Sol DeWitt, Incomplete open cube, 1974

Incomplétude et incalculabilité

(Incomplétude (Gödel) et incalculabilité (Turing) en mathématiques)

Jean-Paul Delahaye, Université de Lille 1

CRISTAL (LIFL + LAGIS) **UMR CNRS 9189**

Centre de recherche en informatique, signal et automatique de Lille

Bat M3-Ext, Université de Lille 1, 59655, Villeneuve d'Ascq CEDEX France

***15 Janvier* 2015**

L'incomplétude mathématique est d'abord une idée simple :

C'est l'impossibilité d'arriver à établir un résultat (attendu)
avec des moyens (démonstratifs) fixés à l'avance.

Lorsque cette impossibilité est **démontrée** : on a affaire à une **incomplétude**

... Une vieille histoire ....

Axiome des parallèles ou cinquième postulat d'Euclide (-325 -265)

Il est impossible de déduire l'axiome des parallèles des autres axiomes de la géométrie.

•1• il existe toujours une droite qui passe par deux points du plan.

•2• tout segment peut être étendu suivant sa direction en une droite (infinie).

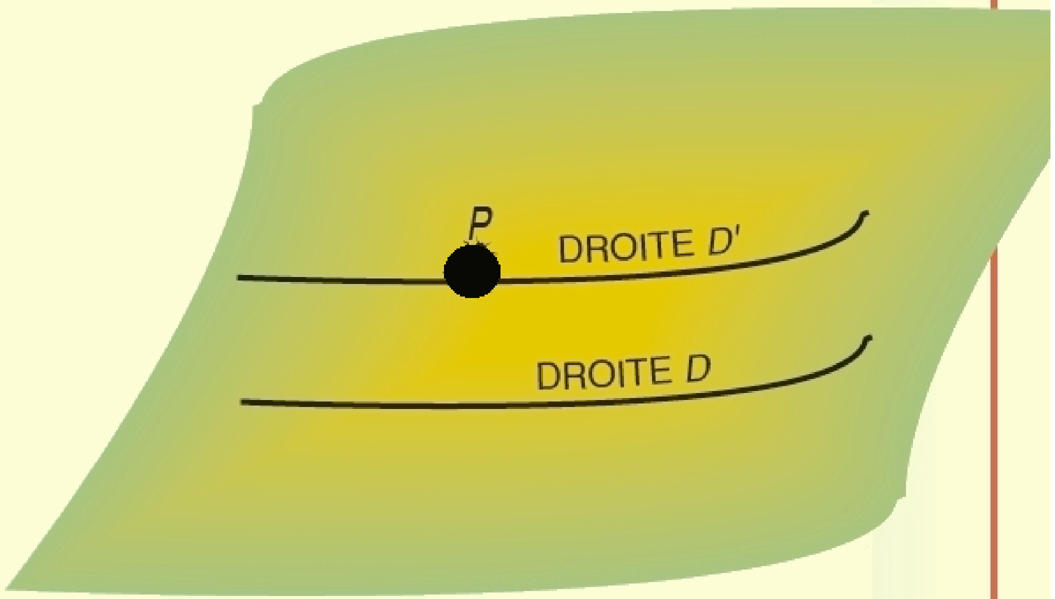
•3• à partir d'un segment, il existe un cercle dont le centre est un des points du segment et dont le rayon est la longueur du segment.

•4• tous les angles droits sont égaux entre eux.

•5• étant donné un point et une droite ne passant pas par ce point, il existe une seule droite passant par ce point et parallèle à la première.

L'AXIOME DES PARALLÈLES

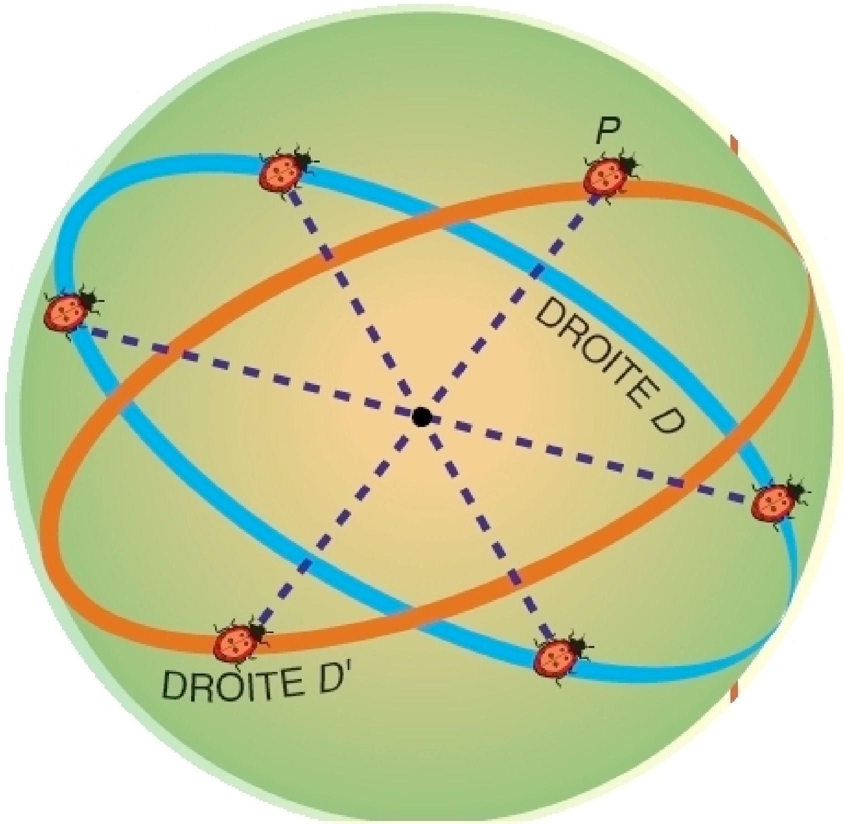
Si *P* est un point donné et si *D* est une droite ne contenant pas *P*, alors dans le plan déterminé par *P* et *D* il existe une droite unique *D'*, contenant *P* et ne rencontrant pas *D*.

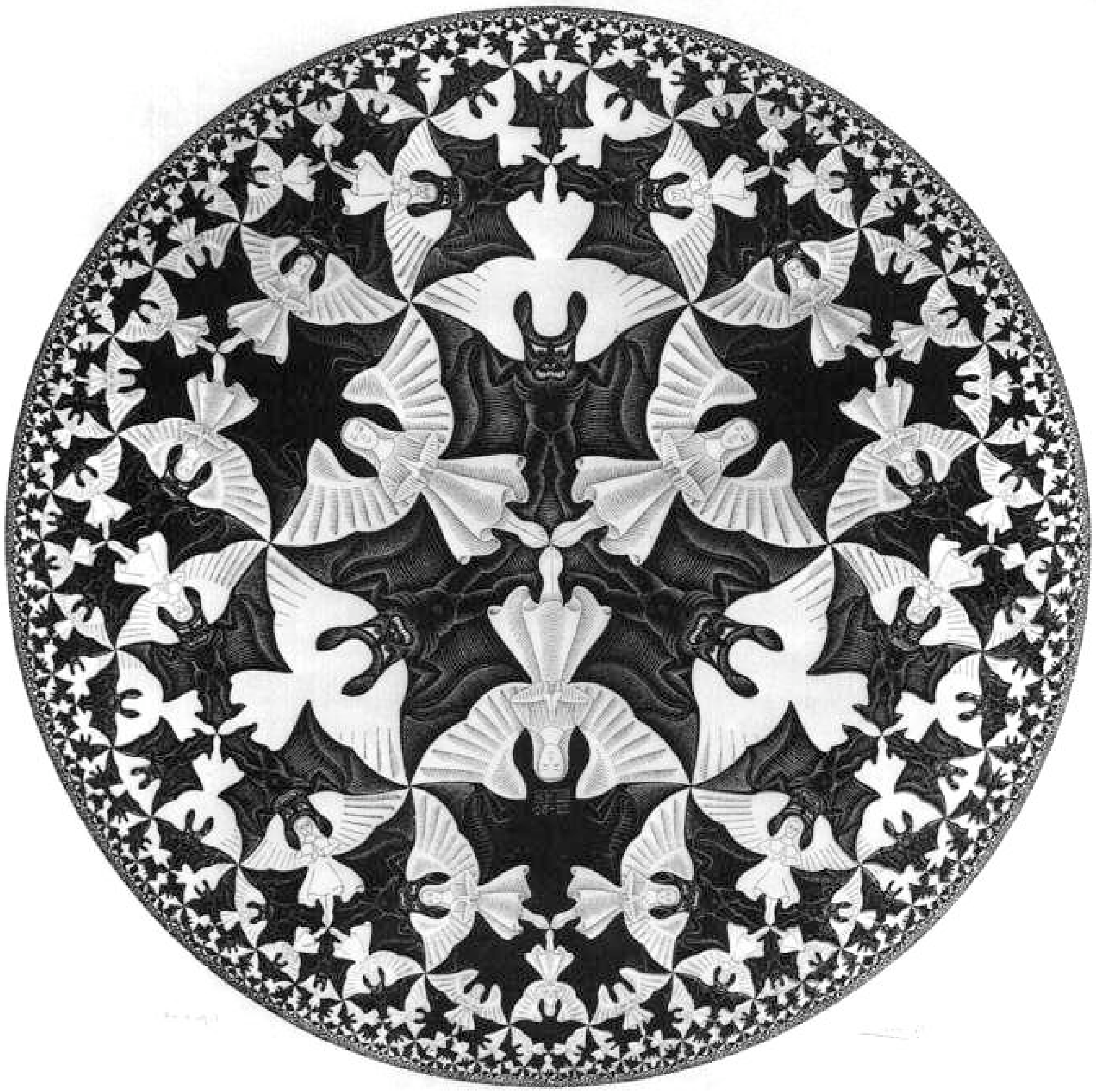


Eugenio Beltrami en 1868.

la géométrie elliptique (ou de Riemann) est consistante si la géométrie euclidienne l'est.

démonstration que l'axiome des parallèles est indécidable dans la géométrie absolue

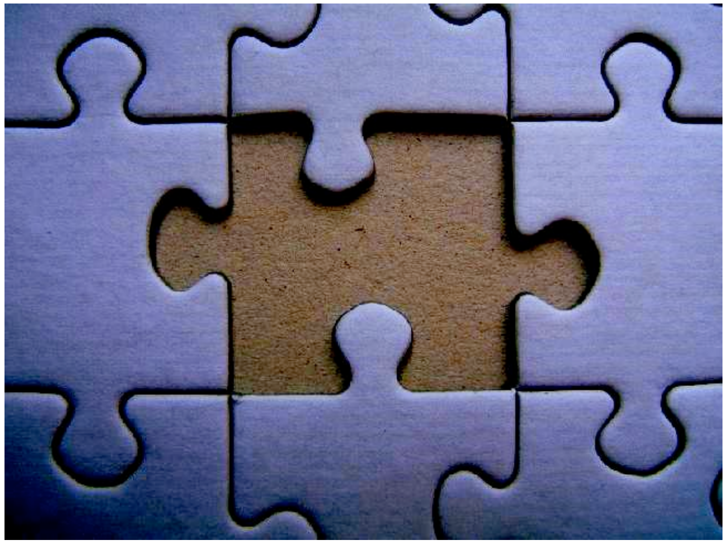




La géométrie sans le cinquième postulat est "**incomplète**"

Certains énoncés de cette géométrie sont "**indécidables**"

Il faut ajouter quelque chose !



L'axiome du choix

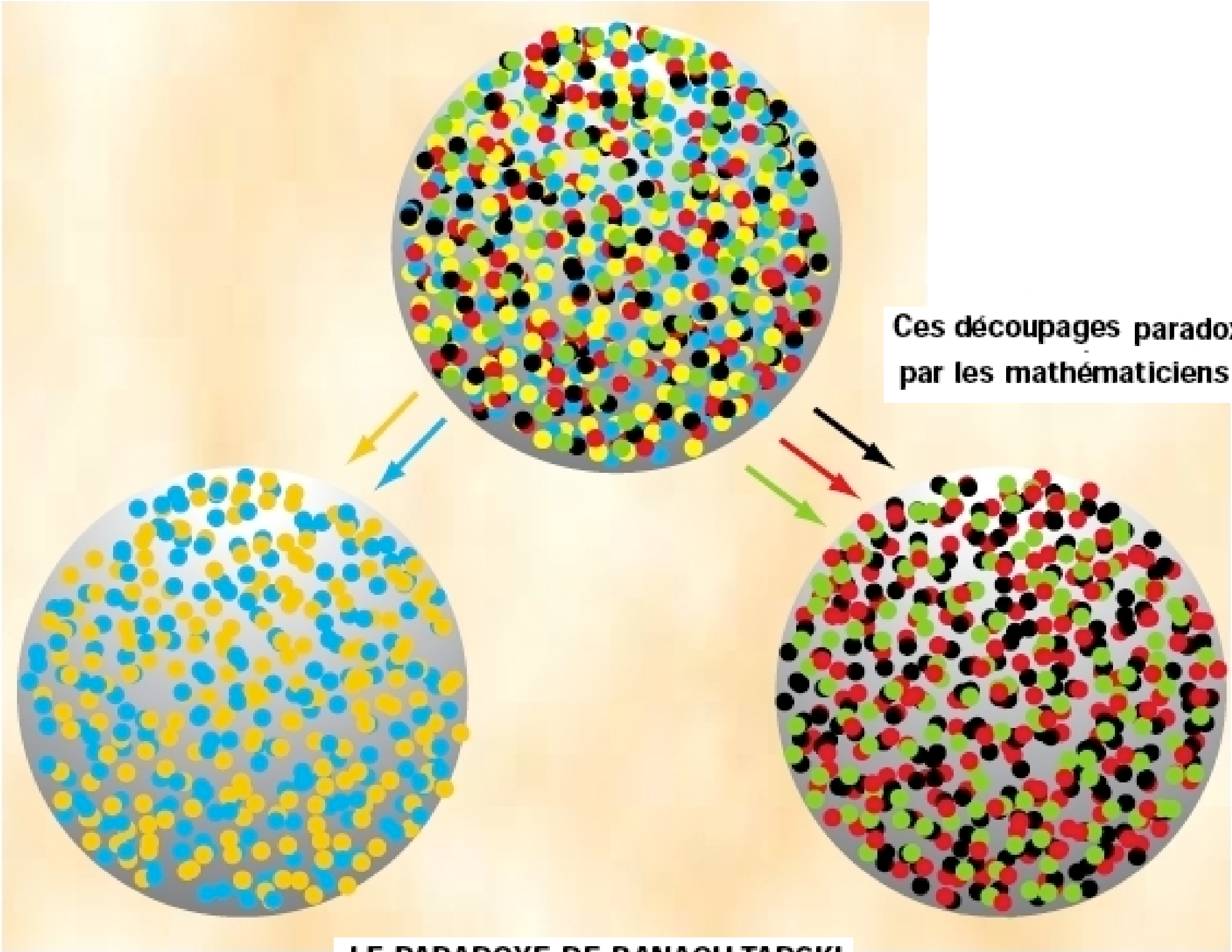
« Si E est un ensemble d'ensembles disjoints deux à deux et non vides, alors il existe un ensemble C qui possède un élément commun avec chaque ensemble de E. »

(C est obtenu en ***choisissant*** un élément dans chaque ensemble de E)

Exemple E = $\{\{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}, \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}, \{\boldsymbol{m}, \boldsymbol{n}\}, \{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}, \boldsymbol{E}\}\}$ C = $\{\boldsymbol{b}, 1, \boldsymbol{n}, \boldsymbol{E}\}$

Il est évident, et pourtant a d'étonnantes conséquences.

L'*axiome du choix* est impossible à déduire des autres axiomes de la théorie des ensembles (ZF)



Ces découpages paradoxaux ont été découverts en 1924 par les mathématiciens polonais Stephan Banach et Alfred Tarski.

LE PARADOXE DE BANACH-TARSKI

1924

L'Hypothèse du continu

L'échelle des infinis de Cantor

N est infini (**infini dénombrable**)

***P*(N)** est plus grand (c'est le même type d'infini que **R : l'infini du continu**)

***P*(*P*(N))** est plus grand (même type d'infini que celui des fonctions de **R** dans **R**)

***P*(*P*(*P*(N)))** est un infini plus grand encore,

etc.

Il y a au moins tous ces infinis.

Hypothèse du continu **HC** est l'affirmation :

il n'existe pas d'infinis intermédiaires entre N et **R** **(ou entre N** et *P*(**N**))

ou encore :

tout sous-ensemble infini de R se met en *correspondance un à un* avec N ou avec R

C'est assez concret :

- vous pouvez vérifier que toutes les parties de **R** auxquelles vous pensez se mettent bien en *correspondance un à un* avec **N** ou **R**.

- vous pouvez essayer de construire un ensemble infini intermédiaire entre **N** et de **R**.

$$\aleph_0 \quad 2^{\aleph_0} \quad 2^{2^{\aleph_0}}, \ldots, 2^{2^{2^{\cdots 2^{\aleph_0}}}} \quad \text{etc.}$$

La question de savoir s'il n'y a rien entre $\aleph_0$ et $2^{\aleph_0}$ peut donc s'écrire est-ce que $\aleph_1 = 2^{\aleph_0}$?

L'affirmation $\aleph_1 = 2^{\aleph_0}$ est appelée *hypothèse du continu.*

L'affirmation que pour tout i : $\aleph_{i+1} = 2^{\aleph_i}$ est appelée hypothèse généralisée du continu.

- G. Cantor pensait que HC était vraie et tenta en vain de la démontrer.

- K. Gödel lui pensait que HC était fausse.

- P. Cohen quoi que formaliste pensait plutôt qu'elle était fausse.

• 1938 **Kurt Gödel** montre que l'on peut ajouter l'hypothèse du continu (HC) à ZF sans introduire de contradiction.

Autrement dit : s'il existe un univers des ensembles conforme aux prescriptions de Zermelo-Fraenkel (ZF), il est certain qu'il existe aussi un univers des ensembles satisfaisant HC.

• 1963 **Paul Cohen** montre que l'on peut ajouter la négation de HC à ZF sans introduire de contradiction.

Autrement dit : s'il existe un univers des ensembles conforme aux prescriptions de Zermelo-Fraenkel, il est certain qu'il existe aussi un univers des ensembles ne satisfaisant pas HC.

En clair :

Les axiomes admis pour l'univers des ensembles ne permettent pas de savoir si HC est vraie ou non.

ZF est incomplet

Deux **interprétations** possibles :

- Les ensembles sont une création de l'esprit humain et les propriétés de l'infini (en particulier HC) sont laissées à son libre choix :

on peut, comme on veut, considérer que HC vraie, ou considérer que HC est fausse.

C'est la position formaliste.

- Les axiomes de ZF ne disent que partiellement ce que sont les ensembles. Il faut trouver de nouveaux axiomes. Quand on aura trouvé les bons et qu'on les ajoutera à ZF, on pourra alors déduire soit que HC est vraie, soit que HC est fausse.

C'est la position réaliste.

Cohen / Gödel

L'incomplétude générale de Kurt Gödel (1931)

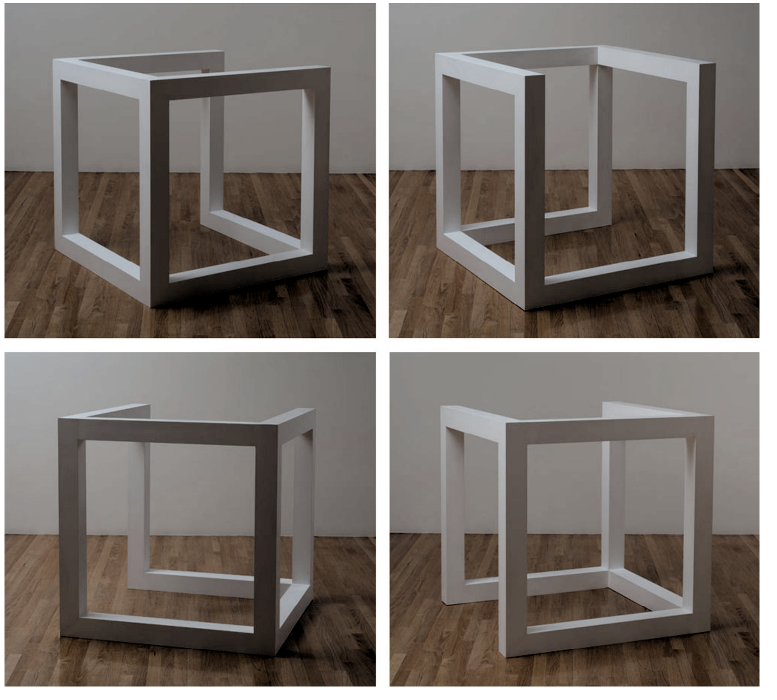
Les indécidables ne sont pas présents seulement en géométrie ou en théorie des ensembles.

Il y a toujours des indécidables :

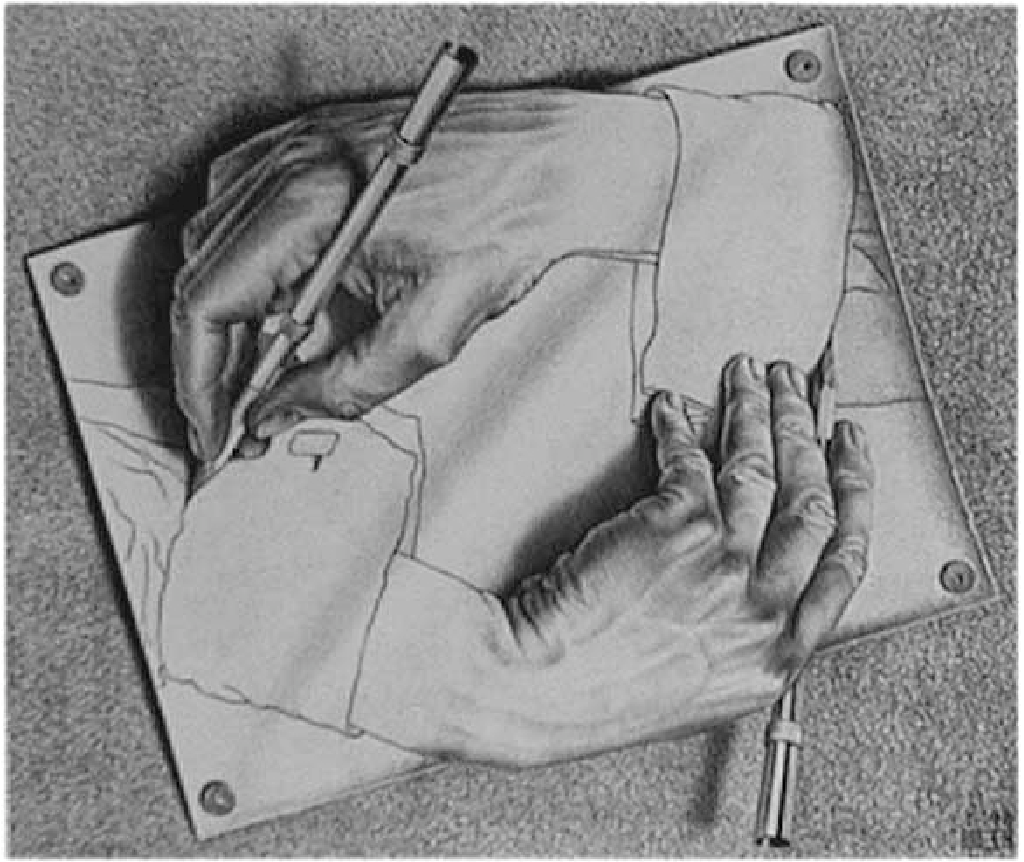
Tout système d'axiomes (intéressant) est incomplet

Il y a toujours des énoncés vrais et ***impossibles*** *à démontrer*

L'incomplétude est générale

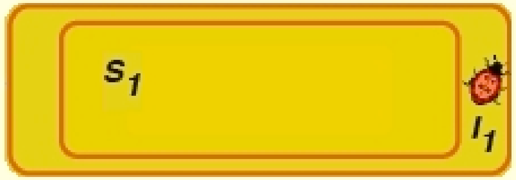


Kurt Gödel (1906-1978)



E : « E n'est pas démontrable dans S »

THÉORÈME DE GÖDEL



Si un système formel permet de faire de l'arithmétique et qu'il est consistant (c'est-à-dire qu'il ne se contredit pas), alors il existe des énoncés *I* dont *S* ne peut démontrer ni qu'ils sont vrais, ni qu'ils sont faux (on les appelle des indécidables de *S*).
Le théorème de Gödel permet de construire explicitement un tel indécidable *I* (sa démonstration est fondée sur l'écriture d'un énoncé codant dans *S* l'affirmation : "je ne suis pas démontrable dans *S*").

L'incomplétude ouvre une ère nouvelle :

"Ce qui est vrai pour les nombres entiers est impossible à déduire d'un nombre fini de règles de raisonnements fixées à l'avance."

"Il est impossible de définir une notion de preuve mathématique générale".

"Les mathématiques ne sont pas complètement formalisables (axiomatisables)"

L'incomplétude est partout

- **La consistance est indécidable (Gödel).**

- **La "complexité" est indécidable (Kolmogorov, Levin, Chaitin)**

"K(s) = n" est toujours indécidable (sauf pour un nombre fini de s).

Le nombre *Oméga* de Chaitin

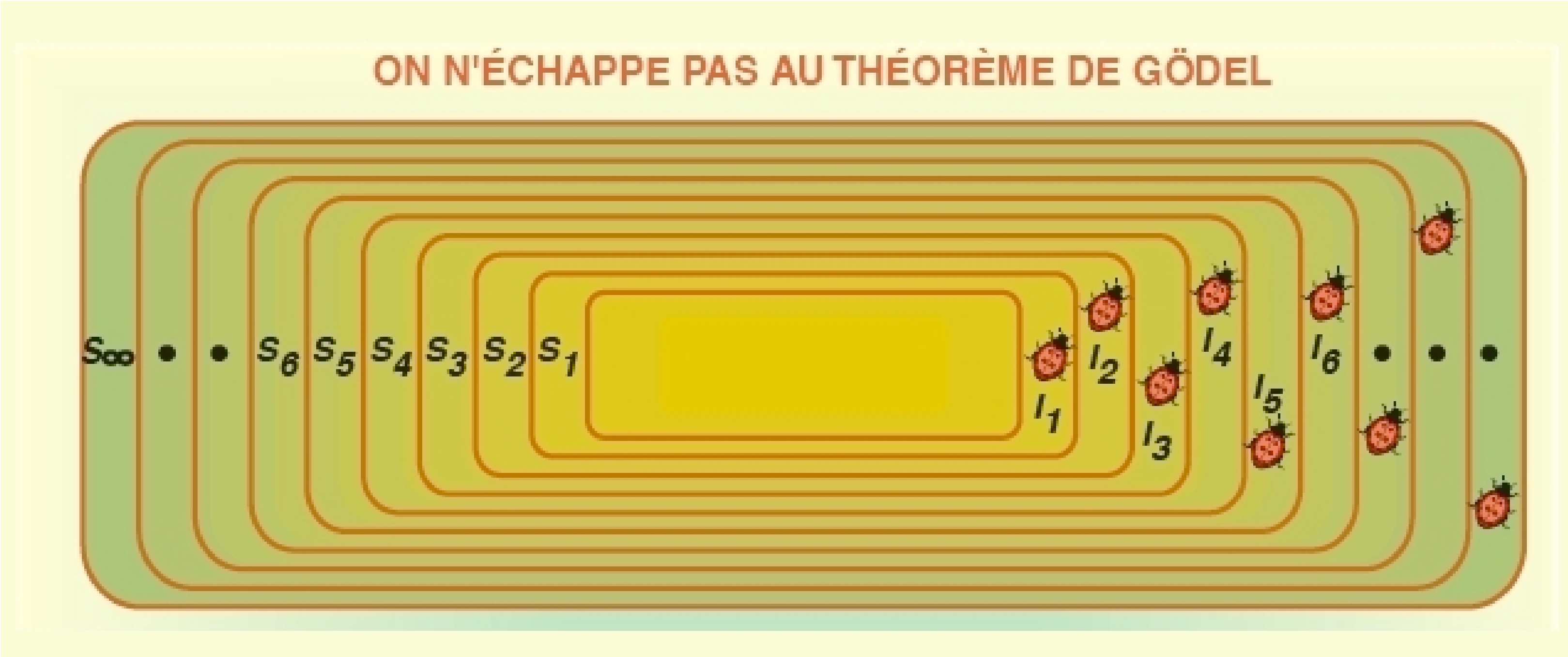
***Oméga* = probabilité de l'arrêt d'une machine universelle à laquelle on donne des programmes choisis au hasard.**

Oméga est : ***irrationnel, transcendant, incalculable, aléatoire***, ***normal***, ***incompressible***

Un système formel ne "connaît" qu'un nombre fini de chiffres du nombre ***Oméga***.

***Oméga* est mathématiquement inconnaissable** !

Le comble de l'incomplétude mathématique !



Le théorème de Gödel est en réalité un théorème d'*incomplétabilité*

- si vous ajoutez quelques axiomes : ça ne complète pas ;

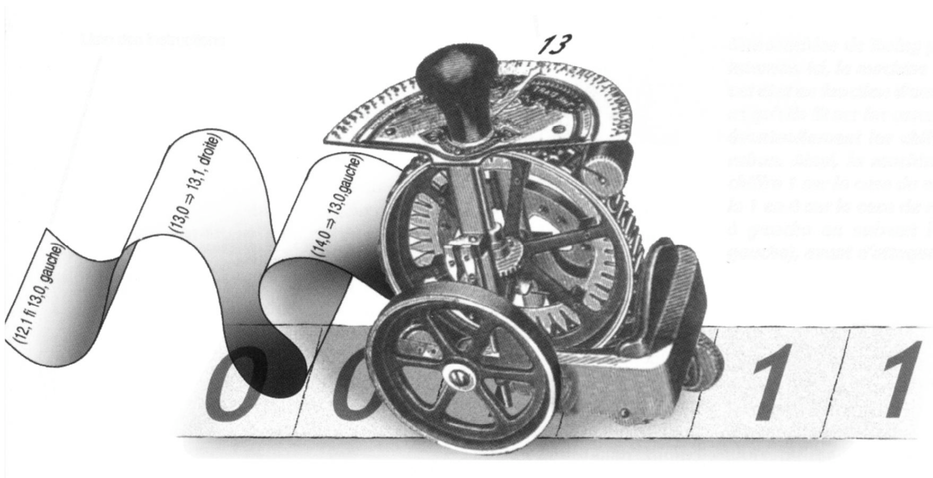
- si vous en ajoutez une infinité par un moyen bien déterminé (algorithmique) :
ça ne complète pas ;

Leonid Levin a démontré une forme encore plus forte de l'incomplétabilité :

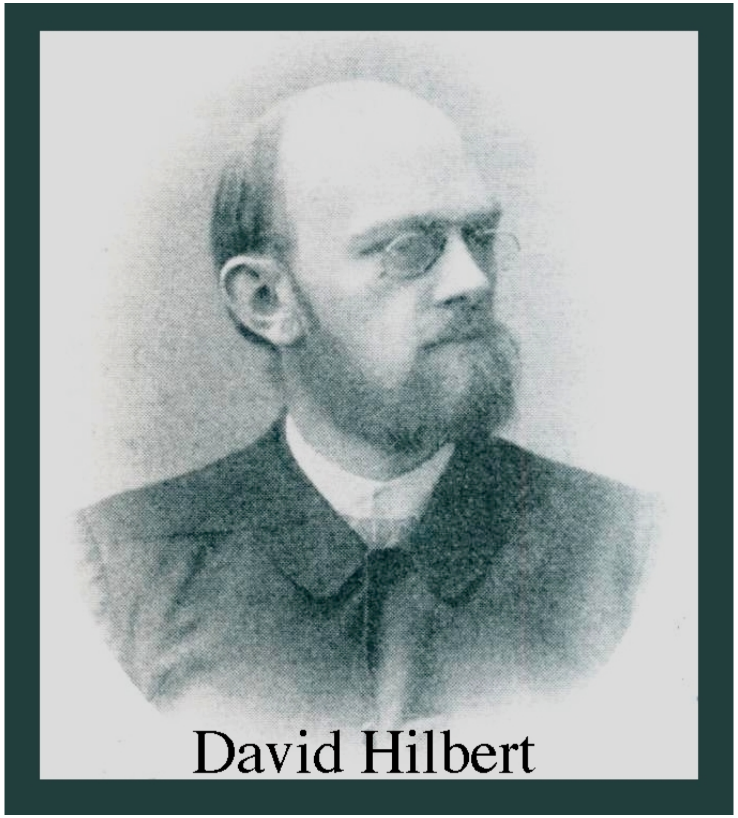
- même si vous utilisez un moyen associant algorithmes et tirages au sort :

ça ne complète pas.

Incalculabilité



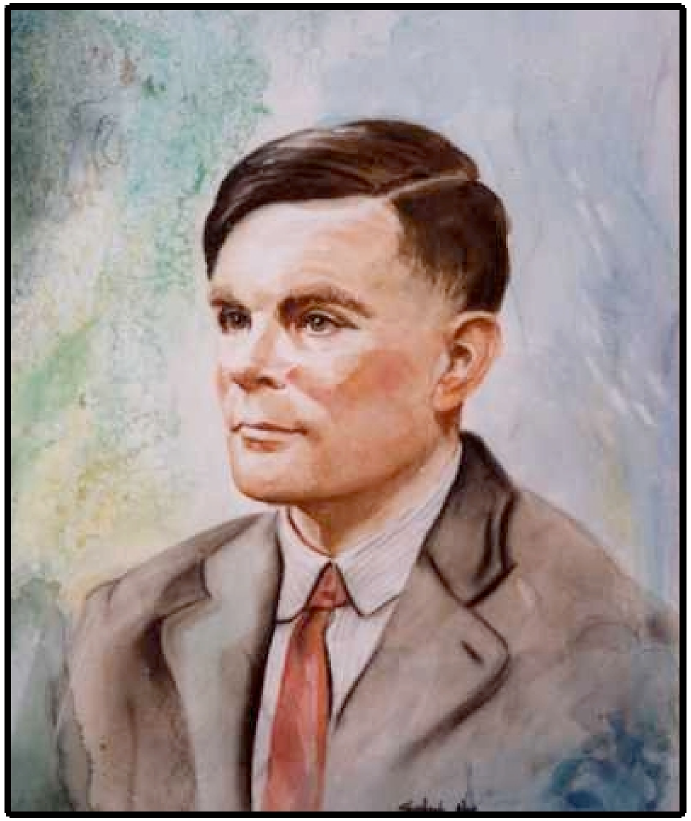
Dixième problème de David Hilbert



1900

«Trouver une méthode qui pour toute équation polynomiale à coefficients entiers indique si, OUI ou NON, elle possède des solutions. »

Exemple : pour $x^2 + y^2 = 10$ la réponse est **oui** ($x = 3$; $y = 1$)



Alan Turing (1912-1954)

Méthode = Algorithme = ce qui est calculable par machine (de Turing)

(thèse de Turing, 1936)

Alan Turing : indécidabilité de l'arrêt d'un programme (1936)

Le *Dixième problème de Hilbert* (posé en 1900) est résolu en 1970 par Youri Matiiassevitch

Des milliers de problèmes sont connus algorithmiquement indécidables.

Il existe des fonctions f de **N** dans **N**, bien définies, mais qu'aucun algorithme ne peut calculer.

Procédé diagonal

f_n n-ième fonction calculable de N dans {0, 1}

$g(n)$ non définie si $f_n(n) = 0$ ou 1

$g(n) = 0$ si $f_n(n)$ non définie

g est parfaitement bien définie,

g n'est pas calculable car différente de tous les f_n

Attention !

Être une *proposition indécidable* est toujours relatif.

Il n'y a pas de propositions absolument indécidables.

Être une *problème algorithmiquement indécidable* est absolu.

... mais le problème comporte une variable.

Liens entre *incomplétude* et *incalculabilité*

Soit S est un système de démonstrations fixé.

Soit P est un problème algorithmiquement indécidable (dépendant d'un paramètre *n*)

(n -> vrai ou faux selon que P(n) est vrai ou faux n'est pas calculable)

Alors parmi tous les énoncés vrais correspondant au problème P,

il y en a un au moins qui est un indécidable de Gödel relativement à S.

Supposons que tous les énoncés concernant P sont démontrables dans S.

Soit alors l'algorithme:

- pour toute *n*, rechercher dans la liste de toutes les démonstrations de S celle qui démontre que « P pour la donnée *n* est vrai » ou celle qui démontre que « P pour la donnée *n* est faux ».

L'hypothèse que tous les énoncés concernant P sont démontrables dans S, signifie que quelle que soit la donnée *n*, l'algorithme décrit s'arrêtera avec la bonne réponse.

On aurait donc un algorithme pour le problème P, ce qui est une contradiction avec l'hypothèse que P est indécidable.

Conclusion : parmi les énoncés vrais associés au problème P, il y en a donc un (au moins) qui est vrai et non démontrable dans S.

Grâce à ce raisonnement, on est certain que dans tout système S, il y a un énoncé de la forme :

« la machine de Turing T ne s'arrête pas »

ou de la forme : **« la machine de Turing T »**

qui est vrai mais indémontrable dans S.

On obtient aussi que dans tout système S

- il y a une équation diophantienne dont on ne peut ni démontrer qu'elle possède des solutions, ni démontrer qu'elle n'en possède pas,

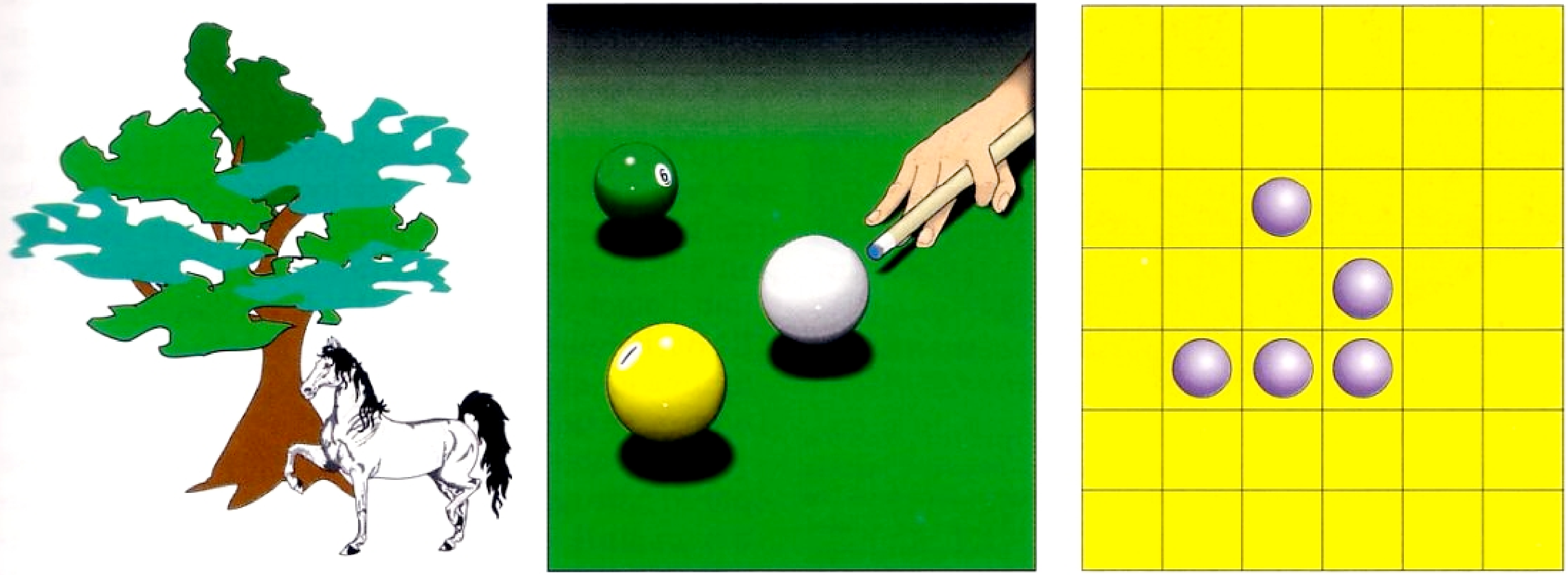
- il y a une configuration du jeu de la vie dont il est impossible d'établir si elle est éternelle ou pas,

etc.

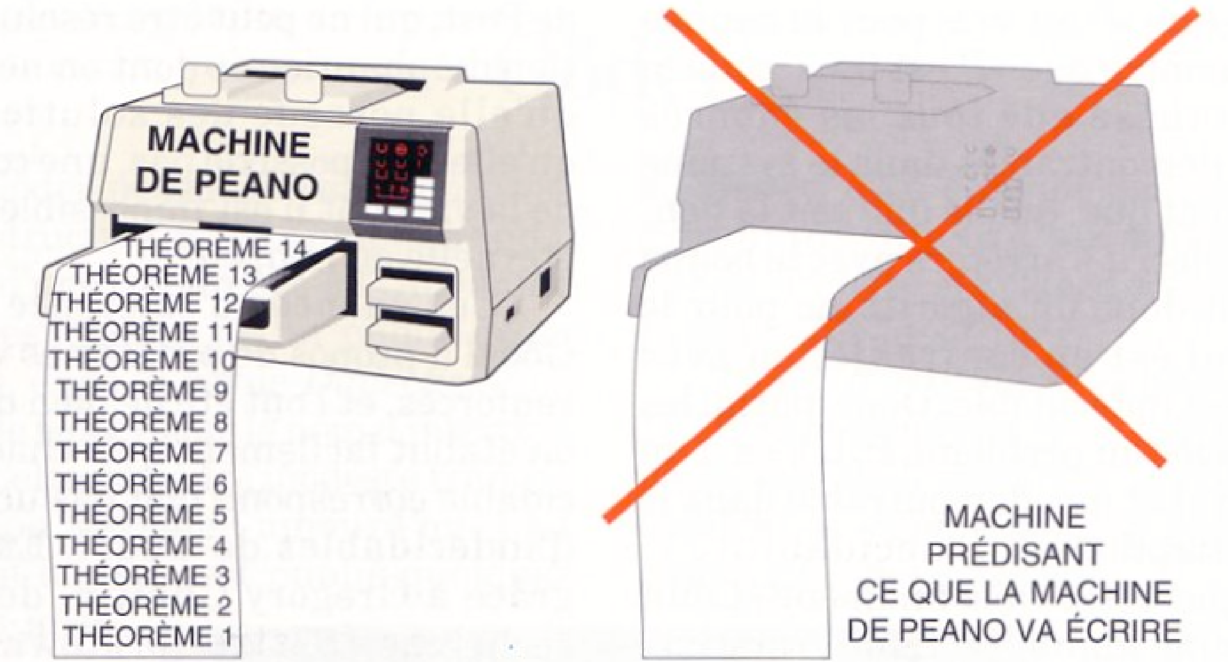
Plus fort : À chaque problème indécidable correspond en fait une infinité d'indécidables de Gödel.

On connaît grâce à Chaitin des problèmes "fortement" indécidables :

tous les énoncés qui leur correspondent sont des indécidables sauf un nombre fini.



TROIS TYPES DE RAISONS s'allient pour empêcher la prévision du futur. La mécanique quantique est à l'origine d'une imprécidibilité fondamentale : par exemple, dans le monde physique *(à gauche)*, on ne peut prévoir à la fois la position et la vitesse d'une particule ; de ce fait, on ne peut pas connaître le futur d'un système simple composé d'une seule particule, et, *a fortiori*, celui de systèmes complexes tels que les êtres vivants. Dans l'univers simplifié de la mécanique classique *(au milieu)*, les physiciens ont également observé que la prévision des phénomènes est impossible : pour prévoir le comportement d'une boule de billard, par exemple, il faudrait connaître avec une précision infinie l'angle de la queue, l'impulsion communiquée à la boule, etc. Enfin, même dans les univers simplifiés à l'extrême tels que celui du Jeu de la vie *(à droite)*, la prévision est impossible en raison de l'indécidabilité mathématique.



UN SYSTÈME FORMEL peut être considéré comme une machine qui produit des théorèmes. Le théorème de Gödel stipule qu'on ne pourra jamais concevoir de machine qui n'énoncerait que des théorèmes d'arithmétique exacts, et qui les énoncerait tous. Notamment la «machine de Peano» (associée au système formel de l'arithmétique de Peano) n'énumère pas tous les théorèmes de l'arithmétique. Le théorème de Church énonce un résultat différent : ce que la machine de Peano écrit sur sa feuille infinie est imprévisible ; il n'existe aucune machine qui, pour tout énoncé d'arithmétique, indique en un temps fini si, oui ou non, la machine de Peano écrira l'énoncé. Qu'il existe des énoncés vrais n'apparaissant pas sur le listing de la machine de Peano, c'est l'indécidabilité de Gödel ; qu'une machine comme la machine de droite ne puisse exister, c'est l'indécidabilité du système formel de l'arithmétique de Peano.

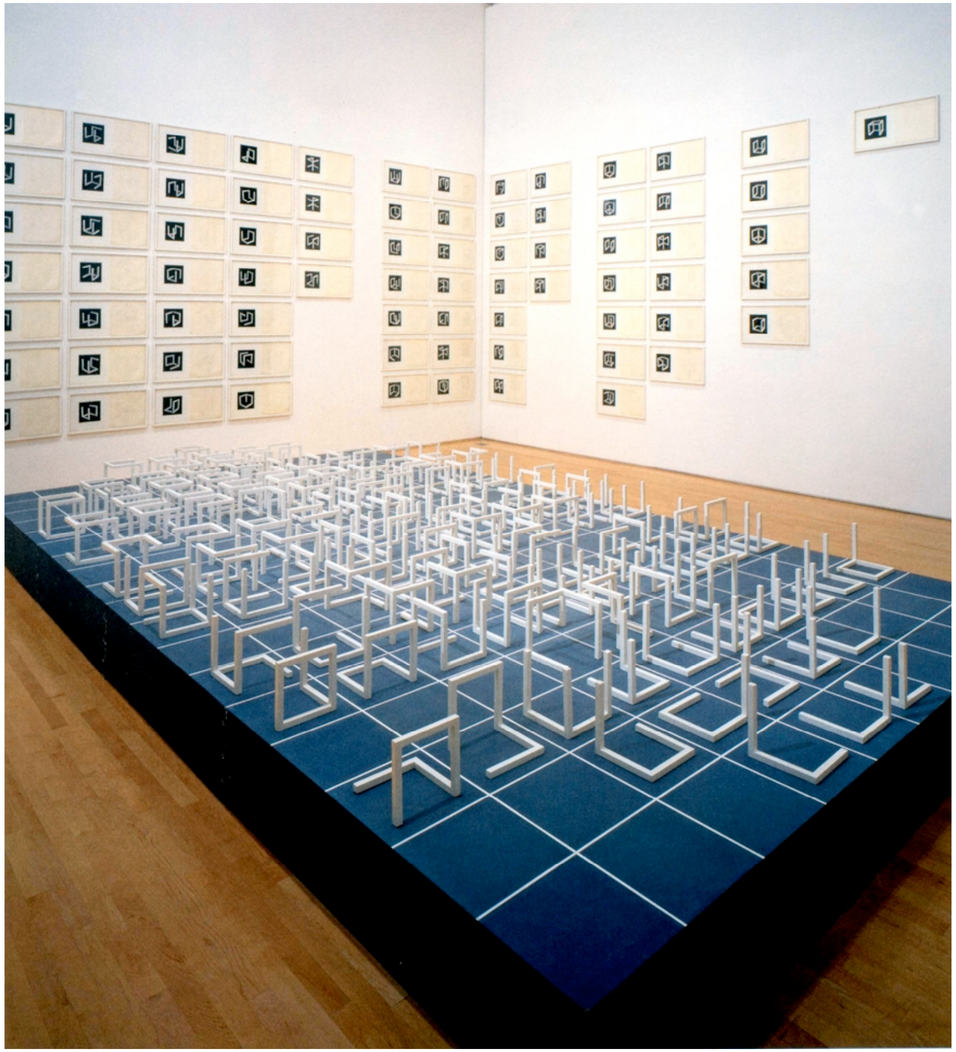
Conclusions :

- *L'incomplétude est partout en mathématiques et c'est en réalité une « incomplétabilité »*

- *La logique mathématique en donne une compréhension de plus en plus fine et profonde et la relie à la complexité.*

- *L'informatique y est confrontée car indécidabilité et incalculabilité sont liées.*


Dr Kurt Gödel



Sol DeWitt Incomplete open cubes