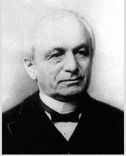
A quoi sert l'infini ?

Patrick Dehornoy
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

- Quelques exemples sur le rôle de l'infini comme outil de démonstration,
  et comme outil d'exploration.



- L.Kronecker : « Dieu a créé les nombres entiers ;
  tout le reste a été créé par l'homme »

$\uparrow$
typiquement : l'infini

- G. Cantor : théorie de l'infini (« théorie des ensembles »)

- Question(s) : Si on ne s'intéresse qu'aux nombres entiers (aux objets finis),
  l'infini est-il nécessaire ? Est-il utile ?

Partie I : L'infini est-il nécessaire ?

« L'infini peut-il être nécessaire pour démontrer des propriétés des objets finis ? »

- Oui : même si on ne s'intéresse qu'aux objets finis,
  le recours à l'infini est nécessaire pour certaines démonstrations.

= peuvent être comptés, dénombrés

- Certains objets mathématiques sont finis,
  (les sommets d'un carré, les paires d'entiers inférieurs à 5,...)

  d'autres sont infinis.
  (les entiers pris dans leur ensemble, les points d'une droite,...)

- Certaines assertions ne mettent en jeu que des objets finis,
  (un hexagone a neuf diagonales, 17 est un nombre premier,...)

  d'autres mettent en jeu au moins un objet infini.
  (il y a plus de points dans une droite que de nombres entiers,...)

- Pour des assertions ne mettant en jeu que des objets finis,
  certaines démonstrations ne mettent en jeu que des objets finis,
  d'autres mettent en jeu (aux étapes intermédiaires) des objets infinis.

- **Assertion 1** : Il existe $\frac{n(n-3)}{2}$ diagonales dans un polygone à n côtés.

- **Démonstration** : Soit a_n le nombre de diagonales dans un polygone à n côtés.
- De chacun des n sommets partent $n-3$ diagonales.
- Chaque diagonale est comptée deux fois ; on a donc $2a_n = n(n-3)$. $\square$

Ici, pas d'usage de l'infini : un seul nombre a_n à la fois.

- **Assertion 2** : Il existe $\frac{1}{n+1}\binom{2n}{n}$ arbres binaires à n sommets.

$\frac{(2n)!}{n!^2}$

- **Démonstration** : Soit a_n le nombre d'arbres à n sommets.
- Posons $F(X) = \sum_1^\infty a_n X^n$.
- La série $F(X)$ satisfait l'équation du second degré $X(F(X))^2 - F(X) + 1 = 0$.
- On a donc $F(X) = (1 - \sqrt{1-4X})/2X$, d'où $a_n = \frac{1}{n+1}\binom{2n}{n}$. $\square$

Ici, usage de l'infini : tous les nombres a_n à la fois.

- Peut-on éviter les exemples du second type ?

« Toute assertion (vraie) ne mettant en jeu que des objets finis
peut-elle être démontrée en n'utilisant que des objets finis ? »

« des méthodes finitistes »

- D. Hilbert (1900) : peut-être...

⇝ programme de Hilbert

- K. Gödel (1931) : non !

⇝ (premier) théorème d'incomplétude

- Une approximation raisonnable :
  finitistement démontrable = démontrable dans le système de Peano PA
  (propriétés de base de $+$ et $\times$ sur $\mathbb{N}$ et récurrence)

- Premier théorème d'incomplétude (Gödel, 1931) :
  Si S est un système formel non-contradictoire, explicite, et incluant PA,
  il existe des assertions vraies mais non démontrables dans S.

- Corollaire : Si le système PA est non-contradictoire,
  il existe des assertions vraies mais non démontrables dans PA.

- Des exemples ? Les formules de Gödel (codages du paradoxe du menteur)
- Des exemples naturels ?

$\rightsquigarrow$ des énoncés d'arithmétique vrais non démontrables dans PA

$\uparrow$

?????

$\uparrow$

démontrables en utilisant l'infini

- Ecriture d'un entier en base p itérée :

$$26 = [11010]_2 = 2^4 + 2^3 + 2^1 \quad \leftarrow \text{écriture en base } 2$$
$$= 2^{2^2} + 2^{2+1} + 2 \quad \leftarrow \text{écriture en base } 2 \text{ itérée}$$

- Définition : Pour $p < q$, transformation $T_{p,q}$:
  $=$ remplacer p par q dans l'écriture en base p itérée.

- Exemple :

$$26 = 2^{2^2} + 2^{2+1} + 2 \xrightarrow{T_{2,3}} 3^{3^3} + 3^{3+1} + 3 = 7.625.597.485.071$$

(une fonction très croissante...)

• Définition : La suite de Goodstein partant de d :

$$d \longrightarrow \boxed{T_{2,3}} \longrightarrow \dots \longrightarrow \boxed{-1} \longrightarrow \dots \longrightarrow \boxed{T_{3,4}} \longrightarrow \dots \longrightarrow \boxed{-1} \longrightarrow \dots \longrightarrow \boxed{T_{4,5}} \longrightarrow \dots$$

• Exemple : partant de $\mathbf{26}$:

$$\mathbf{26}, \quad \mathbf{7.625.597.485.071}, \quad \mathbf{7.625.597.485.070}, \quad \dots$$

Clairement : la suite tend (très) vite vers l'infini.

• Théorème (Goodstein, 1942) :
Quel que soit d, la suite de Goodstein partant de d atteint après un nombre fini d'étapes la valeur $\mathbf{0}$.

- Démontrer le théorème de Goodstein en utilisant l'infini ?

$\rightsquigarrow$ Utiliser les ordinaux de Cantor.

- Les ordinaux de Cantor (1880-86) : un prolongement de la suite des entiers naturels dans lequel toute famille non vide a un plus petit élément :

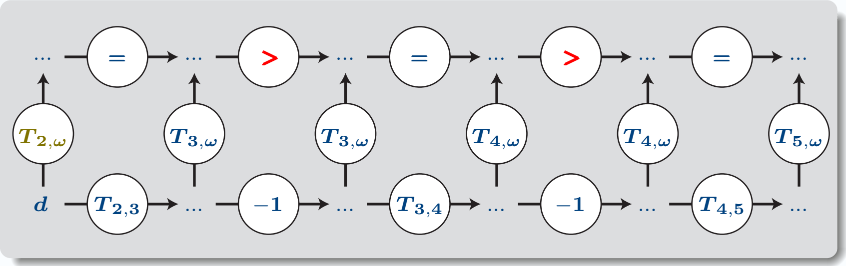
$$\mathbf{0}\ ,\ \mathbf{1}\ ,\ \mathbf{2}\ ,\ \dots,\ \boldsymbol{\omega}\ ,\ \boldsymbol{\omega+1}\ ,\ \boldsymbol{\omega+2}\ ,\ \dots,\ \omega+\omega=\boldsymbol{\omega.2},$$
$$\boldsymbol{\omega.2+1},\ \dots,\ \boldsymbol{\omega.3},\ \dots,\ \omega.\omega=\boldsymbol{\omega^2},\ \boldsymbol{\omega^2+1},\ \dots,\ \boldsymbol{\omega^2+\omega},$$
$$\dots,\ \boldsymbol{\omega^2.2},\ \dots,\ \omega^2.\omega=\boldsymbol{\omega^3},\ \dots,\ \boldsymbol{\omega^\omega},\ \dots,\ \boldsymbol{\omega^{\omega^\omega}},\ \dots$$

- Les ordinaux de Cantor existent-ils ?

- (Zermelo, Von Neumann, 1905–1920)
Dès qu'on postule l'existence d'au moins un ensemble infini, les ordinaux de Cantor existent (avec les propriétés escomptées).

• Démonstration : Il n'existe pas de suite infinie d'ordinaux strictement décroissante : si on a $\alpha_0 > \alpha_1 > \alpha_2 > \ldots$, l'ensemble $\{\alpha_0, \alpha_1, \ldots\}$ n'a pas de plus petit élément. Donc : toute suite strictement décroissante d'ordinaux est finie.

Considérons la suite de Goodstein partant de d :



Forcément, en haut, on arrive à 0 au bout d'un nombre fini d'étapes,
et la seule possibilité est que, en bas, on arrive à 0 au même moment. $\square$

- Démontrer le théorème de Goodstein sans l'infini ?

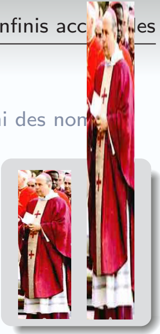
- Théorème (Kirby–Paris, 1982) : Le théorème de Goodstein ne peut pas être démontré dans le système de Peano PA.

$\approx$ non démontrable par récurrence
$\approx$ non démontrable sans infini

- (Principe de la démonstration: La fonction de Goodstein croît si vite qu'elle dépasse toute fonction dont l'existence est démontrable dans PA.)

- Le théorème de Goodstein est un exemple de «vrai» résultat d'arithmétique qui ne peut pas être démontré sans introduire l'infini.

... et il y a même bien pire...



• Dès qu'il existe un infini, il en existe plusieurs (Cantor, 1873 : l'infini des nom réels n'est pas celui des nombres entiers), et même une infinité.

• Programme de Gödel : Au-delà des infinis accessibles (ceux qui existent dès qu'on postule l'existence d'un ensemble infini), introduire des super-infinis (« grands cardinaux ») dont chacun dépasse les précédents comme l'infini dépasse le fini :

fini $<$ infini $<$ super-infini $<$ hyper-infini $<$ ultra-infini $<$ ...

• L'existence d'un infini ne garantit pas celle des super-infinis

$\rightsquigarrow$ purement spéculatif (?)

• (H. Friedman, 1980–2012) Des analogues du théorème de Goodstein: des résultats de théorie des graphes finis démontrables à partir de l'existence de divers super-infinis, mais pas sans.

entiers, graphes...
↓

• Résumé : Il existe des assertions ne mettant en jeu que des objets finis, démontrables si on postule l'existence d'objets (super)-infinis, mais pas sinon.

• Conclusion de la partie 1 : Même si on ne s'intéresse qu'au fini,
l'infini — ou même l'ultra-infini — est (dans certains cas)
un outil de démonstration indispensable.

• Un bémol : Même si les théorèmes de Goodstein et Friedman sont explicites et ne mettent en jeu que des objets finis, ils restent assez marginaux...

(Depuis 4, la suite de Goodstein atteint $\mathbf{0}$ en... $\mathbf{3} \times \mathbf{2}^{\mathbf{402.653.211}} - \mathbf{3}$ étapes.)

• Rien n'interdit que des énoncés « vraiment » importants exigent l'usage de l'(ultra)-infini pour être démontrés, mais, à ce jour, ce n'est pas (encore) arrivé.

Partie II : L'infini est-il utile ?

« Même quand il n'est pas nécessaire, l'(ultra)-infini peut-il être utile ? »

- Oui : l'usage de l'(ultra)-infini donne des moyens supplémentaires pour démontrer et même pour découvrir des propriétés des objets finis.

- Ordre bizarre : pourquoi après la première partie ? « utile < nécessaire » ?
  - Réponse 1 : L'infini est utile comme outil de démonstration ;
  - Réponse 2 : L'infini, et même l'ultra-infini, est utile comme outil d'exploration.

• **Théorème** : Le nombre de nombres premiers $\leqslant n$ est approximativement $\frac{n}{\log n}$.

• Conjecturé par Gauss en 1792

analyse complexe

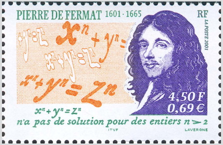
↓

• Démontré par des méthodes infinitistes
par Hadamard et de la Vallée-Poussin en 1896

• Démontré par des méthodes finitistes
par Erdös et Selberg en 1949.

- Théorème : L'équation $x^n + y^n = z^n$ n'a pas de solution non triviale pour $n \geqslant 3$.

- Affirmé par Fermat en 1637



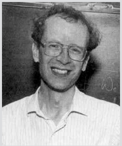
- Démontré par des méthodes infinitistes par Wiles en 1994

$\uparrow$

théorie de Grothendieck

$\uparrow$

utilise l'infini, et même un peu de super-infini



- Encore incertain si démontrable par des moyens purement finitistes

(travaux en cours de Macintyre et autres)

- Donc : l'usage de l'infini donne des moyens supplémentaires
  pour démontrer des propriétés des objets finis (ici : les nombres entiers).

... une banalité : toute utilisation des nombres réels
et de l'analyse est une utilisation de l'infini !

- Mais alors...

- Question bis : En est-il de même de l'ultra-infini ?

« Les spéculations sur l'ultra-infini peuvent-elles mener
à des résultats vraiment concrets ? »

- Une drôle de table de multiplication : la table de Laver à 4 éléments

$\times$	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 $+1$ mod 4 dans la 1ère colonne,

compléter en un LD-système, *i.e.*, avoir partout $x \times (y \times z) = (x \times y) \times (x \times z)$.

$$\begin{aligned}
&\mathbf{4 \times 2 = 4 \times (1 \times 1) = (4 \times 1) \times (4 \times 1) = 1 \times 1 = 2},\\
&\mathbf{4 \times 3 = 4 \times (2 \times 1) = (4 \times 2) \times (4 \times 1) = 2 \times 1 = 3},\\
&\mathbf{4 \times 4 = 4 \times (3 \times 1) = (4 \times 3) \times (4 \times 1) = 3 \times 1 = 4},\\
&\mathbf{3 \times 2 = 3 \times (1 \times 1) = (3 \times 1) \times (3 \times 1) = 4 \times 4 = 4},\dots
\end{aligned}$$

- Proposition (Laver) : La construction marche pour toutes les puissances de 2.

$\rightsquigarrow$ la table de Laver à $1, 2, 4, 8, 16, 32, \dots$ éléments.

• Question : Combien de valeurs dans la 1ère ligne de la table à n éléments ?

- table à	**1** élément :	**1**	**1** valeur
- table à	**2** éléments :	**2**, **2**	**1** valeur
- table à	**4** éléments :	**2**, **4**, **2**, **4**	**2** valeurs
- table à	**8** éléments :	**2**, **4**, **6**, **8**, **2**, **4**, **6**, **8**	**4** valeurs
- table à	**16** éléments :	**2**, **12**, **14**, **16**, **2**, **12**, **14**, **16**, **2**, ...	**4** valeurs
- table à	**32** éléments :	**2**, **12**, **14**, **16**, **18**, **28**, **30**, **32**, **2**, ...	**8** valeurs
- table à	**64** éléments :	**2**, **12**, **14**, **48**, **50**, **60**, **62**, **64**, **2**, ...	**8** valeurs
- table à	**128** éléments :	**2**, **12**, **14**, **112**, **114**, **124**, **126**, **128**, **2**, ...	**8** valeurs
- table à	**256** éléments :	**2**, **12**, **14**, **240**, **242**, **252**, **254**, **256**, **2**, ...	**8** valeurs
- table à	**512** éléments :	**2**, **12**, **14**, **240**, **242**, **252**, **254**, **256**, **258**, **268**, **270**, **496**, **498**, **508**, **510**, **512**, **2**,...	**16** valeurs

• Théorème (R. Laver, 1994).— S'il existe un ensemble ultra-infini, il existe une table avec plus de 16 valeurs dans la 1ère ligne (et idem avec un nombre de valeurs aussi grand qu'on veut).

- Quel est le rapport entre l'ultra-infini et les tables de Laver ?
  - Un certain axiome de grand cardinal (« il existe un rang auto-similaire ») entraîne l'existence d'un certain (hypothétique) LD-système $\boldsymbol{X}$... ...dont les tables de Laver sont des quotients finis.
- Sait-on démontrer l'existence d'un rang auto-similaire et du système $\boldsymbol{X}$?
  - Non, et on sait que c'est impossible.
- Sait-on démontrer l'existence des tables de Laver sans utiliser d'ultra-infini ?
  - Oui, c'est facile.
- Sait-on démontrer le résultat de Laver sans utiliser d'ultra-infini ?
  - Non, pas à ce jour.
- Peut-on démontrer le résultat de Laver sans utiliser d'ultra-infini ?
  - On ne sait pas, probablement oui (?), semble difficile, mais pourquoi pas ?

- Dans tous les cas, quelle que soit la suite, c'est l'utilisation de l'(ultra)-infini qui aura permis de découvrir le résultat de Laver, et de montrer qu'il est plausible.

- En physique : à partir d'une intuition de physicien, deviner une propriété, puis passer au mathématicien pour une « vraie » démonstration.

- Ici : à partir d'une intuition de logicien (existence d'ultra-infini), deviner une propriété (théorème de Laver, existence d'un LD-système ordonné), puis passer au mathématicien pour une « vraie » démonstration.

↑
sans ultra-infini

- Résumé : Lorsqu'on s'intéresse aux objets finis :
  - Il existe des cas où l'infini n'est ni nécessaire, ni utile ;
  - Il existe des cas où l'infini est nécessaire comme moyen de démonstration — mais, en pratique, ils sont souvent peu concrets ;
  - Il existe des cas où l'infini, et même l'ultra-infini, quoique non nécessaire, est utile (voire décisif) comme moyen de découverte.

- Conclusion : Même si on ne s'intéresse qu'au fini et à l'effectif, et qu'on ne croit pas à l'existence de l'(ultra)-infini, il serait regrettable de se priver des intuitions qu'il apporte.

- Question : Les Martiens utilisent-ils l'(ultra)-infini ?