Cohen
- II. Que signifie découvrir de nouveaux axiomes vrais ?
- III. Une application d'un type nouveau: les tables de Laver

- Loi d'autodistributivité (à gauche) :

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z). \tag{LD}$$

  - Exemple classique 1 : E module et $x \cdot y := (1 - \lambda)x + \lambda y$;
  - Exemple classique 2 : G groupe et $x \cdot y := xyx^{-1}$.

    NB: idempotents ($x \cdot x = x$), donc toute structure monogène est triviale
  - (Brieskorn,...) contrepartie algébrique du mouvement de Reidemeister III...

- Une opération sur $\{1, 2, 3, 4\}$: la table de Laver à 4 éléments

$\cdot$	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

- Commencer avec $+1 \bmod 4$ dans la première colonne,
  et compléter en utilisant la règle $x \cdot (y \cdot 1) = (x \cdot y) \cdot (x \cdot 1)$:

$$\begin{aligned}
&4 \cdot 2 = 4 \cdot (1 \cdot 1) = (4 \cdot 1) \cdot (4 \cdot 1) = 1 \cdot 1 = 2,\\
&4 \cdot 3 = 4 \cdot (2 \cdot 1) = (4 \cdot 2) \cdot (4 \cdot 1) = 2 \cdot 1 = 3,\\
&4 \cdot 4 = 4 \cdot (3 \cdot 1) = (4 \cdot 3) \cdot (4 \cdot 1) = 3 \cdot 1 = 4,\\
&3 \cdot 2 = 3 \cdot (1 \cdot 1) = (3 \cdot 1) \cdot (3 \cdot 1) = 4 \cdot 4 = 4, \ldots
\end{aligned}$$

- La construction marche pour toutes les tailles :

- <u>Proposition</u> (Laver) : (i) *Pour tout N, il existe une unique opération $\cdot$ sur $\{1, ..., N\}$ vérifiant*

$$x \cdot 1 = x + 1 \bmod N \quad \text{et}$$
$$x \cdot (y \cdot 1) = (x \cdot y) \cdot (x \cdot 1).$$

(ii) *L'opération obtenue obéit à la loi LD si, et seulement si, N est une puissance de 2.*

  - $A_n :=$ la table de Laver à 2^n éléments.

- Pour $n \geqslant 1$, on a $1 \cdot 1 = 2 \neq 1$ dans A_n : <u>non</u> idempotent.
  - différent de la conjugaison des groupes et autres LD-structures classiques ;
  - contrepartie de $\mathbb{Z}/n\mathbb{Z}$ dans le monde autodistributif :
    A_n présenté par $\langle 1 \mid 1_{[2^n]} = 1 \rangle_{LD}$, avec $x_{[p]} = (...((x{\cdot}x){\cdot}x)...){\cdot}x$, p termes, ...

Tables de Laver : exemples

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

• Proposition (Laver) : *Pour tout $p \leqslant 2^n$, il existe un entier $\pi_n(p)$, puissance de 2, tel que la $p^{\text{ème}}$ ligne de A_n est la répétition périodique de $\pi_n(p)$ valeurs croissant de $p+1 \bmod 2^{\mathrm{n}}$ à 2^n.*

• Exemple :

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

- $\pi_3(1) = 4$
- $\pi_3(2) = 4$
- $\pi_3(3) = 2$
- $\pi_3(4) = 4$
- $\pi_3(5) = 2$
- $\pi_3(6) = 2$
- $\pi_3(7) = 1$
- $\pi_3(8) = 8$

• Quelques valeurs des périodes de 1 et 2 :

n	0	1	2	3	4	5	6	7	8	9	10	11	...
$\pi_n(1)$	1	1	2	4	4	8	8	8	8	16	16	16	...
$\pi_n(2)$	–	2	2	4	4	8	8	16	16	16	16	16	...

- Question 1 : A-t-on toujours $\pi_n(2) \geqslant \pi_n(1)$?
- Question 2 : La période $\pi_n(1)$ tend-elle vers l'infini avec n ? Atteint-elle 32 ?

• Théorème (Laver, 1995) : *S'il existe un ensemble super-infini — « un cardinal de Laver »—, la réponse aux questions sur les périodes est positive.*

• Définition : Un rang est un ensemble R t.q. $f : R \to R$ entraîne $f \in R$. (? Cela existe...)

• Supposons qu'il existe un ensemble super-infini (i.e., $\exists$ plongement...) :
- alors il existe un rang super-infini, disons R ;
- si i, j sont des plongements sur R, alors $i : R \to R$ et $j \in R$, donc i s'applique à j ;
- « être un plongement » est $\in$-définissable (??), donc $i(j)$ est un plongement ;
- « être l'image de... » est $\in$-définissable,
  donc $\ell = j(k)$ entraîne $i(\ell)=i(j)(i(k))$, *i.e.*, $i(j(k))=i(j)(i(k))$: loi LD.

• Proposition (Laver) : *Supposons que j est un plongement sur un rang R.*
- *L'ensemble Iter(j) des itérés de j — i.e., j, $j(j)$, $j(j)(j)$... — obéit à la loi LD.*
- *Pour tout n, il existe une congruence sur Iter(j) avec 2^n classes et telle que la première colonne de la table du quotient est un cycle, donc le quotient est A_n.*
- *(dictionnaire) Pour $m \leqslant n$ et $p \leqslant 2^n$:*
  $\pi_n(p) = 2^m < \pi_{n+1}(p) = 2^{m+1} \quad \Longleftrightarrow \quad j_{[p]}(\mathrm{crit}(j_{[2^m]})) = \mathrm{crit}(j_{[2^n]})$.

$\uparrow$ $j(j)(j)...(j)$, p fois j $\quad \uparrow$ le plus petit ordinal bougé par...

- Lemme : *Si j est un plongement, alors, pour tout ordinal α, on a $j(j)(\alpha) \leqslant j(\alpha)$.*

  ▸ Démonstration : Il existe β vérifiant $j(\beta) > \alpha$, donc il existe un plus petit tel β, et alors on a $j(\beta) > \alpha$ et
  $$\forall\gamma < \beta \; (j(\gamma) \leqslant \alpha). \qquad (*)$$
  On applique le plongement j à $(*)$:
  $$\forall\gamma < j(\beta) \; (j(j)(\gamma) \leqslant j(\alpha)). \qquad (**)$$
  En prenant $\gamma = \alpha$ dans $(**)$, on obtient $j(j)(\alpha) \leqslant j(\alpha)$. □

- Proposition (Laver) : *S'il existe un ensemble «super-infini» — à savoir s'il existe un cardinal de Laver — alors, pour tout n, on a $\pi_n(2) \geqslant \pi_n(1)$.*

- Idem (plus difficile) pour la question 1 (période de 1 dans A_n tend vers l'∞).

- Démonstrations alternatives sans axiome de grand cardinal ? Pas encore...
  - ▸ résultats partiels de Drápal... mais pas de preuve complète pour le moment ;
  - ▸ situation étrange : pourquoi un lien entre des tables finies et des grands infinis ?

• Dernière question : Les propriétés des tables de Laver sont-elles une application de la théorie des ensembles ?

- Pour le moment, oui ; plus tard, formellement non si démontrations alternatives.
- Mais, à jamais, c'est la théorie des ensembles qui a fait découvrir les propriétés...
- Une analogie : En physique : par une intuition physique, deviner un énoncé, puis le passer au mathématicien pour une preuve formelle ; Ici: par une intuition logique (existence d'un ensemble super-infini), deviner un énoncé (les périodes dans les tables de Laver tendent vers l'∞), puis le passer au mathématicien pour une preuve formelle.
- Pas besoin de croire à l'existence des grands cardinaux pour les utiliser...

RÉSUMÉ :

• La théorie des ensembles est une théorie de l'infini, explorant les diverses possibilités (ni plus, ni moins: les «maths modernes» étaient un malentendu...)

• L'Histoire continue :

- Une théorie cohérénte au-delà de ZF est possible ;
- Il existe un consensus pour enrichir ZF en ZF+DP ;
- L'étape suivante inclura une solution du problème du continu.

- W. Hugh Woodin, *Strong axioms of infinity and the search for V*, Proceedings ICM Hyderabad 2010, pp. 504–528

- P. Dehornoy, La théorie des ensembles, Calvage & Mounet (2017)

//dehornoy.users.lmno.cnrs.fr/