Logique

fondements, applications, perspectives

Les sept merveilles de la logique

http ://www.dirk-k-lange.de/PSC/

FIG. 1 – *Explication logique* - Siegfried Jegard (2005)

Matthieu Deconinck
Dirk Lange
Olivier Marfaing
Matthieu Rambaud
Jimena Royo-Letelier

Table des matières

Introduction

Pangloss enseignait la métaphysico-théologo-cosmolonigologie. Il prouvait admirablement qu'il n'y a pas d'effet sans cause, et que, dans ce meilleur des mondes possibles, le château de monseigneur le baron était le plus beau des châteaux et madame la meilleure des baronnes possibles. « Il est démontré, disait-il, que les choses ne peuvent être autrement : car, tout étant fait pour une fin, tout est nécessairement pour la meilleure fin. Remarquez bien que les nez ont été faits pour porter des lunettes, aussi avons-nous des lunettes. Les jambes sont visiblement instituées pour être chaussées, et nous avons des chausses. Les pierres ont été formées pour être taillées, et pour en faire des châteaux, aussi monseigneur a un très beau château ; le plus grand baron de la province doit 1etre le mieux logé ; et, les cochons étant faits pour être mangés, nous mangeons du porc toute l'année : par conséquent, ceux qui ont avancé que tout est bien ont dit une sotise ; il fallait dire que tout est au mieux. »

***Voltaire**,Candide*

L'histoire de notre groupe de *Projet Scientifique Collectif* est peut-être un peu particulière dans le sens où l'idée du sujet est apparue avant que l'équipe ne se forme. En effet, nous étions tous attirés par différents thèmes intellectuellement fascinants comme la théorie des modèles, la logique quantique ou le théorème de Gödel. Nous souhaitions également aborder une matière qui n'est que rarement enseignée en tant que telle : *la logique*.

Notre perspective pendant ces 7 mois a été la suivante : la logique est une discipline encore plus abstraite que les mathématiques, il est donc particulièrement intéressant d'en présenter les enjeux, les perspectives et les applications afin de montrer que cette discipline ne relève pas uniquement du domaine intellectuel.

Cette science présentant de multiples facettes, il nous a semblé clair que dans le cadre d'un PSC il fallait se limiter à quelques aspects traités en profondeur plutôt que de « lister » un grand nombre de résultats que nous n'aurions pu approfondir par manque de temps.

Faire des choix n'est pas toujours facile et ici tout particulièrement parce qu'il fallait nous restreindre tout en montrant la richesse de la logique, ses applications à différents domaines (pas seulement les mathématiques) et le développement important qu'elle a connu ces deux derniers siècles. Nous tenons ici à remercier tout particulièrement notre tuteur M.Yves Laszlo pour les nombreuses pistes qu'il nous a indiquées.

L'étude que nous présentons ne se veut donc pas exhaustive (même au sein des différents domaines abordés) ; l'objectif est d'initier le néophyte à certains aspects de cette science ancienne mais encore très dynamique. Nous avons mis l'accent sur un certain nombre de résultats particulièrement surprenants.

Ce dossier a été construit de manière à pouvoir être lu de manière non-linéaire. Le premier chapitre (*Il était une fois... la logique* page 11) est central car il explicite la cohérence du tout et renvoie à chacune des six autres parties dont le détail est donné ci-dessous. Ces derniers sont regroupés dans trois grandes thématiques (enjeux, applications et perpectives) mais peuvent être lus indépendamment les uns des autres.

Logique
enjeux, applications et perspectives

« Sept merveilles de la logique : »

I. Il était une fois... la logique (page 11)

« Qu'est ce que la logique ? »

La logique est dans une première approche l'étude des règles formelles que doit respecter toute déduction correcte. Ainsi, elle s'occupe de la validité d'un raisonnement du point de vue de sa structure et donc ne regarde pas dans un premier temps le contenu des énoncés utilisés pour le raisonnement. On parle aussi de la « logique formelle ».[1]

Cette définition soulève deux points très importants :
- la logique est une science des structures ; *a priori* elle ne s'intéresse pas à la signification de ses objets d'études. Ce point de vue sera particulièrement important dans les parties sur le théorème de Gödel (page 49) et la théorie des modèles (page 99).
- le terme « déduction » implique une structure du raisonnement bien particulière : en effet on doit toujours déduire « à partir de quelque chose » ; ainsi cette structure présuppose l'existence de postulats, d'axiomes sur lesquels on peut initier un raisonnement.

Cette partie prend la forme d'un petit parcours historique qui détaille comment et pourquoi « l'axiomatique » s'est développée depuis l'âge des Grecs jusqu'aux grands développements de la logique du XIXème et du XXème siècle (paradoxe de Russell,

[1] définition de *Enzyklopedie in 15 Bänden*.2007

théorème de Gödel, théorie des modèles). On montre notamment comment la résolution des paradoxes logiques peut être source de progrès considérables. Un exemple est présenté dans la partie *Le paradoxe aux cent têtes* (page 17).

II. Le paradoxe aux cent têtes (page 17)

« *Cette phrase est fausse* »

Cette phrase est-elle vraie ou fausse ?

- Paradoxe du Crétois
- Paradoxe du menteur (ou d'Epiménide)
- Paradoxe du barbier
- Paradoxe de Grelling-Nelson
- Paradoxe de Richard
- Paradoxe de Berry
- Paradoxe de Russell

. . .autant de versions du « paradoxe de l'auto-référence ».

Dans cette partie nous présentons le processus de construction de la théorie des ensembles (axiomatique Z-F) et nous montrerons en quoi il est intimement lié à la résolution de ce paradoxe.

III. La multiplication des pains (page 37)

Le paradoxe de Banach-Tarski
ou
« *Comment découper une grenouille pour fabriquer un boeuf avec les morceaux* »

Nous nous intéressons ici à une conséquence assez spectaculaire de l'axiome du choix indénombrable : *le paradoxe de Banach-Tarski* (en fait il s'agit plus d'un théorème contre-intuitif que d'un véritable paradoxe). Il montre notamment qu'accepter (ou refuser) l'axiome du choix peut être lourd de conséquences.

IV. Le chapitre IV n'est pas démontrable (page 49)

Premier théorème d'incomplétude de Gödel

Le théorème de Gödel (1931), qui utilise le paradoxe de l'auto-référence, constitue l'un des résultats les plus spectaculaires du XXème siècle. Il montra en effet que toute théorie mathématique tentant de décrire les nombres entiers était nécessairement incomplète ; c'est à dire qu'il existe des théorèmes formulables en son sein que cette théorie ne peut ni démontrer ni infirmer. Nous présenterons ici la démonstration de ce résultat.

V. L'explosion convergente (page 79)

Les suites de Goodstein

Les suites de Goodstein sont un exemple explicite de question indécidable au sein de l'arithmétique de Peano. Ce sont des suites qui gonflent jusqu'à des tailles gigantesques... avant de converger vers 0. Pour démontrer cette propriété il est nécessaire d'introduire des nombres infinis : les ordinaux.

VI. Les Mille et un théorèmes (page 99)

La théorie des modèles

La théorie des modèles est un outil extrêmement puissant de démonstration.

Elle étudie les propriétés syntaxiques des formules mathématiques pour exprimer les relations entre ces dernières et les structures algébriques qui les satisfont. Nous traiterons l'exemple du théorème d'Ax.

VII. Une porte doit être ouverte et fermée (page 111)

logique quantique

La logique quantique est une très belle construction de l'esprit qui prolonge naturellement la logique usuelle. Elle permet aussi de faire tourner, sur le papier, des algorithmes beaucoup plus performants que ceux que nous connaissons. Une question subsiste : verrons-nous un jour fonctionner un ordinateur quantique ?

Le dossier est également disponible sur notre site web :

http ://www.dirk-k-lange.de/PSC/

Celui-ci contient une brève présentation du groupe et de nos motivations, l'ensemble des sept chapitres dans des fichiers séparés ainsi que les supports pédagogiques que nous avons créés à l'occasion des trois exposés donnés au Séminaire Des Elèves (Théorie des Modèles, Théorème de Gödel et Suites de Goodstein).

FIG. 2 – L'Université au Moyen-Age (La logique - La rhétorique)

Chapitre 1

Il était une fois... la logique

« On passe sa vie à romancer les motifs
et à simplifier les faits. »
Boris Vian

Dahan-Dalmedico et Pfeiffer écrivent dans leur livre [5] *Histoire des mathématiques - Routes et dédales* que « les débuts de la philosophie et de la science déductive se sont développés à Milet, puissante ville marchande et riche centre intellectuel largement ouvert aux influences orientales ». Selon [5] (p.41), c'est avec l'école ionienne et surtout avec Thalès que « les objets de discussions, les propositions mathématiques ne sont plus de simples énoncés traduisant des faits empiriques mais nécessitent désormais une démonstration qui conduit, d'une ou de plusieurs propositions, dites prémisses, à une conclusion nécessaire ». L'histoire des preuves dans les mathématiques semble commencer environ à cette époque.

Platon (427-347 avant J.-C.) et les platoniciens sont les premiers à être pleinement conscients du caractère abstrait des objets mathématiques et Platon s'interroge sur la nature et la structure des mathématiques. Les platoniciens commencent à distinguer entre « monde réel » et « monde des idées ». C'est dans le « monde des idées » qu'ils cherchent les connaissances vraies et pas dans le monde réel où on ne peut regarder que des réalisations souvent très imparfaites, très insuffisantes des objets de la pensée : il est par exemple impossible de *tracer* une droite (qui est un objet d'une longueur infinie !) ou un cercle parfait dans le « monde réel ». Cette perception des mathématiques selon laquelle tout se passe dans la pensée a des conséquences pour les méthodes de démonstrations : il est strictement interdit d'utiliser une expérience pour une démonstration mathématique car une expérience ne peut se passer que dans le « monde réel » et pas dans le « monde des idées ». Par conséquent, les platoniciens n'acceptent que des raisonnements déductifs qui conduisent à des résultats absolument certains si les prémisses sont correctes et ce choix transforme les mathématiques.

Un peu plus tard, Aristote (384-322 avant J.-C.) écrit « savoir, c'est connaître par le moyen de la démonstration » et commence à distinguer les définitions, les axiomes, les hypothèses et soulève le problème de l'existence des objets définis car définir un objet ne garantit pas nécessairement l'existence de l'objet en question. Il écrit dans *secondes analytiques, Livre I* [1] :

[1] les exemples proposés ne sont pas d'Aristote mais de l'auteur de ce document

Aristote : définitions et éléments de la démonstration :

- Toute connaissance rationnelle, soit enseignée, soit acquise, dérive toujours de notions antérieures (par exemple la notion de triangle dérive de la notion de point)
- Les notions antérieures ne peuvent être nécessairement que de deux espèces (qui ne s'excluent pas mutuellement) : ou bien, c'est l'existence même de la chose qu'il faut préalablement connaître, ou bien, c'est le nom seul de la chose qu'il faut comprendre (par exemple en géométrie il faut supposer l'existence d'objets qu'on appelera points ou droites).
- J'appelle thèse d'un principe syllogistique immédiat la proposition qui ne peut pas être démontrée, et qu'il n'est pas indispensable de connaître pour apprendre quelque chose (par exemple la proposition « ce triangle est rouge » qui ne relève pas de la géométrie) ; celle au contraire que l'on doit nécessairement connaître pour apprendre quelquechose, je la nomme axiome (par exemple « par deux points ne passent qu'une droite »).
- La thèse qui prend l'une quelconque des deux parties de l'énonciation, c'est-à-dire qui affirme ou qui nie l'existence de l'objet, reçoit le nom d'hypothèse. La thèse qui est dénuée de ces conditions, est une définition.

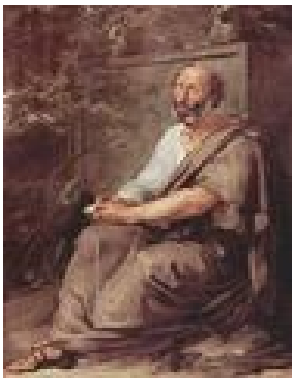


FIG. 1.1 – Aristote

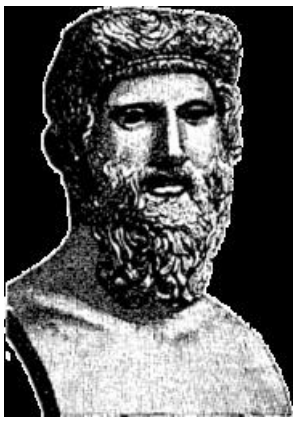


FIG. 1.2 – Platon

Pour conclure cet intermezzo grec, il faut mentionner « les Eléments » d'Euclide (365-300 avant J.-C.), un ouvrage constitué de 13 livres. Bien qu'aujourd'hui on soit presque sûr qu'Euclide n'en est pas l'unique auteur, ils ont une importance faramineuse pour les mathématiques, car sa méthode de dériver des propriétés d'objets géométriques et des nombres naturels à partir d'un système d'axiomes est assez remarquable. De plus cette méthode revêtait un caractère symbolique qui en a fait une référence pendant plus d'un millénaire.

Conclusion :
Déjà à l'époque d'Euclide, on a des systèmes d'axiomes , des « notions premières » qui forment la base des mathématiques et desquels on déduit des propositions, des théorèmes. **cf *La théorie des ensembles et le processus d'axiomatisation* page 17**

Faisons maintenant un grand pas dans le temps pour nous retrouver au mil-

lieu du XIXème siècle. Avec son ouvrage *The Mathematical Analysis of Logic* (1847), George Boole (1815 - 1864) créa le premier calcul algébrique en logique ce qui lui valut l'appellation de « père de la logique moderne des mathématiques », laquelle logique se distingue de la logique philosophique par une formalisation conséquente.

En 1872, Georg Cantor (1845-1918) définissait la notion d'ensemble : *« un ensemble est une collection d'objets particuliers, bien distingués de notre conception ou de la pensée. Ces objets qui donc font partie de cet ensemble s'appellent éléments. »*. Ainsi, Cantor avait créé ce qu'on appelle aujourd'hui la théorie naïve des ensembles. Mais cette définition d'un ensemble peut amener à des contradictions, surtout quand on commence à regarder des ensembles qui peuvent se contenir eux-mêmes. Un exemple symptomatique de telles contradictions est le paradoxe du barbier (ou du menteur) encore appelé antinomie de Russell (cf *Le paradoxe aux cent têtes* page 17).

FIG. 1.3 – Georg Cantor

En 1902, Russell présenta ce paradoxe dans une lettre à Gottlob Frege qui à l'époque venait de publier un ouvrage dans lequel il avait construit une axiomatique pour la théorie des ensembles. L'oeuvre de Frege était donc incohérente. Le problème soulevé par le paradoxe de Russell ne fut résolu que quelques années plus tard. En effet en 1908, Ernst Zermelo publie un système axiomatique pour la théorie des ensembles qui, en 1922, est complété par un ouvrage de Abraham Fraenkel. Ce système, appelé « système de Zermelo-Fraenkel », évite l'antinomie de Russell (cf *Le paradoxe aux cent têtes* page 17).

On peut résumer le processus ainsi :
- Au début, il y a une définition (Cantor)
- A partir de cette définition on crée une axiomatique (Frege)
- Russell montre avec son paradoxe que cette axiomatique est contradictoire
- On améliore l'axiomatique et on retourne à l'étape deux (Zermelo-Fraenkel)

On peut se demander ce qu'a apporté ce petit épisode à l'histoire des sciences. Tout d'abord, le « système de Zermelo-Fraenkel » (en fait un système quasiment équivalent) est à la base des Mathématiques actuelles.
Ensuite, afin de résoudre son paradoxe Russell a inventé la théorie des types[2] ; ainsi

[2]selon cette théorie il y a des ensembles simples, qui ne peuvent contenir que des éléments simples mais pas des ensembles. Des ensembles qui contiennent des ensembles simples et des éléments

même si c'est de manière fortuite le paradoxe de Russell a été source de progrès dans un domaine apparement assez éloigné de celui dont il est issu[3].
Enfin ce paradoxe a soulevé deux points fondamentaux de la recherche d'axiomes. En effet peut-être subsiste-t-il au sein du système de Zermelo-Fraenkel d'autres paradoxes auxquels personne n'a pensé. Peut-on vraiment être sûr que ce système est libre de contradictions ? Ensuite ce sytème est-il assez puissant ? En d'autres termes est-il capable de démontrer tous les théorèmes vrais et d'infirmer tous les théorèmes faux ?

C'est ici que David Hilbert et Kurt Gödel entrent en scène. Le lecteur attentif aura remarqué que les questions que nous venons de soulever ne sont pas *stricto sensu* de nature mathématique ; en effet elles portent sur le langage mathématique. Cette étude de la syntaxe des mathématiques s'appelle les *métamathématiques*.

FIG. 1.4 – David Hilbert, 1912

FIG. 1.5 – Kurt Gödel

Le « programme de Hilbert » formulé entre 1920 et 1922 par David Hilbert est d'ailleurs d'ordre métamathématique. Il réclame de baser les mathématiques sur un système d'axiomatique libre de contradictions et complet. Hilbert voulait redéfinir les mathématiques comme « système formel ». Dans ce système, on pourrait ainsi automatiser le processus de démonstration : on se donne des axiomes et des règles de transformation ; tout théorème vrai pourrait être déduit en transformant les axiomes avec ces règles et jamais ce procédé ne permettrait de prouver quelque chose et son contraire.

Ce projet intéresse de nombreux mathématiciens. Cependant leur travail sera interrompu de manière tout à fait surprenante et alors inédite. En 1931, Kurt Gödel démontre qu'un système formel non-contradictoire et suffisamment riche pour inclure l'arithmétique est incomplet et ne peut démontrer sa cohérence en s'appuyant sur ses axiomes.

Le « *Gödelsche Unvollständigkeitssatz* » publié dans le fameux article « *Über formal unentscheidbare Sätze der Principia mathematica und verwandter Systeme* » a eu un impact considérable tant en philosophie qu'en Mathématiques ; il est consi-

appartiennent au deuxième type. Des ensembles qui peuvent contenir des ensembles du deuxième type appartiennent au troisème type etc. Dans ce système la création de l'ensemble qui contient les ensembles qui ne se contiennent pas eux-mêmes est impossible pour des raisons syntaxiques.

[3]ce phénomène est récurrent dans l'histoire des sciences

déré comme l'un des grands théorèmes du vingtième siècle. Nous présenterons la démonstration de Gödel : *Le Chapitre IV n'est pas démontrable* page 49.

Ce théorème est un théorème métamathématique, Gödel a dû donner une définition rigoureuse de la notion de formule. Cette étude formelle du langage mathématique fait abstraction du *sens* des *phrases* ainsi créées. Elle est à rapprocher de la démarche utilisée en théorie des modèles (*Les Mille et un théorèmes* page 99).

Le XXe siècle n'a pas connu uniquement des découvertes en logique classique. Par exemple, le développement d'autres sciences comme la physique et l'informatique a conduit à l'émergence d'une nouvelle forme de logique : la logique quantique, aujourd'hui à la base de l'informatique quantique, qui est un domaine de recherche très actif (*Une porte doit être ouverte et fermée* page 111).

FIG. 1.6 – La logique ou l'art de penser

Chapitre 2

Le paradoxe aux cent têtes

« Le chemin des paradoxes est le chemin du vrai.
Pour éprouver la Réalité, il faut la voir sur la corde raide.
C'est lorsque les Vérités deviennent des funambules que l'on peut les juger. »
Oscar Wilde, Le portrait de Dorian Gray

FIG. 2.1 – *poésie de Francis Ponge*

2.1 Les paradoxes de l'auto-référence

L'auto-référence est la propriété, pour un système, de faire référence à lui-même. Elle est rendue possible lorsqu'il existe deux niveaux logiques, un niveau et un méta-niveau. Nous allons ici présenter de nombreux paradoxes liés à l'auto-référence. Tous ces paradoxes renvoient à la théorie des ensembles ; le lecteur est invité à imaginer les ensembles adéquats dans chacun des exemples proposés.
La plus ancienne trace de ce paradoxe est relatée dans la Bible :

« Quelqu'un d'entre eux, leur propre prophète, a dit : Les Crétois sont toujours menteurs, de méchantes bêtes, des ventres paresseux. »
l'épître à Tite, Paul de Tarse.

Ce prophète, qui vécut au VIIe siècle av. J.-C., serait Épiménide le **Crétois**.

On rencontre l'auto-référence dans de nombreux domaines comme la littérature, la philosophie, l'informatique, la linguistique ou les mathématiques. Nous allons faire une courte présentation de ces différents paradoxes avant de montrer comment on peut les éviter dans le cadre de la théorie des ensembles (cf **??** page **??**).

2.1.1 Les paradoxes du menteur et du barbier

« *Je mens.* » ou « *Cette phrase est fausse.* » sont les versions les plus simples.

Cependant on regrette souvent leur formulation imprécise : que désigne « Cette » ? Que signifie « mentir » ?
Voici un exemple un peu plus compliqué qui renvoie directement à la théorie des ensembles :
« *Dans le petit village de Thiercelieux, il y a un barbier. Ce barbier rase tous les villageois qui ne se rasent pas eux-mêmes et il ne rase que ceux là. Le barbier se rase-t-il ?* »

2.1.2 Le paradoxe de Grelling-Nelson (linguistique)

Le paradoxe de Grelling-Nelson est un paradoxe sémantique formulé en 1908 par Kurt Grelling et Leonard Nelson.

On qualifie d'*hétérologique* un mot qui décrit son contraire. Par exemple : « long » est un mot hétérologique en ceci qu'il n'est pas « long » ; de même pour « monosyllabique ». Au contraire, « court », « lisible »ou « existe » sont *autologiques*.

« hétérolgique » est-il hétérologique ?

Cet exemple nous permet la remarque suivante. Je me donne une propriété et je cherche à classer les objets en deux tas, ceux qui vérifient la propriété et ceux qui vérifient sa négation.
Alors il se crée automatiquement quatre classes (certaines peuvent être vides) :
- La classe des éléments qui vérifient la proporiété (« court » est autologique)
- La classe des éléments qui vérifient la négation de la proporiété (« long » est hétérologique)
- La classe des éléments pour lesquels on ne peut répondre pour des raisons syntaxiques (« aspirateur » est un mot qui ne peut décrire un mot)
- La classe des éléments pour lesquels on ne peut répondre pour des raisons sémantiques (« hétérologique »)

2.1.3 Le paradoxe de Richard

Le paradoxe de Richard est une version plus formelle du paradoxe de l'auto-référence publié en 1905 par le mathématicien français Jules Richard. En fait ce paradoxe est une supercherie assez subtile mais qui a son intérêt car elle émet l'idée de « projeter » un langage dans **N** (c'est à dire de numéroter les phrases) ; cette idée est

un point crucial de la démonstration du théorème de Gödel (*Le chapitre 4 n'est pas démontrable* page 79).

Voici une esquisse du paradoxe de Richard.

1. On suppose qu'on dispose d'un langage (comme le français) dans lequel on puisse formuler et définir des concepts arithmétiques des entiers naturels (par exemple être un nombre premier, être un carré parfait...).
2. Il existe différentes propriétés arithmétiques qui peuvent s'exprimer dans ce langage (à partir de concepts primitifs dont on admettra qu'ils sont compris : l'addition, la multiplication, la divisibilité...).
   exemples:
   – être premier ≡ « *qui n'est divisible que par lui-même et par un* ».
   – être pair ≡ « *qui est divisible par 2* ».
3. Il est clair que chacune de ces propriétés sera exprimée à l'aide d'un nombre fini de lettres. On peut donc les classer par taille puis au sein des propriétés de même taille par ordre alphabétique. Ce classement nous permet alors de numéroter ces propriétés.
4. Imaginons que la propriété 17 soit « *qui n'est divisible que par lui-même et par un* » ; on remarque que 17 vérifie la propriété dont il est le numéro.
   Au contraire, si 15 est le numéro de « *qui est le produit de* 3 *et* 3 » alors 15 ne vérifie pas la propriété 15.
   On dira que 15 est *richardien* et que 17 n'est pas *richardien*.
5. « qui est richardien » est une propriété sur les nombres entiers. Elle possède donc un numéro n_0 d'après le classement décrit en 3.
6. n_0 est-il richardien ?

En fait, comme nous l'avons dit, cet énoncé contient une erreur. Pour la détecter soyons un peu formalistes.
Soit E l'ensemble des phrases ; A le sous-ensemble des phrases décrivant une propriété arithmétique à l'aide de concepts connus et B son complémentaire : par exemple « *qui est divisible par deux* » est dans $\mathcal{A}$ mais « *qui est richardien* »est dans B car on ne sait pas encore ce que signifie richardien ; comme E est dénombrable on peut considérer que A et B sont des sous-ensembles de $\mathbf{N}$; ainsi n_0 est dans B.
On définit alors sur $E \times A$ la relation suivante : $n\ Ver\ m$ ssi n « vérifie »la propriété m ; il est clair que cette relation ne peut être définie sur un ensemble plus grand.
On a alors deux possibilités pour définir la propriété d'« être richardien » :

- $n \in A$ est richardien ssi $\overline{n\ Ver\ n}$ mais alors n_0 (cf 5) n'appartient pas au domaine de définition de « *qui est richardien* »donc la question 6 n'a aucun sens.
- $n \in A$ est anti-richardien ssi $n\ Ver\ n$; $n \in E$ est richardien ssi $n \in A$ et $n \in A \Rightarrow$ (n n'est pas anti-richardien). Ainsi la réponse à la question 6 est trivialement non.

2.1.4 Paradoxe de Russell

Formulés par Russell en 1905, ce paradoxe est une dernière version du paradoxe l'auto-référence appliquée cette fois à la théories des ensembles : il y a deux types d'ensembles : les ensembles pervers qui ne sont pas éléments d'eux mêmes et les ensembles gentils dont l'un des éléments est l'ensemble lui-même. L'ensemble des ensembles pervers est-il pervers ? La résolution de ce paradoxe a eu une place centrale dans la construction de la théorie des ensembles et son processus d'axiomatisation. La partie suivante développe ce point.

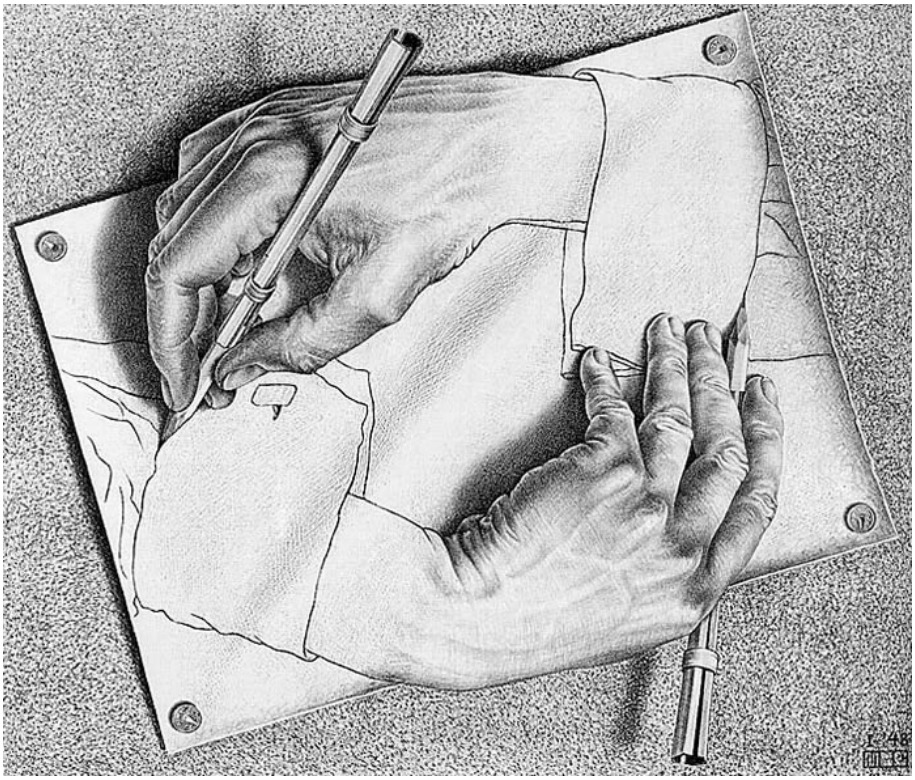


FIG. 2.2 – *Drawing Hands* (Escher - 1948)

2.2 La théorie des ensembles et le processus d'axiomatisation

Dans la section précédente nous avons donné un bref aperçu du développement historique de la logique mathématique. Nous avons aussi mentionné le paradoxe de Russell et son impact sur le développement de l'axiomatique de la théorie des ensembles. Le but de ce chapitre sera alors d'expliquer plus formellement comment a été élaboré le système de Zermelo-Fraenkel qui est aujourd'hui à la base de la théorie des ensembles. Nous nous attacherons à montrer *où* et *comment* le paradoxe de Russell intervient et la manière dont on a pu y échapper. Nous essayerons de nous poser des questions d'ordre général qui interviennent naturellement quand on construit une théorie.

C'est pourquoi avant de donner les axiomes ZFC nous nous intéresserons aux propriétés des objets qu'ils décrivent, c'est-à-dire les ensembles. Nous procéderons en trois temps :

1. *Pourquoi une théorie des ensembles*
2. *Le cas particulier des ensembles finis*
3. *La construction des axiomes*

2.2.1 Pourquoi une théorie des ensembles ?

Avant de se demander ce qu'est exactement *un ensemble* on peut se poser la question : *Pourquoi créer une théorie des ensembles ?* Certes, les ensembles interviennent souvent dans les mathématiques mais ce n'est pas une raison suffisante ; en effet, les suites sont des objets d'usage courant mais il n'existe pas de théorie générale des suites. Ce qui a motivé la création d'une théorie des ensembles est l'apparition à la fin du XIXème et au début du XXème siècle de problèmes ouverts difficiles mettant en jeu des ensembles.

Nous allons présenter ici très brièvement un de ces problèmes, *l'hypothèse du continu*, qui ont donné lieu à la création de la théorie des ensembles. Aussi nous présenterons des énoncés concernant les ensembles dans un ordre qui représente une chaîne « naturelle » de questions pour aboutir à *l'hypothèse du continu*[1].

Commençons donc par la question :
Comment peut-on *comparer* la « taille » des ensembles ?

Définition *équipotence*

On dit que deux ensembles A et B sont en bijection (sont équipotents), s'il existe une bijection de A sur B.

[1] Tous ces énoncés sont très connus. C'est pourquoi on se permettra de ne pas donner les démonstrations (qui ne sont pas vraiment difficiles) cf [6]

Une propriété étant définie, on veut disposer d'un critère pour tester si cette propriété est vérifiée. La proposition suivante en donne un ; c'est aussi un bon outil pour les démonstrations des quelques propositions et lemmes qui suivent.

Proposition *théorème de Cantor-Bernstein*

Si A et B sont deux ensembles tels qu'il existe une injection de A dans B et une injection de B dans A alors A et B sont en bijection.

Un premier niveau de comparaison de la taille des ensembles est la distinction fini/infini et la notion de cardinal :

Définition *fini/ infini*

Un ensemble E est dit fini *s'il existe $n \in \boldsymbol{N}$ tel qu'il existe une bijection*

$$\Phi : E \to \{1, \ldots, n\}$$

Un ensemble qui n'est pas fini est dit infini.

Proposition *critère de bijection*

Toute injection d'un ensemble fini dans lui-même est une bijection.

Corollaire

Tout ensemble fini est en bijection avec un unique intervalle $\{1, \ldots, n\} \subset \boldsymbol{N}$.

Pour le cas des ensembles finis nous sommes maintenant capables de définir sans ambigüité (par l'unicité du corollaire précédent) le cardinal de l'ensemble.

Définition *cardinal dans le cas fini*

Soit E un ensemble fini alors le cardinal *de E est défini comme l'unique $n \in \boldsymbol{N}$ tel que E soit en bijection avec l'intervalle $\{1, \ldots, n\}$.*

Deux ensembles finis sont alors en bijection ssi ils ont le même cardinal. On peut donc *comparer* les ensembles finis à partir de leur cardinal.
Le « niveau suivant » concerne les ensembles en bijection avec $\mathbf{N}$.

Définition *dénombrable*

Un ensemble E est dit dénombrable s'il existe une bijection entre E et $\boldsymbol{N}$.

Nous savons alors *dénombrer*. Donnons tout de suite quelques exemples d'ensembles dénombrables.

Proposition

Le produit $\boldsymbol{N} \times \boldsymbol{N}$ est dénombrable

Corollaire

$\boldsymbol{Z}$ et $\boldsymbol{Q}$ sont dénombrables.

La démonstration de la proposition suivante en 1874 par Georg Cantor marque le début de la théorie des ensembles :

Proposition

$\boldsymbol{R}$ n'est pas dénombrable.

En fait $\mathbf{R}$ est équipotent à $\wp(\mathbf{N})$ et la propriété précédente est alors conséquence du résultat plus général suivant, dû lui aussi à Cantor :

Proposition *Pour tout ensemble A, il n'existe pas de surjection de A sur $\wp(A)$.*

On exhibe de cette manière une suite de « tailles d'infinis » : à savoir $\mathbf{N}$, $\wp(N)$, $\wp(\wp(\mathbf{N}))$...

La taille de $\mathbf{R}$ est supérieure à la taille de $\mathbf{N}$ car $\mathbf{N} \subset \mathbf{R}$ et $\mathbf{R}$ n'est pas dénombrable. Mais parmi les sous-ensembles infinis de $\mathbf{R}$, on a par exemple $\mathbf{Z}$, $\mathbf{Q}$ et $\mathbf{N}$ qui sont dénombrables et $\mathbf{R}$ qui ne l'est pas. Se pose alors naturellement la question suivante

problème du continu :

Est-ce que tout sous-ensemble infini de $\boldsymbol{R}$ est en bijection soit avec $\boldsymbol{R}$ soit avec $\boldsymbol{N}$?

Autrement dit : Existe-t-il des tailles intermédiaires entre celle de $\mathbf{N}$ et celle de $\mathbf{R}$, la dernière étant appelée *le continu* ?

C'est à la fin du XIXe siècle que Cantor posa cette question. Ce problème a été un des moteurs les plus forts du développement de la théorie des ensembles au cours du XXe siècle ; la réponse est assez particulière ... [2]

[2]En 1940 Kurt Gödel démontra que l'hypothèse du continu (la non-existence d'ensembles de cardinal strictement compris entre le cardinal de $\mathbf{N}$ et celui de $\mathbf{R}$) ne peut pas être refutée à partir des axiomes ZFC. Dans les années 1960 Paul Cohen démontra (ce qui lui apportera la médaille

La création d'une théorie des ensembles est alors justifiée : l'objectif est de résoudre des problèmes ouverts.

Comment allons nous procéder ? Il va falloir organiser nos connaissances sur les objets mathématiques que sont les ensembles et donc nous poser les deux questions suivantes :

Qu'est-ce qu'est un ensemble ?

Quelles sont les propriétés d'un ensemble ?

* l'utilité des ensembles est de pouvoir réunir des objets. Il est donc important qu'un ensemble soit complètement déterminé par ses éléments et par eux seuls
* il est également intéressant de définir l'ensemble des éléments vérifiant une certaine propriété. Mais attention, à un même ensemble peuvent correspondre plusieurs propriétés. Par exemple l'ensemble des nombres pairs est l'ensemble des nombres divisibles par deux mais aussi l'ensemble des nombre dont l'écriture décimale se termine par $0, 2, 4, 6$ ou 8

2.2.2 Opérations ensemblistes et le cas fini

Nous allons étudier un cas particulier, le cas des ensembles finis. Il y a deux raisons à cela : tout d'abord parce que toute théorie générale sur les ensembles devra contenir ce cas particulier ; ensuite parce que la théorie des ensembles finis et les propriétés des opérations ensemblistes sur les ensembles finis sont complètement décrites par la notion d'algèbre de Boole. Pour les démonstrations de cette section, on renvoie à [6].

Rappelons la définition des opérations ensemblistes :

Définition *inclusion, parties*

Pour des ensembles A et B on dit que A est inclus *dans B ou encore que A est une* partie *de B (ce qu'on va noter comme $A \subseteq B$) si tout élément de A est élément de B. On note $\mathcal{P}(A)$ l'ensemble des parties de A.*

Définition *opérations ensemblistes*

Pour deux ensembles A et B on définit dans cet ordre : l'union, l'intersection, la différence et la différence symétrique de A et B comme suit :

$A \cup B = \{x | x \in A \text{ ou } x \in B\}$

$A \cap B = \{x | x \in A \text{ et } x \in B\}$

$A \setminus B = \{x \in A | x \notin B\}$

Fields) qu'on ne peut pas non plus la déduire de ces axiomes. L'hypothèse du continu constitue ainsi un exemple concret d'énoncé indécidable. **cf section correspondante dans ce rapport**.

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

.

Quelquefois on se place dans le contexte d'un « grand » ensemble Ω dont on regarde des sous-ensembles $A \subseteq \Omega$. Dans ce cas on définit aussi le complémentaire d'une partie A :

$$A^c = \Omega \setminus A$$

Le lemme suivant va permettre le lien avec les algèbres de Boole.

Lemme

La relation d'inclusion est une relation d'ordre.

Définissons maintenant ce qu'est une algèbre de Boole.

Définition *treillis, algèbre de Boole*

Soit X un ensemble muni d'une relation d'ordre $\leq$. On dit que $(X, \leq)$ est un treillis *si chaque paire d'éléments de X possède une borne supérieure et une borne inférieure.*
Un treillis est dit distributif *si l'opération sup est distributive par rapport à l'opération inf et vice versa.*
Un treillis est dit complémenté, s'il possède un minimum, noté 0*, un maximum, noté* 1*, et si*

$$\forall\ x \in X\ \exists\ x^c \in X : \sup(x, x^c) = 1 \text{ et } \inf(x, x^c) = 0$$

On dit que x^c est un complément *de x.*
Un treillis distributif et complémenté est appelé algèbre de Boole.

Dans un groupe, on a *existence* et *unicité* de l'inverse. Intéressons nous donc à la question de l'unicité du complément.

Lemme

Soit $(X, \leq)$ un treillis distributif possédant un minimum 0 *et un maximum* 1*, alors pour tout élément $a \in X$ il existe au plus un élément $b \in X$ tel que* $\inf(a, b) = 0$ *et* $\sup(a, b) = 1$.

Le lien entre algèbres de Boole et ensembles est donné par la proposition suivante

Proposition *algèbre de Boole*

Pour tout ensemble A, $(\mathcal{P}(A), \subseteq)$ est une algèbre de Boole où l'opération sup *est* $\cup$*, l'opération* inf *est* $\cap$*, le minimum est* $\emptyset$*, le maximum est l'ensemble A lui-même et le complément est le complémentaire.*

On sait maintenant que $(\mathcal{P}(A), \subseteq)$ est une algèbre de Boole. Nous allons maintenant montrer que toute algèbre de Boole finie peut être vue comme un système $(\mathcal{P}(A), \subseteq)$ pour un ensemble fini A . Ainsi en axiomatisant les algèbres de Boole nous aurons axiomatisé la théorie des ensembles finis.

Axiomatisation des algèbres de Boole

Proposition *schéma d'axiome 1*

Soit $(T, \leq)$ un treillis. On pose pour $a, b \in T$:

$a \vee b = \sup(a, b)$

$a \wedge b = \inf(a, b)$

Alors $(T, \vee, \wedge)$ vérifie les lois :

$$\begin{array}{rclll rcll} x \vee x & = & x & (I_0) & & x \wedge x & = & x & (J_0) \\ x \vee y & = & y \vee x & (I_1) & & x \wedge y & = & y \wedge x & (J_1) \\ x \vee (y \vee z) & = & (x \vee y) \vee z & (I_2) & & x \wedge (y \wedge z) & = & (x \wedge y) \wedge z & (J_2) \\ x \vee (x \wedge y) & = & x & (I_3) & & x \wedge (x \vee y) & = & x & (J_3) \end{array}$$

Et en plus, $a \leq b$ est équivalent à $a \vee b = b$ et à $a \wedge b = a$.

À l'inverse, si $(T, \vee, \wedge)$ vérifie les lois $(I_1), (I_2), (I_3)$ et $(J_1), (J_2), (J_3)$ et si on note pour $a, b \in T$: $a \leq b$ pour $a \vee b = b$, alors $(T, \leq)$ est un treillis et $\vee$ est l'opération sup *et $\wedge$ est l'opération* inf.

Proposition *schéma d'axiome 2*

Soit $(B, \leq)$ une algèbre de Boole de minimum 0 et de maximum 1. Posons pour $a, b \in B$: $a \vee b = \sup(a, b)$ et $a \wedge b = \inf(a, b)$. Notons de plus $\bar{a}$ l'unique élément vérifiant $a \vee \bar{a} = 1$ et $a \wedge \bar{a} = 0$.
Alors $(B, \vee, \wedge, 0, 1, ^-)$ vérifie les lois $(I_0), \ldots, (J_3)$ de l'axiomatisation 1, et, de plus :

$$\begin{array}{rclll rcll} x \vee (y \wedge z) & = & (x \vee y) \wedge (x \vee z) & (I_4) & & x \wedge (y \vee z) & = & (x \wedge y) \vee (x \wedge z) & (J_4) \\ x \vee 0 = x & \text{et} & x \vee 1 = 1 & (I_5) & & x \wedge 0 = 0 & \text{et} & x \wedge 1 = 1 & (J_5) \\ x \vee \bar{x} & = & 1 & (I_6) & & x \wedge \bar{x} & = & 0 & (J_2) \end{array}$$

Inversement, supposons que $(B, \vee, \wedge, 0, 1, ^-)$ satisfait aux lois $(I_1), \ldots, (J_6)$ et notons $a \leq b$ pour $a \vee b = b$. Alors $(B, \leq)$ est une algèbre de Boole avec les opérations sup (resp inf) qui sont $\vee$ (resp. $\wedge$) et le maximum est 1 et le minimum est 0.

Ceci montre alors que l'on peut appeler algèbre de Boole une structure algébrique $(B, \vee, \wedge, 0, 1, ^-)$ qui vérifie les lois pour inf et sup du schéma d'axiome 2.

Donnons-nous une troisième caractérisation, toujours basée sur des lois algébriques.

Définition *anneau de Boole*

Un anneau commutatif et idempotent (i.e. $x^2 = x$ pour tout x) est appelé anneau de

Boole.

Proposition *équivalence*

(i) Soit $(B, \vee, \wedge, 0, 1, ^-)$ *une algèbre de Boole. Définissons* Δ *par* $a\Delta b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$. *Alors* $(B, \Delta, \wedge)$ *est un anneau de Boole.*

(ii) Supposons inversement que $(B, +, \cdot)$ *est un anneau de Boole. Alors* $(B, \vee, \wedge, 0, 1, ^-)$ *est une algèbre de Boole où on a défini* $\vee, \wedge$ *et* $^-$ *par* $a \vee b = a + b + ab$, $a \wedge b = ab$ *et* $\bar{a} = 1 + a$.

.

Finalement, nous pouvons démontrer que toute algèbre de Boole finie a une structure de $(\mathcal{P}(A), \subseteq)$ pour un ensemble A.

Proposition *algèbres de Boole finies*

Toute algèbre de Boole finie est isomorphe à une algèbre du type $(\mathcal{P}(A), \subseteq)$

Cette proposition montre bien que la notion d'algèbre de Boole capture toutes les propriétés des ensembles $\mathcal{P}(A)$ finis et donc que les axiomes du schéma d'axiome 2 caractérisent complètement les opérations ensemblistes pour les ensembles finis.

2.2.3 L'axiomatisation

Dans la section précédente on a vu que l'on maîtrisait bien le cas des ensembles finis. Mais comme la première section de ce chapitre l'a montré, les grands problèmes ouverts concernent les ensembles de taille infinie. Comment *spécifier* ce que sont les ensembles ? On utilise ici le mot *spécifier*, car comme on va le montrer dans la toute première partie de cette section, *définir* les ensembles pose des problèmes et donc, la seule possibilité qui reste est le recours à une *axiomatisation*.

Ainsi, dans cette section, nous allons d'abord illustrer quelles sont les difficultés à *définir* les ensembles pour ensuite aborder la question centrale de ce chapitre : Comment axiomatiser la théorie des ensembles ? Nous suivrons une démarche chronologique.

Pour aborder la question de la définition des ensembles, on va utiliser un formalisme proche de celui des langages de programmation par objets.

Supposons donné, pour chaque couple de types $(\tau, \tilde{\tau})$ le type $\tau \to \tilde{\tau}$, ie le type des fonctions allant des objets de τ vers les objets de $\tilde{\tau}$. Alors on peut se donner un type, appelé dans la suite **Bool**, ne comportant que deux objets, appelés VRAI et FAUX. On introduit la notation $x : \tau$ pour dire que x est un objet du type τ.

« Définition » *ensemble*
Pour tout type τ, le type $\tau \to \boldsymbol{Bool}$ est noté $\boldsymbol{Ens}_\tau$ et les objets de type $\boldsymbol{Ens}_\tau$ sont appelés ensembles *d'objets de type τ. Pour x de type τ et A de type $\boldsymbol{Ens}_\tau$ on dit que x est élément de A, ce qu'on notera $x \in_\tau A$ si on a $A(x) = VRAI$.*

Une fois définis les ensembles, regardons s'ils ont, selon cette définition, vraiment les propriétés que l'on *souhaite*.

Proposition *propriétés*
(i) Un objet de type $\boldsymbol{Ens}_\tau$ est déterminé par ses éléments.
(ii) Pour tous $a_1, \ldots, a_n$ de type τ il existe un objet de type $\boldsymbol{Ens}_\tau$ ayant $a_1, \ldots, a_n$ pour éléments.
(iii) Pour chaque propriété $\mathcal{P}(x : \tau)$ des objets de type τ il existe un objet de type $\boldsymbol{Ens}_\tau$ dont les éléments sont exactement les éléments de type τ satisfaisant $\mathcal{P}$.

Si on regarde une démonstration pour la proposition précédente comme par exemple celle donné dans [6], on constate que la démonstration, dans l'essentiel, n'est rien d'autre qu'une *vérification de la cohérence du vocabulaire introduit avant*. Quel est le problème ici ? Le problème ici est tout simplement qu'on n'a pas vraiment donné un point de départ pour la théorie des ensembles parce qu'on a défini les ensembles en supposant que les fonctions sont déjà présentes donc en particulier définies. Mais donc, la question du fondement de la théorie des ensembles est juste reportée à la définition des fonctions et celle-ci, classiquement, est faite à partir des ensembles, en définissant une fonction comme une partie d'un produit cartésien d'ensembles.

Le phénomène rencontré ici est en fait assez général : on rencontre la même difficulté en arithmétique ou en géométrie quand il s'agit de définir des concepts premiers. Mais si la question de la définition des objets est réellement importante pour le philosophe, elle n'est que très secondaire pour le mathématicien : le mathématicien n'a en fait de relation avec les objets qu'il manipule que par leurs propriétés. D'où l'idée d'adopter une approche axiomatique des ensembles, qui loin de les définir, se contentera de donner leurs propriétés.

Conclusion
La tentative de définir les ensembles n'a pas de réussite, il faut donc se contenter d'une approche axiomatique.

Le mot AXIOME provient du grec :*dire ce qui est considéré comme digne ou convenable.*
Il s'agit donc de choisir un système d'axiomes qui restitue les propriétés « naturelles » des ensembles. On veut par ailleurs trouver un nombre minimal d'axiomes dont dépend la théorie.

Ainsi, il faut se demander de nouveau quelles sont les propriétés des ensembles . Il y a deux propriétés fondamentales :

La première est dans un certain sens un principe d'unicité, qui dit qu'un ensemble est complètement déterminé par ses éléments (voir la première section)

La seconde serait un principe d'existence qui dit qu'on peut spécifier un ensemble soit en donnant explicitement une liste de ses éléments, soit en donnant une propriété satisfaite exactement par les éléments de l'ensemble.

Ces deux propriétés amènent naturellement aux trois axiomes suivants :

Définition *extensionalité, extension, compréhension*

On appelle axiome d'extensionnalité *(EX 1)pour les objets de type τ l'assertion*

$$\forall\ A, \tilde{A} : \boldsymbol{Ens}_\tau(A = \tilde{A} \Leftrightarrow \forall\ x : \tau(x \in A \Leftrightarrow x \in \tilde{A}))$$

Pour $a_1, \ldots, a_n$ de type τ on appelle axiome d'extension *(EX 2) pour $a_1, \ldots, a_n$ l'assertion*

$$\exists A : \boldsymbol{Ens}_\tau \forall x : \tau(x \in A \Leftrightarrow (x = a_1 \text{ ou } \ldots \text{ ou } x = a_n))$$

Pour $\mathcal{P}(x)$ propritété faisant sens pour les objets de type τ on appelle axiome de compréhension *(COMP) en $\mathcal{P}$ l'assertion*

$$\exists A : \boldsymbol{Ens}_\tau \forall x : \tau(x \in A \Leftrightarrow \mathcal{P}(x) \text{ est vraie })$$

On note que l'on pourrait faire l'économie de (EX 2) car une définition d'un ensemble par extension est un cas particulier d'une définition par compréhension : l'ensemble défini par extension comme $\{a_1, \ldots, a_n\}$ est le même que l'ensemble défini par compréhension comme $\{x : \tau | \mathcal{P}(x)\}$ où $\mathcal{P}(x) = (x = a_1) \vee (x = a_2) \vee \cdots \vee (x = a_n)$.

C'est à peu près ainsi que CANTOR avait formulé la théorie des ensembles vers 1890. Malheureusement on devait constater que cette axiomatique n'est pas libre de contradictions comme le montre le paradoxe de Berry :

2.2.3.1 Le paradoxe de Berry

Proposition *paradoxe de Berry*

Soit $\mathcal{P}(n)$ la propriété « n est un entier définissable par une phrase allemande d'au plus 140 caractères ». Alors il ne peut exister d'ensembles des entiers possédant la propriété $\mathcal{P}$

Démonstration :

Disons d'abord, que l'on a choisi la langue allemande et pas la langue française car la dernière, avec les accents, apostrophes etc est un peu plus compliquée à maîtriser en termes de signes nécessaires pour pouvoir formuler une phrase. L'allemand peut

se contenter des 26 lettres de l'alphabet, sans accents, sans apostrophes etc. En prenant en compte les blancs, il y a au plus 27^{140} *phrases allemandes de moins de 140 caractères.*

Chaque telle phrase ne peut correspondre qu'à un seul entier. Il y a donc par conséquence au plus 27^{140} *tels entiers et si on appelle* E *l'ensemble de ces entiers qui peuvent être définis avec une phrase allemande d'au plus 140 caractères, alors* E *qui est de taille finie a forcement un complémentaire* $E^c = \boldsymbol{N} \setminus E \subset \boldsymbol{N}$.

Maintenant on sait que tout sous-ensemble non vide des entiers contient un plus petit élément, et donc il existe $n_0 := \inf(\mathbb{E}^c)$. *Traduisons maintenant la phrase « je suis le plus petit entier non définissable par une phrase allemande d'au plus cent quarente caractères » en allemand et on trouvera : « ich bin die kleinste natuerliche Zahl die man nicht mit einem deutschen Satz von weniger als hundertvierzig Buchstaben definieren kann » et cette phrase a 135 caractères (les blancs inclus). Ce résultat est donc en contradiction avec l'existence d'un ensemble* $E = \{n : \boldsymbol{Ent} | \mathcal{P}(n)\}$ *où* ***Ent*** *désigne le type des entiers.*

Le système de CANTOR qui consiste en les axiomes (EX 1), (EX 2) et (COMP) n'est donc pas libre de contradictions. Il faut le changer mais comment ? Pour pouvoir répondre à cette question il faut se demander ce qui fait, dans le système de Cantor que le paradoxe de Berry existe. Apparemment c'est la possibilité de définir un ensemble par compréhension, mais on ne peut abandonner complètement cet axiome car l'introduction d'ensembles définis par compréhension est fréquente en mathématiques.
Ce qui « crée » le paradoxe est le fait qu'on définit la propriété $\mathcal{P}(n)$ à l'aide d'une phrase informelle : en particulier le terme « définissable » « change » presque de sens au cours de la démonstration. Il faut donc restreindre la compréhension aux propriétés exprimées dans un langage suffisamment rigide, c'est-à-dire aux propriétés exprimées à l'aide de *formules*.

La prochaine étape est alors d'étudier le langage des mathématiques et de le *formaliser*, c'est-à-dire de définir ses *signes* et sa « grammaire », c'est-à-dire les règles qui définissent les *formules*.

La construction d'une logique formelle ne pouvait être réalisée dans le cadre du PSC. On se contentera donc d'une discussion très informelle. Le lecteur en trouvera une explication plus détaillée par exemple dans [6].

L'idée générale de cette formalisation du langage est :

fixer une *signature* $\sum$ qui consiste en

- une liste de types
- une liste d'opérations et de relations qui relient des objets de ces types

définir inductivement les formules en la signature $\sum$ comme des suites finies de symboles qui sont

- soit des variables avec indication de type
- soit des opérations et relations de $\sum$

- soit le signe $=$
- soit des connecteurs logiques comme $\Rightarrow$, $\Leftarrow$, non, $\wedge$, $\vee$
- soit des quantificateurs $\forall$ ou $\exists$
- soit des parenthèses

Par exemple la formule $(\forall n : Ent)(\exists p, q : Ent)(n = p * p + q * q)$ est une formule en la signature $\sum_1$ comportant le type Ent et les relations binaires $+$ et $*$.

On appelle *formule du premier ordre* une formule dont les seules variables portent sur les éléments des types déclarés dans $\sum$, à l'exclusion des ensembles de tels éléments. Les formules du second ordre seront les formules dont les variables peuvent porter sur les éléments des types et sur les ensembles de tels éléments, et ainsi de suite.
Par exemple la formule précédente est du premier ordre en la signature $\sum_1$ alors que la formule suivante :

$$\forall A : Ens_{Ent}(((0 \in A) \wedge (\forall n : Ent(n \in A \Rightarrow n + 1 \in A))) \Rightarrow (\forall n : Ent)(n \in A))$$

est du deuxième ordre.

Définition *compréhension, version réduite*

Pour $\mathcal{F}(x, x_1, \ldots, x_n)$ formule du premier ordre en une signature comportant l'unique type τ, on appelle axiome de compréhension *en $\mathcal{F}$ l'assertion*

$$\forall a_1, \ldots, a_n : \tau \exists A : \boldsymbol{Ens}_\tau \forall x : \tau(x \in A \Leftrightarrow \mathcal{F}(x, a_1, \ldots, a_n))$$

On est alors dans la situation décrite plus haut : cette version de la compréhension réduite garde la possibilité de définir par compréhension pour des propriétés exprimables par une formule du premier ordre. Ainsi on échappe au paradoxe de Berry car « être définissable par une phrase allemande d'au plus 140 caractères » n'est pas exprimable par une telle formule.

Le système ainsi obtenu en remplaçant la compréhension par la compréhension réduite est souvent appelé système de FREGE, en faisant référence au logicien FREGE qui avait proposé un tel système vers 1893.

Pour n'importe quelle signature, les formules $x = x$ et $x \neq x$ sont toujours des formules de premier ordre en cette signature. On introduit alors deux ensembles :

Définition *plein, vide*

Soit τ un type quelconque. L'ensemble plein (resp. vide) *de type τ est l'ensemble*

$\{x : \tau | x = x\}$ *(resp.* $\{x : \tau | x \neq x\}$*). On le note* Ω_τ *(resp.* $\emptyset_\tau$*).*

2.2.3.2 Le paradoxe de Russell

Mais il semble alors légitime d'introduire un type général ensemble, regroupant tous les types Ens_τ. Mais si l'axiome de compréhension est valide dans le type *Ens* pour les formules contenant $\in$, alors on arrive au *paradoxe de Russell.*

Proposition *paradoxe de Russell*

L'existence d'un ensemble de tous les ensembles non éléments d'eux-mêmes est une hypothèse contradictoire.

Démonstration
Supposons qu'on puisse définir par compréhension l'ensemble

$$A := \{X : \boldsymbol{Ens} | X \notin X\}$$

A serait donc un ensemble tel que

$$\forall X : \boldsymbol{Ens} \text{ on a } X \in A \Leftrightarrow X \notin X$$

Mais cela veut dire que $X \in A$ *est soit VRAI soit FAUX pour chaque ensemble* X*. Alors, comme A est aussi un ensemble*

soit $A \in A$ *mais alors par la propriété qui définit A par compréhension on a* $A \notin A$

soit $A \notin A$ *alors à cause de la même propriété définissant A on a* $A \in A$

Ces deux possibilités étant toutes les deux contradictoires un tel ensemble A ne peut pas exister.

De nouveau on se retrouve face à un paradoxe.
Il se présente, dans un premier temps deux possibilités :

(i) on interdit la création d'un type **Ens** de tous les ensembles et on construit des « tours » sur chaque type τ du genre τ -> $\mathbf{Ens}_\tau$ -> $\mathbf{Ens}_{\mathbf{Ens}_\tau}$ -> $\mathbf{Ens}_{\mathbf{Ens}_{\mathbf{Ens}_\tau}}$ $\cdots$ où la relation d'appartenance n'est définie que entre un type μ et l'instance un en-dessus $\mathbf{Ens}_\mu$. Donc par exemple entre $\mathbf{Ens}_{\mathbf{Ens}_\tau}$ et $\mathbf{Ens}_{\mathbf{Ens}_{\mathbf{Ens}_\tau}}$.
Par conséquent, des formules comme $X \in X$ pour X dans n'importe quel type n'ont plus de sens, car $\in$ n'est pas déclaré pour deux objets du même type. Un tel système n'a par contre pas apporté de grands succès et il présente l'inconvénient d'être très compliqué.

(ii) on restreint de nouveau les possibilités de *définir par compréhension* pour échapper au paradoxe de Russell.
Celle-ci est la démarche choisie par la théorie des ensembles classique et c'est aussi celle-ci qu'on va présenter.

De nouveau, si on veut échapper au paradoxe de Russell, comme dans le cas du paradoxe de Berry, on doit se demander : Quel est exactement le point délicat dans

l'axiome de compréhension qui fait que ce paradoxe existe ? Une explication possible est que d'une certaine manière « l'ensemble des ensembles » est *trop grand* pour être un ensemble - il reste à précicer ce que *trop grand* veut dire.

L'idée est alors, de ne donner le droit de définir par compréhension que si cette définition, d'une certaine manière, représente une « sélection dans un ensemble », une « séparation ». Autrement dit : l'ancien énoncé était l'axiome de compréhension

(i) pour chaque formule $\mathcal{F}(x, x_1, \ldots, x_n)$ dans un type

(ii) et pour chaque choix de $a_1, \ldots, a_n$ de l'ensemble $\{x|\mathcal{F}(x, a_1, \ldots, a_n)\}$

A l'opposé, la *séparation* se fait à l'intérieur d'un ensemble E, c'est-à-dire que l'on demande explicitement pour la définition par compréhension que les objets x qu'on va séparer soient déjà des éléments d'un ensemble E, ce qui veut dire qu'on ne donne la possibilité de définir par compréhension que pour des formules de la forme

$$x \in E \text{ et } \mathcal{F}(x, x_1, \ldots, x_n)$$

Définition *séparation*

Pour $\mathcal{F}(x, x_1, \ldots, x_n)$ formule du premier ordre en une signature comportant l'unique type τ, on appelle axiome de séparation *en $\mathcal{F}$ l'assertion*

$$\forall a_1, \ldots, a_n : \tau \forall A : \boldsymbol{Ens}_\tau \exists B : \boldsymbol{Ens}_\tau \forall x : \tau (x \in B \Leftrightarrow (x \in A \text{ et } \mathcal{F}(x, a_1, \ldots, a_))))$$

On note $\{x \in A|\mathcal{F}(x, a_1, \ldots, a_n)\}$ l'ensemble B dont l'existence est affirmée par l'Axiome de séparation.

Remarque :

Si tous les objets d'un type τ forment un ensemble Ω_τ, alors tout ensemble $\{x : \tau|F(x)\}$ (défini par compréhension) coincide avec l'ensemble $\{x \in \Omega_\tau|F(x)\}$(défini par séparation).

Dans le cas où il n'existe pas d'ensemble formé par tous les objets d'un type τ, alors définir par séparation représente une restriction qui, comme on vera tout de suite a des conséquences fondamentales :

Proposition *ensemble de tous les ensembles*

Les objets de type « ensemble » ne forment pas un ensemble.

Démonstration :

L'existence d'un ensemble des ensembles voudrait dire que la définition par séparation amène au même ensemble que la définition par compréhension selon la remarque précédente. Mais la définition par compréhension associée à la formule $a \notin a$ définirait un ensemble de tous les ensembles qui ne se contiennent pas eux-mêmes ce qui est en contradiction avec le paradoxe de Russell.

Avec l'axiome d'extensionnalité et la famille infinie de tous les axiomes de séparation en chacune des formules du premier ordre on a pu échapper aux paradoxes de

Russell et Berry.

Mais, il se pose un nouveau problème : le pas qu'on a fait de l'axiome de compréhension vers l'axiome de séparation nous a amené dans une situation où par exemple l'existence des ensembles définis par extension n'est pas garantie ce qui est fortement contre-intuitif si on regarde les besoins usuels des mathématiciens. En toute généralité cela veut dire qu'on est forcé de réintroduire des opérations ensemblistes de base qui ne sont plus garanties par la séparation seule. L'ajout des deux axiomes suivantes qui garantissent l'existence de paires et donnent la possibilité de réunir des ensembles résout ce problème.

Définition *paire, union*

On appelle axiomes de la paire *et* de l'union *pour le type τ les assertions*

$$\forall a, b : \tau \exists A : \boldsymbol{Ens}_\tau(a \in A \text{ et } b \in A)$$

$$\forall A : \boldsymbol{Ens}_{\boldsymbol{Ens}_\tau} \exists B : \boldsymbol{Ens}_\tau \forall x : \tau(\exists X : \boldsymbol{Ens}_\tau(x \in X \text{ et } X \in A) \Rightarrow x \in B)$$

Le lemme suivant nous dit alors que les problèmes mentionnés plus haut sont maintenant réglés.

Lemme

L'axiome d'extension pour le type τ est conséquence des axiomes d'extensionnalité, de la paire, de l'union et de séparation pour le type τ et de l'axiome de la paire pour le type $\boldsymbol{Ens}_\tau$.

Par contre, autre défaut encore, l'existence de l'ensemble des parties d'un ensemble n'est pas garantie, donc on rajoute l'axiome suivant.

Définition *parties*

On appelle axiome des parties *pour le type τ l'assertion* $\forall A : \boldsymbol{Ens}_\tau \exists B : \boldsymbol{Ens}_{\boldsymbol{Ens}_\tau} \forall X : \boldsymbol{Ens}_\tau(X \subseteq A \Rightarrow X \in B)$

Une fois les axiomes d'extensionnalité et de séparation présents, l'axiome des parties nous garantit l'existence de l'ensemble des parties d'un ensemble E. En plus, on n'a pas seulement l'existence mais aussi l'unicité de cet ensemble des parties de E.

Conclusion

- Au début, CANTOR avait proposé une axiomatisation
- On a échappé au paradoxe de BERRY en changeant l'axiome de compréhension en axiome de compréhension réduit
- Restait encore le paradoxe de Russell auquel on a échappé en remplaçant l'axiome de compréhension réduit par les axiomes de séparation et en introduisant les axiomes de la paire, de l'union et des parties

On espère maintenant que ce système ne contiendra plus d'autres paradoxes et sera suffissamment riche pour pouvoir fonder la théorie des ensembles .

Pour pouvoir fonder une théorie des ensembles basée sur les axiomes de séparation, l'axiome d'extensionnalité, de la paire, de l'union et des parties il nous faudrait alors :

- fonder une théorie particulière pour chaque type τ et chaque signature adaptée à τ

Mais en fait, cela n'est pas ce qu'on cherche. On cherche à fonder une théorie des ensembles « globale », indépendamment du type (par exemple ensembles d'entiers, ensembles des réels etc). Une possibilité qui s'offre ici est de se restreindre aux ensembles, dits *purs*. Sans trop préciser la définition d'un ensemble pur on se contente ici de dire que travailler avec des ensembles purs veut dire se placer dans un environnement où tous les objets sont des ensembles qui eux-mêmes contiennent de nouveau des ensembles qui eux-mêmes contiennent des ensembles ... Il existe au moins un tel ensemble, à savoir l'ensemble vide $\emptyset$. En ce qui concerne le choix d'une signature, il faut remarquer que les opérations et relations ensemblistes (voir section 2 de ce chapitre) se définissent juste à partir de $\in$ et les autres signes (voir liste plus haut) présentes dans une signature. Notant $\mathbf{Ens}_{\text{pur}}$ le type des ensembles purs on peut donner alors la définition suivante :

Définition *formule ensembliste*

On note $\sum_{\text{ens}}$ la signature comportant un unique type d'objets $\boldsymbol{Ens}_{\text{pur}}$ et un unique symbole de relation binaire $\in$ et on appelle formule ensembliste *toute formule du premier ordre en la signature $\sum_{\text{ens}}$.*

Etant maintenant dans la situation où toutes les variables sont du même type, à savoir du type $\mathbf{Ens}_{\text{pur}}$, il n'est plus nécessaire de typer les variables dans les formules ensemblistes et on peut maintenant présenter une première base de la théorie des ensembles, le systeme $\mathcal{Z}_{\text{fini}}$:

Définition *système $\mathcal{Z}_{\text{fini}}$*

On note $\mathcal{Z}_{\text{fini}}$ le système consistant en les axiomes d'extensionnalité, de la paire, de l'union, des parties et pour chaque formule ensembliste $\mathcal{F}$, de l'axiome de séparation en $\mathcal{F}$.

Le système $\mathcal{Z}_{\text{fini}}$ consiste donc en la liste (infinie !) des axiomes suivantes :

(Ext) $\forall a, b\ (\forall x(x \in a \Leftrightarrow x \in b) \Rightarrow a = b)$

(Paire) $\forall a, b\ \exists c\ (a \in c \text{ et } b \in c)$

(Un) $\forall a\ \exists b\ \forall x\ (\exists y(x \in y \text{ et } y \in a) \Rightarrow x \in b)$

(Par) $\forall a\ \exists b\ \forall x\ (\forall y(y \in x \Rightarrow y \in a) \Rightarrow x \in b)$

et, pour chaque formule ensembliste $\mathcal{F}(x, a_1, \ldots, a_n)$ où les variables a et b n'apparaissent pas (au moins pas comme variables libres)

(Sep_F) $\forall a, a_1, \ldots, a_n\ \exists b\ \forall x\ (x \in b \Leftrightarrow (x \in a \text{ et } \mathcal{F}(x, a_1, \ldots, a_n)))$

Si on utilise $\mathcal{Z}_{\text{fini}}$ comme base de travail, on constate que ce système est déjà riche mais quand même « incomplet » à plusieurs égards. Un premier aspect est qu'il n'y a aucun axiome qui garantit qu'il existe un ensemble. Les mathématiciens ont été amenés à baser la théorie des ensembles sur le système **ZFC** (dit système de Zermelo-Fraenkel avec axiome du choix) qui consiste en les axiomes de $\mathcal{Z}_{\text{fini}}$ et les axiomes suivants :

1. L'axiome de l'ensemble vide *(il y a un ensemble sans éléments noté $\emptyset$)*

$$\exists B : \forall A : \text{ non } (A \in B)$$

FIG. 2.3 – illustration de l'ensemble vide

2. L'axiome de l'infini *(il y a un ensemble A qui contient l'ensemble vide et pour chaque élément x aussi $x \cup \{x\}$)*

$$\exists A(\emptyset \in A \wedge \forall X(X \in A \Rightarrow X \cup \{X\} \in A))$$

3. L'axiome de fondation *(chaque ensemble non-vide A contient un élément B tel que A et B soient disjoints)*

$$\forall A(A \neq \emptyset \Rightarrow \exists B(B \in A \wedge \text{ non}\exists C(C \in A \wedge C \in B)))$$

4. L'axiome de remplacement

$$\forall A\ \exists B\ \forall C\ (C \in B \Leftrightarrow \exists D(D \in A \wedge F(D, C)))$$

et l'axiome du choix.

Conclusion
Les mathématiques, science déductive, ont besoin d'axiomes. Ce chapitre a montré que le choix des axiomes n'est pas arbitraire (même si on a toujours plusieurs choix possibles qui amènent à une théorie cohérente et le choix définitif résulte de discussions et consensus) En revanche, ce processus est souvent très difficile car il faut à la fois construire suffisemment d'axiomes pour décrire les objets qui nous intéressent et éviter les contradictions. Historiquement, la construction d'axiomes adéquats se fait par corrections successives, les paradoxes étant le moteur de cette évolution.

Chapitre 3

La multiplication des pains

« Jésus prit les cinq pains et les deux poissons, et,
levant les yeux vers le ciel, il les bénit.
Puis, il les rompit, et les donna aux disciples,
afin qu'ils les distribuassent à la foule.
Tous mangèrent et furent rassasiés,
et l'on emporta douze paniers pleins des morceaux qui restaient.' »
évangile de Luc 9, 16 - 17

Introduction

Le but de cette partie est de démontrer le théorème de Banach-Tarski. Il s'énonce comme suit :

soient A et B deux parties quelconques dans $\mathbf{R}^3$ telles que chacune contienne une boule et soit contenue dans une boule : par exemple
A = une grenouille et B = un boeuf
ou bien
A = un pain et B = un millier de pains
ALORS
il existe une manière de découper A en un nombre fini de morceaux tel qu'en recollant ces morceaux d'une certaine manière on parvienne à reconstituer B.

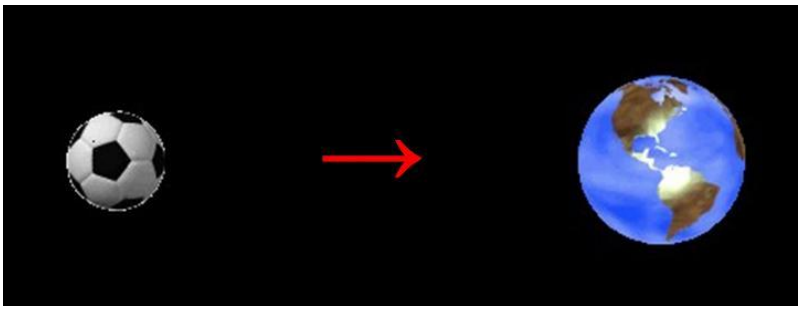
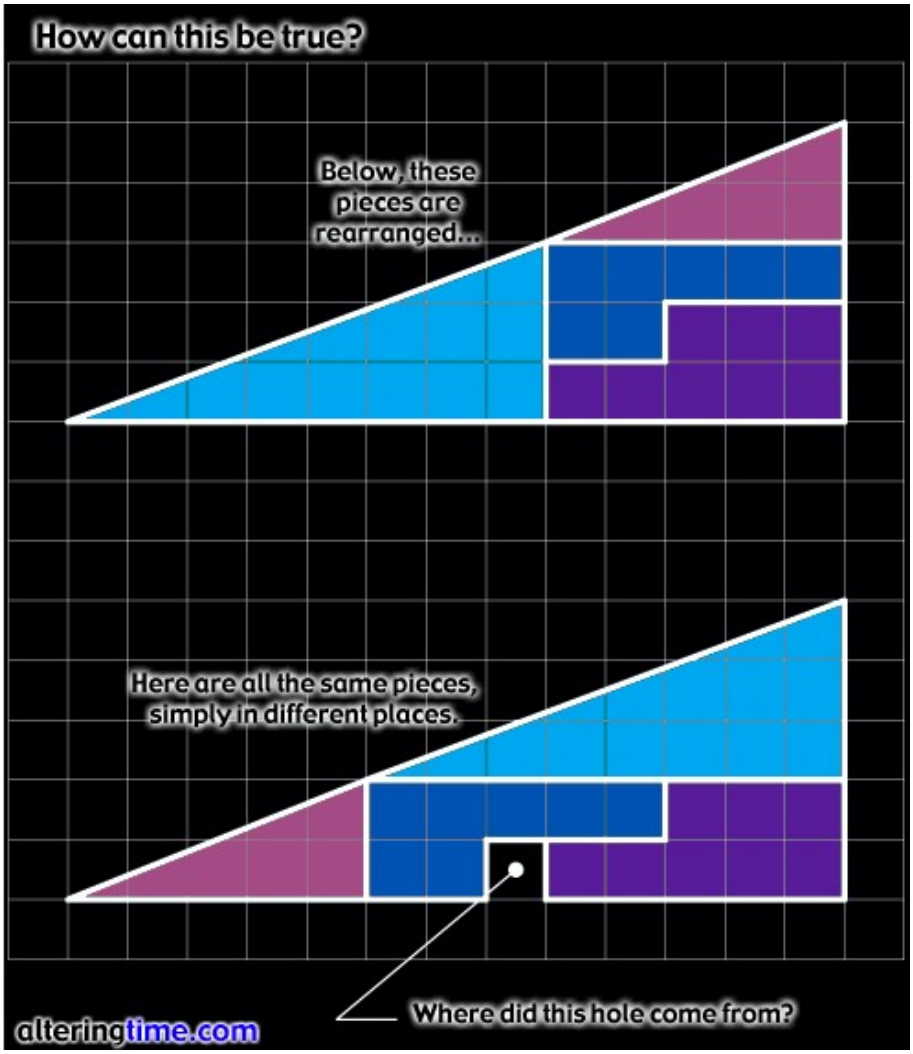


FIG. 3.1 – On peut découper un ballon et reconstituer la Terre entière avec les morceaux.

Remarque: Rien n'impose que A et B aient le même volume : intuitivement, il y a génération (ou destruction) de matière. Dit autrement, on reconstitue B tout entier (sans trous).

Historiquement ce théorème a servi à montrer que dans $\mathbf{R}^3$, il n'existe pas de mesure non nulle, simplement additive, invariante par déplacement et universelle (i.e qui mesure toute partie bornée) alors qu'il en existe dans $\mathbf{R}^2$ ou dans $\mathbf{R}$ (pour en savoir plus cf 3.6 page 47). Dans le cadre de la logique, ce théorème nous intéresse pour deux raisons. D'une part, il illustre la différence qu'il y a en mathématiques entre un paradoxe et une vérité fortement contre-intuitive (le théorème de Banach Tarski appartenant à la seconde catégorie). D'autre part, il fait explicitement appel à l'*axiome du choix indénombrable* (cf « Le paradoxe aux cents têtes ») montrant ainsi que les problématiques autours de l'axiome du choix ne sont pas purement théoriques et influent sur notre manière de percevoir l'espace.



3.1 Définitions

Les lettres A,B,C et D désignent des éléments de $P(\mathbf{R}^3)$ et les lettres S et K respectivement la sphère unité et la boule unité de $\mathbf{R}^3$ et O leur centre.

Définition 1 *A et B sont dits superposables s' il existe un déplacement D tel que $A = D(B)$; on écrit alors $A\mathcal{D}B$.*

Définition 2 *A et B sont dits puzzle-superposables si il existe $n \in \boldsymbol{N}$, $(A_i)_{i=1..n}$ et $(B_i)_{i=1..n}$ découpages (≡partitions) respectifs de A et B tels que $\forall i\ A_i\mathcal{D}B_i$; on écrit alors $A\mathcal{P}B$.*

Remarque: $\mathcal{D}$ et $\mathcal{P}$ sont des relations d'équivalences.

Théorème de Banach-Tarski
Soient A et B bornés, d'intérieur non vide. Alors $A\mathcal{P}B$.

La démonstration suit.

3.2 Deux lemmes

Lemme 1 *Toute boule est puzzle équivalente à elle même privée de son centre (ou de n'importe quel autre point).*

Démonstration

Il suffit de montrer que : $K\ \mathcal{P}\ K - O$.
Soit $\Delta = \{(\cos\ n,\ \sin\ n,\ 0); n \in \mathbf{N}\}$ et r la rotation d'axe (Oz) et d'angle un radian.
Ainsi $r(\Delta) = \Delta - a$ [1] où $a = (1, 0, 0)$.

On a donc $K\ \mathcal{P}\ (K - a)$ car [2] $K \left\{ \begin{array}{ccc} \Delta & \mathcal{D} & \Delta - a \\ K - \Delta & \mathcal{D} & K - \Delta \end{array} \right\} K - a$

D'autre part $K - a \left\{ \begin{array}{ccc} K - \{a; O\} & \mathcal{D} & K - \{a; O\} \\ O & \mathcal{D} & a \end{array} \right\} K - 0$ i.e $K - a\ \mathcal{P}\ K - O$

Enfin $K\ \mathcal{P}\ K - O$.

■

Lemme 2 *Soit $D \subset S$ un ensemble dénombrable. Alors $(S - D)\ \mathcal{P}\ S$.*

Démonstration

[1] en toute rigueur on devrait écrire $\Delta - \{a\}$

[2] cette écriture signifie que $(\Delta, K - \Delta)$ est une partition de K, $(\Delta - a, K - \Delta)$ est une partition de $K - a$ et que l'on passe d'une partition à l'autre par des déplacements

Soit δ tel que ni δ ni $-\delta$ ne sont dans $S - D$ (il en existe car sinon D a le cardinal d'une demi-shpère).

$\forall (x, y) \in D^2 : \ \forall n \in \mathbf{N}^* \ :$

il existe au plus n rotations r d'axe $(-\delta, \delta)$ telles que $r^n(x) = y$.

(il suffit de distinguer le cas où x et y sont à égale distance de $(-\delta, \delta)$ du cas où ils ne le sont pas)

Donc $A = \{r$ rotation d'axe $(-\delta, \delta) / \ \exists n \in \mathbf{N}^*, \ (x, y) \in D^2 : \ r^n(x) = y\}$ est dénombrable.
En effet $A = \bigcup_{n \in \mathbf{N}^*, (x,y) \in D^2} A_n(x, y)$
avec $A_n(x, y) = \{r$ rotation d'axe $(-\delta, \delta) / r^n(x) = y \ \}$ (on rappelle que D est dénombrable)

Dès lors comme l'ensemble des rotations d'axe $(-\delta, \delta)$ est dénombrable, il existe ρ d'axe $(-\delta, \delta)$ tel que pour tout n dans $\mathbf{N}^*$ et pour tout couple (x, y) dans D^2 : $\rho^n(x) \neq y$.
i.e $\forall n \in \mathbf{N}^* \ \rho^n(D) \subset S - D$

Soit alors $U = \bigcup_{n \in \mathbf{N}} \rho^n(D)$,
ainsi $\rho(U) = \bigcup_{n \in \mathbf{N}^*} \rho^n(D) = U - D$.

Ainsi $S \left\{ \begin{array}{ccc} U & \mathcal{D} & U - D \\ S - U & \mathcal{D} & S - U \end{array} \right\} S - D$ i.e $(S - D) \ \mathcal{P} \ S$

■

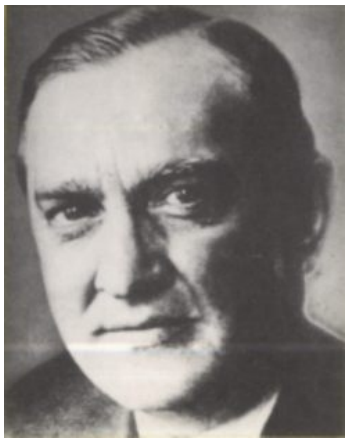


FIG. 3.2 – Stefan Banach (1892-1945)

3.3 Paradoxe de la Sphère (Hausdorff 1914)

Paradoxe de la Sphère
il existe (A, B, C, D) *un découpage de* S *vérifiant :*
– D *est dénombrable ;*
– $A \mathcal{D} B \mathcal{D} C$;
– $(B \cup C)\ \mathcal{D} A$.

Remarque: on a aussi $(C \cup A)\ \mathcal{D}\ B$ et $(A \cup B)\ \mathcal{D}\ C$; malgré les apparences A,B et C ont exactement le même « statut ».

Démonstration

Nous allons procéder en deux temps.

1. construire un groupe de rotations G engendré par deux rotation u et v et trouver une partition I, J et K de G vérifiant : $J = vI$; $K = vJ$; et $I = u(J \cup K)$.
2. appliquer G à la sphère

Etape 1

Soient u et v deux rotations de matrices respectives U et V définies par :

$$U = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & \sqrt{3}/2 \\ 0 & -\sqrt{3}/2 & -1/2 \end{pmatrix}$$

Soit G le groupe engendré par u et v. Soit $r \in G - \{Id; u\}$. Alors comme $u^2 = Id$ et $v^3 = Id$:

$$(*) \qquad r = u^{\varepsilon_1} v^{n_k} u v^{n_{k-1}} \dots u v^{n_1} u^{\varepsilon_2} \text{ avec } \begin{cases} \varepsilon_1, \varepsilon_2 \in \{0; 1\} \\ n_1, \dots, n_k \in \{1; 2\} \end{cases}$$

Montrons que cette écriture est unique puis utilisons-la pour classer les éléments de G.
Par récurrence, on montre que r a pour matrice R telle que :

$$R = \tfrac{1}{2^k} \begin{pmatrix} P_1 & P_2 & P_3\sqrt{3} \\ P_4 & I_1 & I_2\sqrt{3} \\ P_5\sqrt{3} & I_3\sqrt{3} & I_4 \end{pmatrix}$$

où les I_i sont des entiers impairs et les P_i des entiers pairs.

Ceci montre que toute rotation r de G qui s'écrit de la manière (*) est distincte de l'identité (et de u).
On en déduit que l'écriture (*) est unique. En effet si $r = u^{\varepsilon_1} v^{n_k} u v^{n_{k-1}} \dots u v^{n_1} u^{\varepsilon_2} = u^{\varepsilon_1'} v^{n_{k'}'} u v^{n_{k'-1}'} \dots u v^{n_1'} u^{\varepsilon_2'}$ alors d'après la forme de R, on a $k' = k$ et donc $r \circ r^{-1} = Id = u^{\varepsilon_1} v^{n_k} u v^{n_{k-1}} \dots u v^{n_1} u^{\varepsilon_2} u^{-\varepsilon_2'} v^{-n_1'} \dots u v^{-n_{k-1}'} u v^{-n_k'} u^{-\varepsilon_1'}$. Comme cette écriture ne peut pas être du type (*) on a nécéssairement $\varepsilon_2 = \varepsilon_2'$ puis de même $v^{n_1} = v^{n_1'}$

et ainsi de suite.

Dès lors, on peut classer les rotations de G selon leur écriture (*) dans trois sous-ensembles de G : I,J et K.
Dans I on met toutes les rotations de la forme $(v^2u)^n$ (donc $Id \in I$).
Dans J on met toutes les rotations de la forme $u(v^2u)^n$ (donc $u \in J$).
Dans K on met toutes les rotations de la forme $vu(v^2u)^n$.
Pour les rotations restantes on met celles dont le premier terme dans (*) est u (resp. v et v^2) dans I (resp. J et K). Par exemple, v ou vuv (mais pas vu) sont dans J et v^2uv (mais pas v^2u) est dans K.
On a ainsi les relations suivantes :

(1) $J = vI$

(2) $K = vJ$

(3) $I = u(J \cup K)$.

Ces égalités se montrent simplement par double inclusion (par exemple $vI \subset J$ et $v^2J \subset I$ pour $J = vI$).

Remarque: Un classement plus simple pour obtenir les mêmes relations semble être le suivant : les rotations de premier terme u vont dans I, celles de premier terme v dans J et celles de premier terme v^2 dans K. Cependant, de cette manière Id (et u aussi en fait) n'est pas classée et aucuns des trois ensembles ne lui convient si on veut que les relations (1), (2) et (3) soient valables.

Etape 2

Appliquons G à S et étudions ses orbites ($\equiv$ classes d'équivalence de $\mathcal{R}$ où $\mathcal{R}$ est définie par $x\mathcal{R}y \Leftrightarrow \exists r \in G : \ y = r(x)$).
Tout d'abord enlevons tous les points qui peuvent être des points fixes.
Soit $D = \{x \in S / \ \exists r \in G - \{Id\} : \ r(x) = x\}$.
Comme toute rotation a au plus 2 points fixes sur S et que G est dénombrable, D est dénombrable.
De plus, D est stable par G ($x \in D$ et $r \in G \ \Rightarrow \ r(x) \in D$) donc $S - D$ est stable par G.
Ainsi, on peut parler des orbites de G sur $S-D$ (qui forment une partition de $S-D$).

Soit T un ensemble constitué d'un élément de chaque orbite (**axiome du choix indénombrable**). Soit alors :

$$A = I(T)$$
$$B = J(T)$$
$$C = K(T)$$

1. (A, B, C) est un découpage de $S - D$:
   a) A, B et C sont disjoints car on a ôté les points fixes (...)
   b) $A \cup B \cup \ C = S - D$ car $I \cup J \cup \ K = G$
2. $B = v(A), \ C = v(B)$ et $A = u(B \cup C)$ (d'après (1),(2) et (3))

On a enfin le découpage souhaité : (A, B, C, D) avec $A\mathcal{D}B\mathcal{D}C$, $A\mathcal{D}(B \cup C)$ et D dénombrable.

■

FIG. 3.3 – Felix Hausdorff (1868-1942)

3.4 Duplication de la Boule

Commençons par dupliquer la sphère à l'aide du théorème précedent.
Soient S_1 (resp. S_2) la sphère de rayon 1 et de centre O_1 (resp. O_2) ; O_1 et O_2 sont pris de manière à ce que S_1 etS_2 soient disjointes.
Soit (A_1, B_1, C_1, D_1) le découpage de S_1 obtenu par la translation de vecteur $\overrightarrow{OO_1}$ à partir du découpage (A, B, C, D) de S donné par le paradoxe de la sphère. De même pour l'indice 2.
On a donc en utilisant des relations du type $B\mathcal{D}A\mathcal{D}A_1$:

$$S - D \left\{ \begin{array}{lllll} A & \mathcal{D} & B \cup C & \mathcal{P} & A_1 \cup A_2 \\ B & \mathcal{D} & C \cup A & \mathcal{P} & B_1 \cup B_2 \\ C & \mathcal{D} & A \cup B & \mathcal{P} & C_1 \cup C_2 \end{array} \right\} (S_1 - D_1) \cup (S_2 - D_2)$$

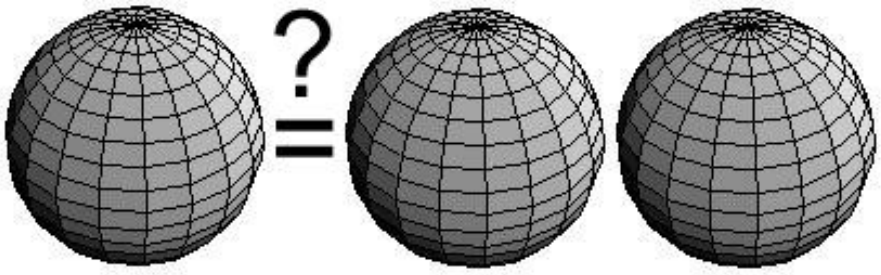
Donc $(S - D)\ \mathcal{P}\ (S_1 - D_1) \cup (S_2 - D_2)$.
D'après le **Lemme 2.** on en déduit $S\ \mathcal{P}\ (S_1 \cup S_2)$

Pour dupliquer la boule il suffit de procéder comme suit :
- d'après ce qui précède, on a une partition de S, $(A_i)_{i=1..n}$, une partition de $S_1 \cup S_2$, $(B_i)_{i=1..n}$ et n déplacements D_i qui transforment A_i en B_i.
- $\forall i$ soit $A_i' = \{]O; x];\ x \in A_i\}$ et $B_i' = \{]O_1; x_1];\ x_1 \in B_i \cap S_1\} \bigcup \{]O_2; x_2]; x_2 \in B_i \cap S_2\}$
- alors $\forall i\ B_i' = D_i(A_i')$
- donc $K/\{O\}\ \mathcal{P}\ (K_1/\{O_1\} \cup K_2/\{O_2\})$[3]

Le **Lemme 1.** permet de conclure :

$$B\ \ \mathcal{P}\ \ (\ B_1\ \cup\ B_2\ )$$

Par une récurrence immédiate, on obtient que toute boule de rayon 1 est puzzle-superposable à n boules de rayon 1 disjointes deux à deux. On a le même résultat avec une boule de rayon quelconque.



[3] K_1 (resp. K_2) désignent la boule de centre O_1 (resp. O_2) et de rayon 1

3.5 Théorème de Banach-Tarski

Théorème 3.1 (dit de Cantor-Bernstein) *Soient $a \subset A$ et $b \subset B$. Alors :*

$$A\mathcal{D}b \text{ et } b\mathcal{D}B \;\Rightarrow\; A\mathcal{D}B$$

Démonstration

La démonstration est exactement celle du théorème de Cantor-Bernstein de la théorie des ensembles qui énonce que si il y a une injection de A vers B et une injection de B vers A alors il y a une bijection entre A et B.
Soient
– $(A_i)_{i=1..n}$, $(a_i)_{i=1..m}$, $(B_i)_{i=1..m}$ et $(b_i)_{i=1..n}$ des découpages respectifs de A,a,B et b
– $(f_i)_{i=1..n}$ et $(g_i)_{i=1..m}$ des suites finies de déplacements
tels que $\forall i f_i(A_i) = b_i$ et $g_i(B_i) = a_i$

Soit f (resp. g) l'injection définie sur A (resp. B) qui coincide avec f_i (resp. g_i) sur chaque A_i (resp. B_i).
Soit $X = \bigcup_{n\in\mathbf{N}}(g \circ f)^n(a)$ et h définie de A dans B la fonction qui coincide avec f sur $A - a$ et g^{-1} sur a. En utilisant les méthodes classiques on montre facilement que h est bijective.
On utilise alors le découpage suivant de A :

$$((X \cap A_i)_{i=1..n},\ ((A/X) \cap a_i)_{i=1..m}))$$

h est un déplacement sur chacun de ces ensembles et transporte ce découpage en un découpage de B. Donc $A\ \mathcal{P}\ B$.

■

Théorème de Banach Tarski : *Soient A et B bornés, d'intérieur non vide. Alors $A\mathcal{P}B$.*

Démonstration

Il suffit de montrer que pour tout A borné d'intérieur non vide, A est puzzle-équivalent à la boule unité K.

A est d'intérieur non vide donc il contient une boule K_r de rayon $r > 0$. Il est borné c'est à dire inclu dans un compact ; ainsi il existe un recouvrement fini de A par des boules de rayons r : $(K_i)_{i=1..n}$. On définit alors $(A_i)_{i=1..n}$ de la manière suivante :

$$A_1 = A \cap K_1,\ A_2 = (A \cap K_2) - A_1,\ \cdots,\ A_n = (A \cap K_n) - A_1.$$

On translate les K_i (et les A_i qui sont à l'intérieur) hors de A de manière à ce qu'elles soient toutes disjointes deux à deux. L'union de ces n boules est puzzle-équivalente à K_r donc $\bigcup_{i=1..n} A_i$ (c'est à dire A) est puzzle-équivalent à un sous-ensemble de K_r.

D'autre part K_r est inclue dans A donc puzzle-équivalente à une sous-partie de A. Dès lors le théorème de Cantor-Bernstein énonce que :

$$A \mathcal{P} K_r$$

En appliquant ce résultat pour $A = K$ on obtient que $\forall r < 1 : \ K \mathcal{P} K_r$. En appliquant ce résultat pour tout $r > 1$ avec $A =$ *une boule de rayon* r on trouve que $\forall r > 1 : \ K \mathcal{P} K_r$.

$$\text{Donc } A \ \mathcal{P} \ K_r \ \mathcal{P} \ K.$$

■

FIG. 3.4 – Alfred Tarski (1902-1983)

3.6 Mesures universelles sur R et $\mathbf{R}^2$

Il existe des mesures universelles (c'est à dire qui mesurent tout), simplement additives invariantes par les isométries et non trivialement nulle sur $\mathbf{R}$ et $\mathbf{R}^2$ (*Banach* - 1923). Elles peuvent être construites à partir du théorème de Von Neumann[4] (qui utilise l'axiome du choix indénombrable).

Théorème de Von Neumann (1929)
Soit G un groupe abélien. Il existe une mesure universelle σ sur G, invariante par translation et telle $\sigma(G) = 1$. Une telle mesure est dite de Von Neumann.

Pour construire une mesure universelle sur $\mathbf{R}$ et $\mathbf{R}^2$ on procède en tois étapes :
- on prend σ une mesure de Von Neuman sur $\mathbf{R}/\mathbf{Z}$ et $\mathbf{R}^2/\mathbf{Z}^2$.
- on étend cette mesure à $\mathbf{R}$ et $\mathbf{R}^2$ (par exemple sur $\mathbf{R}$ on prend $\mu(A) = \sum_{+\infty}^{n=0} \sigma(p(A \cap [n, n+1]))$ où p est la surjection canonique) ; on appelle cette nouvelle mesure qui est toujours invariante par les translations μ.
- pour rendre μ invariante par les isométries on fait des moyennes :
  soit s_o une symétrie centrale (axiale dans le cas de $\mathbf{R}^2$) :

$$\mu_1(A) = \frac{1}{2}(\mu(A) + \mu(s_o(A)))$$

  Pour $\mathbf{R}$ on a fini car μ est invariante par les isométries.
  Pour $\mathbf{R}^2$, on moyenne encore mais sur les rotations :
  Soit σ_2 une mesure de Von Neumann sur $O^+(2)$ (qui est abélien contrairement à $O^+(3)$).

$$\mu_2(A) = \frac{1}{\sigma_2(O^+(2))} \int_{O^+(2)} \mu_1(r(A)) d\sigma(r)$$

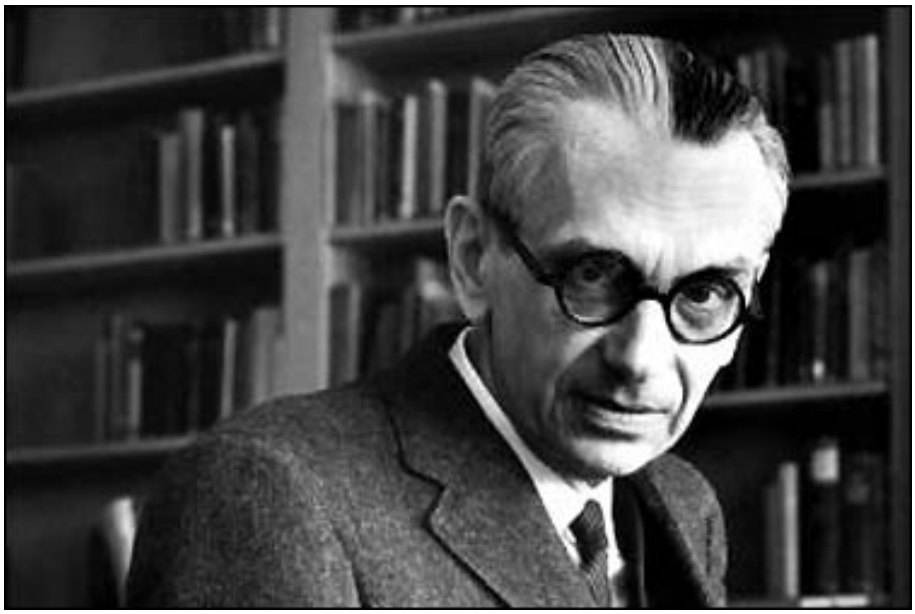
Pour plus d'informations on peut se référer au livre de Marx Guinot (Guinot M., *Le Paradoxe de Banach-Tarski*, Aleas, Lyon(1991).)

[4] Une simple comparaison des dâtes montre que ce n'est pas l'approche qu'a adopté Banach.

Chapitre 4

Le Chapitre 4 n'est pas démontrable

« Les choses capitales qui ont été dites à l'humanité
ont toujours été des choses simples. »
Charles de Gaulle



Premier théorème d'incomplétude de Gödel (1931)
Pour toute classe ω-consistante et récursive k de
FORMULES, il existe des SIGNES DE CLASSE
récursifs r tels ni $\nu GENr$ ni
$NEG(\nu GENr)$ n'appartiennent à $CSQ(k)$.
(ν désigant la $VARIABLE\ LIBRE$ de r)

Le théorème de Gödel

« Le développement des mathématiques vers plus d'exactitude a conduit, comme nous le savons, à en formaliser de larges secteurs, de telle sorte que la démonstration puisse s'y effectuer uniquement au moyen de quelques règles mécaniques. Les systèmes formels les plus complets établis jusqu'à ce jour sont, d'un côté, le système des Principia Mathematica et, de l'autre, le système axiomatique de la théorie des ensembles établi par Zermelo-Fraenkel (et développé par J.von Neumann). Ces deux systèmes sont tellement larges que toutes les méthodes de démonstration utilisées aujourd'hui en mathématiques y sont formalisées, c'est à dire ramenées à quelques axiomes et règles d'inférence. On pourrait par conséquent supposer que ces axiomes et règles d'inférences suffisent pour décider de toute question mathématique qui pourrait s'exprimer formellement dans ces systèmes. Dans ce qui suit, nous montrerons que tel n'est pas le cas et qu'il existe au contraire dans ces deux systèmes des problèmes relativement simples concernant la théorie des entiers que l'on ne saurait trancher sur la base des axiomes. Cette situation n'est pas due comme on pourrait le croire, à la nature spécifique des sytèmes établis mais touche une très large classe de systèmes formels, à laquelle appartiennent en particulier tous les systèmes qui résultent des deux systèmes cités plus haut par addition d'un nombre fini d'axiomes, pourvu que, par ces axiomes, aucune proposition fausse ne puisse être démontrée. »

Kurt Gödel - *Sur les propositions indécidables des Principia Mathematica et des systèmes apparentés I*[1] (1931)

Le premier théorème d'incomplétude de Gödel a été énoncé pour la première fois dans le fameux article *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (*Sur l'indécidabilité formelle des Principia Mathematica et des systèmes apparentés*) publié en 1931. Le but de cette partie est de démontrer ce théorème. Nous précisons que dans le même article Gödel démontrait également son second théorème d'incomplétude mais nous ne nous y intéresserons pas.

Nous avons travaillé à partir d'une traduction française de « Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme » effectuée par Jean-Baptiste Sherrer. Cet article est extrêmement dense et seuls les résultats les plus difficiles y sont démontrés ; aussi nous avons adopté une optique pédagogique en incluant de nombreux exemples.

Dans ce rapport, trouverez une démonstration simplifiée ainsi que la démonstration complète (30 pages). Vous pourrez également trouver les deux démonstrations sur notre site : *http ://www.dirk-k-lange.de/PSC/*.

[1] Le I s'explique de la manière suivante : Gödel avait projeté d'écrire une suite à cet article afin d'en préciser certaines démonstrations. Cependant l'article fut très bien accueilli par la communauté mathématique et Gödel ne jugea pas nécessaire d'écrire ce second volet.

Démonstration simplifiée du théorème de Gödel

4.1 Définition du sytème formel

Construisons un sytème formel $\mathcal{P}$ pouvant décrire les entiers naturels.

Ce système contient des caractères que nous appelerons **signes** (tels que $=$, $0, 1, 2, \ldots$, $\forall$ **:** , x , $y \ldots$).
Ces caractères mis bout à bout selon certaines règles forment des phrases que nous appelerons **formules** (par exemple $\forall n$**:** $n = 0$).
Certaines formules seront appelées **signes de classe** ; ce sont les formules avec une unique variable libre d'entier (par exemple $x = 3$ est un signe de classe). De plus si A est un signe de classe nous désignons par $[A : n]$ la formule obtenue en **substituant** n à la variable de A.
exemple: $[(x = 3) : 7]$ est la formule $7 = 3$.

Ensuite, nous définissons deux sous-ensembles de formules $\mathcal{A}$ et $\mathcal{D}$ avec $\mathcal{A} \subset \mathcal{D}$. Ces ensembles sont construits d'une manière bien particulière :

- $\mathcal{A}$ est appelé l'ensemble des **axiomes** ; les formules dont il est constitué ont la même signification que les axiomes de Peano[2]
- $\mathcal{D}$ est l'ensemble des formules **démontrables** ; pour le construire on définit d'abord une règle de transformation des formules
  - Pour tout entier n, de la formule $(\forall x$**:** $R(x))$ on peut obtenir $R(n)$;
    exemple: on peut transformer $(\forall x$**:** $x = 8)$ en $(3 = 8)$, $(122 = 8)$, $(8 = 8) \ldots$
  - De la formule $f_1 \Rightarrow f$ et de la formule f_1 on peut obtenir la formule f.

  $\mathcal{D}$ sera défini comme l'ensemble des formules que l'on peut obtenir par des transformations successives des axiomes.

4.2 Plongement du sytème $\mathcal{P}$ dans N

Maintenant nous allons injecter ce système dans **N**.

1. A chaque signe nous associons un entier ; par exemple :
   - $= \mapsto 0$
   - $\forall$**:** $\mapsto 1 \ \ldots$
   - $x \mapsto 7$
   - $y \mapsto 8$
   - $\ldots$
2. A chaque suite de signes (et donc à chaque formule) nous associons un entier en utilisant la décomposition en facteurs premiers. On appelera ces nombres les nombres de Gödel.
   exemple: $(\forall x$**:** $x = x) \mapsto 2^1 3^7 5^7 7^0 11^7$

[2]en fait on prend un ensemble un peu plus grand qui est celui décrit dans les *Principia Mathematica* écrit par B.Russell et A.Whitehead publié aux éditions Cambridge en 1925

Tous les concepts définis précédemment sont projetés dans **N**. Par exemple, on dira qu'un entier n est démontrable (et on écrira $Dem(n)$) s'il est le nombre de Gödel d'une formule qui est dans $\mathcal{D}$. De même, on écrira $[a : n]$ le nombre de Gödel de $[A : n]$ (où a est le nombre de Gödel de A).

D'autre part, cette injection de $\mathcal{P}$ dans **N** nous permet de numéroter les signes de classes (selon l'ordre dans lequel sont rangés leurs nombres de Gödel)[3] ; on notera $R(n)$ le nombre de Gödel du signe de classe numéro n.

4.3 Le signe de classe indécidable

Nous considérons maintenant la relation suivante Q définie sur **N** par[4] :

$$Q(n) \Leftrightarrow \overline{Dem}[R(n) : n]$$

Cette relation est une relation sur les nombres entiers donc elle s'exprime par un signe de classe S dans le système $\mathcal{P}$. Ce S correspond à un certain $R(q)$ ($q \in \mathbf{N}$). Alors :

$$[R(q) : q] \text{ est indécidable dans } \mathcal{P}$$

En effet

$$[R(q) : q] \text{ est démontrable } \Rightarrow \overline{Q(q)} \qquad \textbf{(par définition de } \overline{Q}\textbf{)}$$

$$[R(q) : q] \text{ est démontrable } \Rightarrow Q(q) \qquad \textbf{(car } [S : q] \textbf{ est la formule qui exprime } Q\textbf{)}$$

Et

$$(\textit{la négation de } [R(q) : q]) \text{ est démontrable } \Rightarrow \overline{Q(q)}$$

(car la négation de $[S : q]$ **est la formule qui exprime** $\overline{Q}$**)**

$$(\textit{la négation de } [R(q) : q]) \text{ est démontrable } \Rightarrow Q(q) \qquad \textbf{(par définition de } Q\textbf{)}$$

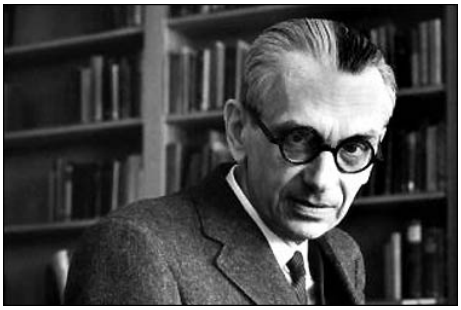


FIG. 4.1 – Kurt Gödel (1906-1978)

[3] cf Le paradoxe de Richard ?? page ??

[4] la barre au-dessus d'une relation représente la négation

Démonstration du théorème de Gödel

Premier théorème d'incomplétude de Gödel (1931)
Pour toute classe ω-consistante et récursive k de $FORMULES$, il existe des $SIGNES\ DE\ CLASSE$ récursifs r tels ni $\nu GENr$ ni $NEG(\nu GENr)$ n'appartiennent à $CSQ(k)$. (ν désigant la $VARIABLE\ LIBRE$ de r)

La majeure partie de cet exposé sera consacrée à expliquer les termes employés dans cet énoncé. Pour commencer nous nous contenterons de la formulation intuitive suivante :
« Il existe des propositions indécidables au sein du système $\mathcal{P}$(et de tout sytème décidable contenant $\mathcal{P}$). »

Schématiquement, le système $\mathcal{P}$ désigne les Mathématiques construites à partir des axiomes suivants.

1. Axiomes de Peano (sur les entiers naturel)
2. Axiomes de la logique propositionnelle
3. Deux axiomes de la théorie des ensembles (axiomes de définition et de compréhension)
4. Deux axiomes sur le quantificateur universel (pour tout : $\forall$)

L'exposé comprend trois parties. Tout d'abord nous allons donner des définitions précises de ce dont nous allons parler c'est à dire du système $\mathcal{P}$; ensuite nous montrerons comment Gödel a construit une proposition indécidable au sein de ce système (et de tout système décidable contenant $\mathcal{P}$). Lors de la démonstration nous aurons admis une notion, un théorème et une propriété tous les trois liés à la notion de *fonctions récursives* ; le but de la dernière partie est de définir cette notion ainsi que de démontrer ce théorème et cette propriété.

4.4 Le système $\mathcal{P}$

Le point le plus important à comprendre pour toute la suite est le suivant. Nous allons étudier des formules c'est à dire des suites de signes **indépendemment de toute signification mathématique** ; tout ce qui nous intéressera sera la structure de ces formules. En ce sens notre travail s'apparentera à celui du grammairien ; en effet le grammairien dira que la phrase « Le bol de soupe chante le fromage de la Tour Eiffel. » est correcte sans se préocupper de son sens.
Cette étude des formules c'est à dire du langage mathématique s'appelle les *métamathématiques* (cf *La théorie des ensembles et le processus d'axiomatisation* page 17) ; on peut utiliser le racourci suivant : les métamathématiques sont aux mathématiques ce que la grammaire française (étude syntaxique) est au français (étude sémantique).

Nous allons procéder en trois étapes (entre parenthèses appaissent les concepts analogues pour le grammairien quand ils existent) :

1. **définir les signes** que nous allons utiliser (**les lettres**) ;
   exemples : $\sim$ ou Π qui représentent respectivement la négation et le quantificateur universel ;
   nous définirons également des propriétés sur l'ensemble des signes (certaines lettres ont la propriété d'être accentuées) ;
   exemple: être une variable libre.
2. **définir les suites de signes valides** (les **mots**) ; on nommera ces suites « **formules** » ;
   nous définirons également des **propriétés** (de la même manière que certains mots ont la propriété d'être des noms communs singuliers) ainsi qu'une **fonction** sur les formules à valeur dans l'ensemble des formules (en grammaire par exemple, sur un certain sous-ensemble des noms communs singuliers je peux définir la fonction à valeur dans les mots, qui à chaque éléments de son ensemble de définition associe cet élément suivi de la lettre « s » : « rat $\mapsto$ rats », « pelle $\mapsto$ pelles »...).
3. définir une propriété particulière : **être démontrable** ;
   - faire une liste de formules que l'on posera comme étant démontrables (les **axiomes**) ;
   - définir des **règles de transformation** qui permettent d'obtenir une formule démontrable à partir d'autres formules démontables ;

Il nous restera alors à exhiber un signe de classe[5] r de variable libre x_1 tel que :

$$\text{ni } \ll x_1\Pi(r) \gg \text{ ni } \ll \sim x_1\Pi(r) \gg \text{ ne sont démontrables}$$

Ceci signifiera qu'on a trouvé une propriété $P(n)$ dépendant de n telle que ni $\forall n P(n)$ ni $\exists n / \overline{P(n)}$ ne sont démontrables.

[5] un signe de classe est une formule particulière qui à la « signification » d'une propriété dépendant d'une variable d'entier : voir plus loin

4.4.1 Les signes primitifs

Un signe primitif est un symbole de la liste suivante :

$$\begin{array}{cccccccccc} & & & & \sim & , & \vee & , & \Pi & , & 0 & , & f & , & (& , &) \\ x_1 & , & y_1 & , & z_1 & , & \ldots & & & & & & & & & & \text{(variables de type 1 : v1)} \\ x_2 & , & y_2 & , & z_2 & , & \ldots & & & & & & & & & & \text{(variables de type 2 : v2)} \\ \vdots & & \vdots & & \vdots & & \vdots & & & & & & & & & & \\ x_n & , & y_n & , & z_n & , & \ldots & & & & & & & & & & \text{(variables de type n : vn)} \end{array}$$

Remarque: on suppose qu'on dispose d'un nombre infini de signes pour chaque variable de type n. On appelle $\mathcal{S}$ l'ensemble des suites finies de signes.
exemple: $y_{58}f(\Pi z_3 \sim$ est dans $\mathcal{S}$ et on dira que y_{58} est une v58.

Définition 3 *On appelle signe de type 1 (s1) tout élément de $\mathcal{S}$ d'une des formes suivantes :*

$$\begin{array}{ccccc} 0 & f0 & ff0 & fff0 & \ldots \\ x_1 & fx_1 & ffx_1 & \ldots & \\ y_1 & fy_1 & \ldots & & \\ z_1 & \ldots & & & \\ \vdots & & & & \end{array}$$

On appelle signe de type n (sn) tout élément de $\mathcal{S}$ étant une variable de type n.
exemple: *x_2 est un signe de type 2, z_{32} est un s32.*

4.4.2 Formules

Avant de donner une définition rigoureuse des formules faisons une description intuitive.
Les formules vont correspondre à des suites de signes auxquelles on peut attacher une signification ; ainsi l'ensemble des formules $\mathcal{F}$ est inclu dans $\mathcal{S}$.
Commenons tout d'abord par expliquer quelle signification on peut donner à chacun des signes primitifs ; dans l'absolu connaître cette signification est superflu mais cela facilite la compréhension de la notion de formule. Voici une liste qui permet de mieux « sentir » les objets que nous allons manipuler.

$$\begin{array}{rcl}
\vee & \longrightarrow & \text{« ou »} \\
\sim & \longrightarrow & \text{« non »} \\
0 & \longrightarrow & \text{« zéro »} \\
f & \longrightarrow & \text{« successeur de »} \\
fff0 & \longrightarrow & \text{« trois »} \\
x_1,\, y_1,\, \ldots & \longrightarrow & \text{« variable d'entier »} \\
x_2,\, y_2,\, \ldots & \longrightarrow & \text{« variable d'ensemble d'entiers »} \\
x_3,\, y_3,\, \ldots & \longrightarrow & \text{« variable d'ensemble d'ensembles d'entiers »} \\
\vdots & \vdots & \vdots \\
x_1\Pi & \longrightarrow & \text{« } \forall x_1 \text{ »} \\
x_2(x_1) & \longrightarrow & \text{« } x_1 \in x_2 \text{ »}
\end{array}$$

Ainsi la formule « $x_1\Pi(x_2(x_1))$ » s'interprétera comme « tout entier est dans l'ensemble x_2 ».

Remarque: on n'a pas introduit de variables pour coder les fonctions de **N** dans **N** ; cela aurait été superflu. En effet une telle fonction est un graphe c'est à dire un ensemble de couples d'entiers ; le couple (a,b) peut lui-même être vu comme un ensemble d'ensembles d'entiers i.e $\{\{a\},\{a,b\}\}$. Ainsi une fonction à une variable entière sera codée par une v4 ; de même on code les fonctions à n variables entières (à valeurs dans **N**) par des v(2n+2).

Remarque: on peut se demander pourquoi Gödel n'a pas utilisé les signes habituels $\forall$ ou $\in$ alors qu'ils lui étaient connus. La raison est simple ; nous utilisons le langage auquel nous sommes habitués ($\forall, :\, \exists, \in, 2\ldots$) pour notre étude (qui relève des mathématiques) et il est nécésssaire de le distinguer du langage que nous étudions ($\Pi, E, f\ldots$) pour éviter les confusions.

Définition 4 *Une formule est un élément de $\mathcal{S}$ d'une des formes suivantes :*

$$\begin{array}{cc} a & (b) \\ \nearrow & \uparrow \\ s(n+1) & sn \end{array}$$

exemple: $x_2(z_1)$
contre-exemple: $y_5(z_7)$

$$\begin{array}{ccccccc} & & & & ou & & \\ (a) \vee (b) & ou & \sim (a) & ou & & x\Pi(a) & \\ \nwarrow\nearrow & & \uparrow & & & \uparrow \quad \uparrow & \\ formules & & formule & & & v1\ formule & \end{array}$$

exemples: $(x_2(z_1)) \vee (y_{32}(x_{31}))\ ;\ \sim (y_1\Pi(y_4(y_3)))$

Nous allons également utiliser la notion d'occurence libre (ou liée) et de variable libre ou liée. Plutôt que de donner une définition rigoureuse qui serait compliquée on se contentera de cet exemple qui se veut exhaustif :

$$\begin{array}{ccccccccccc} x_2\Pi(& & ((x_2(x_1)) & \vee & (x_1\Pi(& & y_2(x_1)) &) &) \\ \uparrow & & \uparrow\ \uparrow & & \uparrow & & \uparrow\ \uparrow & & \\ \text{liée} & & \text{liée libre} & & \text{liée} & & \text{libre liée} & & \end{array}$$

Sous chacune des occurences des variables apparaît la nature de cette occurence (regarder les quantificateurs universels). Si toutes les occurences d'une variable sont liées (resp. libres) la variable est dite liée (resp. libre). Ici x_2 est liée, y_1 est libre et x_1 n'est ni l'un ni l'autre.

Définition 5 *Une formule ayant n v1 libres et dont toutes les autres varaiables sont liées est appelée* ***signe de relation à n places.***

Un signe de relation à n places correspond à une propriété dépendant de n entiers. Pour $n = 1$ on se contentera de dire **signe de classe**.
exemple: $x_2\,\Pi\,(x_2(x_1))$ est un signe de classe de variable libre x_1.

Nous allons maintenant définir une fonction de $\mathcal{F}$ dans $\mathcal{F}$; cette fonction que l'on appellera Sub correspondra à l'opération de substitution d'une variable (les vn) par une valeur (les $f \ldots f0$) ou par une autre variable.
Soit ν une vn et b un sn ; alors $Sub\ \bullet_b^\nu$ est définie de la manière suivante :

$$\begin{array}{rcll} \mathcal{F} & \longrightarrow & \mathcal{F} & \\ a & \longrightarrow & Sub\ a_b^\nu & \text{qui est la formule obtenue} \\ & & & \text{à partir de } a \text{ en remplaçant} \\ & & & \nu \text{ par } b \text{ à chacune de ses} \\ & & & \textbf{occurences libres.} \end{array}$$

exemples:

- $Sub\ [(x_2(x_1)) \vee (x_2(y_1)]_{ff0}^{y_1} = (x_2(x_1)) \vee (x_2(ff0))$

- $Sub\ [(z_2(x_1)) \vee (z_2\Pi(z_2(y_1)))]\ ^{z_2}_{x_2} = (x_2(x_1)) \vee (z_2\Pi(z_2(y_1)))$
- $Sub\ [x_2(x_1)]^{z_2}_{y_2} = x_2(x_1)$

On définit également les fonction suivantes :

$$Neg : a \longmapsto \sim (a)$$

$$Gen : (\nu,\, a) \longmapsto \nu\Pi(a)$$

où a désigne une formule et ν une variable quelconque.

exemples: $Neg(x_2(x_1)) = \sim (x_2(x_1))$, $x_1\ Gen\ x_2(x_1) = x_1\Pi(x_2(x_1))$.

FIG. 4.2 – Kurt Gödel

4.4.3 Formules démontrables

Nous allons maintenant définir un sous-ensemble de $\mathcal{F}$: l'ensemble des formules démontrables. Pour cela nous allons établir une liste (infinie) de formules appelées axiomes et une relation de conséquence immédiate entre les formules ; une formule f sera alors dite démontrable si :

$\exists(f_1, \ldots, f_n) \in \mathcal{F}^n /$ • $f_n = f$
• $\forall i \leq n$: f_i est un axiome ou une concéquence immédiate d'un ou de plusieurs f_j $(j < i)$.

4.4.3.1 Abréviations

A partir de maintenant, plutôt que d'écrire systématiquement les formules en entier on utilisera les abréviations usuelles suivantes :

$$. \ , \ \supset \ , (Ex) \ , \ \equiv \ , \ =$$

dont les significations sont :

$$\begin{array}{rcl} . & \longrightarrow & \text{« et »} \\ \supset & \longrightarrow & \text{« implique } (\Rightarrow) \text{ »} \\ (Ex) & \longrightarrow & \text{« il existe } x \ (\exists x) \text{ »} \\ \equiv & \longrightarrow & \text{« équivaut } (\Leftrightarrow) \text{ »} \\ = & \longrightarrow & \text{« égal »} \end{array}$$

Les quatres premiers symboles sont des abréviations usuelles des signes primitifs. Par contre, le dernier $(=)$ est plus surprenant, il sera défini ainsi :

$$\begin{array}{l} (a = b) \text{ est une abréviation de } c\Pi(\ (c(a)) \supset (c(b))\ ) \\ \quad\uparrow \quad\uparrow \qquad\qquad\qquad\qquad\qquad\qquad\quad \uparrow \\ \quad \text{sn} \quad \text{sn} \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{s(n+1)} \end{array}$$

On évitera également d'écrire les parenthèses superflues (même s'il faut se rappeler qu'en fait elles sont toujours là). On utilisera également le raccourci suivant : $f^n 0$ pour $\underbrace{f f..f}_{n fois} 0$.

4.4.3.2 Axiomes

Voici la liste des axiomes donnés par Gödel (constater que si on leur attribut une signification ils énoncent tous des banalités).

I **Axiomes de Peano** : $\mathcal{A}_1$

II **Axiomes de la logique** : $\mathcal{A}_2$ (on en déduit toutes les tautologies)

III **Axiomes sur le quantificateur universel** : $\mathcal{A}_3$

IV **Axiomes de compréhension (IV.1) et d'extensionalité (IV.1)**[6] : $\mathcal{A}_4$

I.1 $\sim (fx_1 = 0)$,

I.2 $fx_1 = fy_1 \supset x_1 = y_1$,

I.3 $x_2(0).x_1\Pi(\ x_2(x_1) \supset x_2(fx_1)\ ) \supset x_1\Pi(x_2(x_1))$;

II toute formule résultant d'un des schémas suivant où p, q et r sont des formules :

II.1 $p \vee p \supset p$,

II.2 $p \supset p \vee q$,

II.3 $p \vee q \supset q \vee p$,

II.4 $(p \supset q) \supset (r \vee p \supset r \vee q)$.

III toute formule résultant d'un des schémas suivant

III.1 $\nu\Pi(a) \supset Sub\ a^{\nu}_{c}$

III.2 $\nu\Pi(b \vee a) \supset (b \vee \nu\Pi(a))$

a est une formule ; ν est une vn ; c est un sn ne contenant pas de variable liée en a et libre en ν ; b est une formule dans laquelle ν n'a pas d'occurences libres
exemple: $x_1\Pi(x_2(x_1)) \supset (x_2(fffy_1))$ est un axiome

IV.1 $(Eu).(\nu\Pi(u(\nu) \equiv a))$
$\uparrow\ \uparrow\qquad\qquad\uparrow$
v(n+1) vn formule sans occurences libres de u
exemple: $(Ex_2)(x_1\Pi(x_2(x_1) \equiv (x_1 = 0 \vee fx_1 = y_1))$ est un axiome ; et x_2 représente l'ensemble $\{0, y_1 - 1\}$.

IV.2 $x_1\Pi(x_2(x_1) \equiv y_2(x_1)) \supset x_2 = y_2$
$x_2\Pi(x_3(x_2) \equiv y_3(x_2)) \supset x_3 = y_3$
$x_3\Pi(x_4(x_3) \equiv y_4(x_3)) \supset x_4 = y_4$
...

[6] cf *Le paradoxe aux cent têtes* page 17

4.4.3.3 Être démontrable

Définition 6

- *c est une conséquence immédiate de a et b si a est* $b \supset c$.
  exemple: $\sim (ff0 = 0)$ *est une conséquence immédiate de*

$$x_1\Pi(\sim (fx_1 = 0)) \supset (\sim (ff0 = 0)) \text{ et } x_1\Pi(\sim (fx_1 = 0))$$

- *c est une conséquence immédiate de a si c est* $\nu\Pi(a)$ *où* ν *est une vn libre en a.*
  exemple: $x_1\Pi(\sim (fx_1 = 0))$ *est une conséquence immédiate de*

$$\sim (fx_1 = 0)$$

.

Définition 7 *Soit k un ensemble de formules.*
Une formule f est dite (k-)démontrable (et on écrit $Dem_k(f)$*) si il existe une suite finie de formules* $f_1, \ldots, f_n$ *vérifiant :*

- $f_n = f$
- $\forall i$ *:* f_i *est un axiome (ou un élément de k) ou une conséquence immédiate d'un ou deux* f_p *antérieurs.*

On dit alors que $f_1, \ldots, f_n$ *(k-)démontre* f_n*. On écrira* $(f_1, \ldots, f_n)Demf_n$ *ou* $(f_1, \ldots, f_n)Dem_kf_n$.

exemple: $\sim (ff0 = 0)$ est une formule démontrable. En effet, on définit la suite f_1, f_2, f_3, f_4 ainsi :
$f_1 : \sim (fx_1 = 0)$ (Axiome I.1)
$f_2 : x_1\Pi(\sim (fx_1 = 0))$ (conséquence immédiate de f_1)
$f_3 : x_1\Pi(\sim (fx_1 = 0)) \supset (\sim (ff0 = 0))$ (Axiome III.1)
$f_4 : \sim (ff0 = 0)$ (concéquence immédiate de f_2 et f_3)

exercice : montrer que $0 = 0$ est démontrable.

Il ne reste qu'à exhiber une propriété indécidable c'est à dire un signe de classe r de variable libre x_1 tel que : ni $x_1\Pi(r)$ ni $\sim (x_1\Pi(r))$ ne sont démontrables.

4.4.4 Commentaires : théorème du sens

On peut trouver le système $\mathcal{P}$ un peu pauvre ; en effet les concepts d'addition, de multiplication, de divisibilité ... semblent absents. En fait, ce n'est pas le cas ; grosso-modo tout ce qui est récursivement définit à partir de la fonction $x \longmapsto x+1$ et des fonctions constantes peut s'exprimer dans le système $\mathcal{P}$.
C'est ce qu'exprime ce théorème ; il dit que le système $\mathcal{P}$ (qui pour le moment n'est qu'un ensemble de symboles bizarres avec des règles tordues) décrit bien les entiers naturels que nous connaissons. La compréhension de cet énoncé est le pivot central de la démonstration.

Théorème du sens
(Théorème V dans l'article de Gödel)
Pour toute relation récursive R à n variables d'entiers il existe un signe de relation à n places r (avec pour variables libres $x_1, y_1 \ldots \nu_1$) tel que :

$\forall (m_1, \ldots, m_n) \in \boldsymbol{N}^n$:

$$R(m_1, \ldots, m_n) \Rightarrow Dem[Sub\, r^{x_1 \ldots \nu_1}_{f^{m_1}0 \ldots f^{m_n}0}]$$

$$\overline{R(m_1, \ldots, m_n)} \Rightarrow Dem[\sim (Sub\, r^{x_1 \ldots \nu_1}_{f^{m_1}0 \ldots f^{m_n}0})]$$

Démonstration

cf 4.7.5 page 77.

■

Ce théorème dit exactement que les *relations* récursives (encore à définir ... cf 4.7 page 69) sont exprimables dans le système $\mathcal{P}$... par des signes de *relation*. « Exprimer » signifie que chaque fois que la relation est vraie le signe de relation après la substitution adéquate est démontrable et à chaque fois que la relation est fausse la négation du signe de relation après substitution est démontrable.

exemple: Soit R définie par $R(x, y) \Leftrightarrow y = x + 1$.
R est récursive et elle a un signe de relation à deux places associé par le théorème du sens : $y_1 = fx_1$.
Les relations à peine plus compliquées nécéssitent des signes de relation beaucoup plus gros

4.5 Une image bi-univoque du système $\mathcal{P}$

FIG. 4.3 – *Print Galley* (Escher-1956)

En définitive, on constatera que le théorème de Gödel est une version du paradoxe de l'autoréférence (cf *Les paradoxes de l'auto-référence* page 17). La démonstration est basée sur le fait que le système $\mathcal{P}$ et la théorie des entiers naturels sont suffisamment complexes pour permettre cette autoréférence. On gardera à l'esprit que la méthode qu'utilise Gödel reste valable dans d'autres systèmes formels (avec des signes primitifs, des formules et des axiomes différents) s'ils sont capables de déduire les axiomes du système $\mathcal{P}$ (ou des équivalents syntaxiques) ; un exemple d'un tel système est celui qui axiomatise la théorie des ensembles (ZF, cf *La théorie des ensembles et le processus d'axiomatisation* page 17)

Comment procéder ?

L'astuce de Gödel a été de plonger le système $\mathcal{P}$ dans l'ensemble des entiers naturels c'est à dire les objets qu'il décrit : techniquement il a construit une bijection G_1 entre $\mathcal{P}$ (c'est à dire l'ensemble des signes, formules et suite de formules) et un sous-ensemble des nombres entiers $\mathcal{G}$ qu'on appellera l'ensemble des nombres de Gödel. Ainsi la propriété « $f_1, \ldots, f_n$ démontre f » se projettera en une propriété sur les entiers de la manière suivante : on dira que n DEMONTRE m (et on écrira $nDEMm$) si et seulement si n et m sont dans $\mathcal{G}$ et $G_1^{-1}(n)$ démontre $G_1^{-1}(m)$. De même on pourra définir une fonction SUB ainsi que des sous-ensembles de $\mathcal{G}$: le sous-ensemble des VARIABLES DE TYPE n, celui des SIGNES DE CLASSE... Une fois cette correspondance établie, on pourra trouver UN SIGNE DE CLASSE qui dira (plus ou moins) « je ne suis pas démontrable ».

Tout d'abord, comment construire G_1 ?

4.5.1 Définition de G_1(à valeur dans N)

Commençons par définir G_1 sur les signes primitifs :

$$\begin{array}{rrcl} G_1 : & 0 & \longmapsto & 1 \\ & f & \longmapsto & 3 \\ & \sim & \longmapsto & 5 \\ & \vee & \longmapsto & 7 \\ & \Pi & \longmapsto & 9 \\ & (& \longmapsto & 11 \\ &) & \longmapsto & 13 \end{array}$$

Gödel définit G_1 sur les variables de la manière suivante : aux variables de type n (on rappelle qu'il y en a un nombre infini dénombrable) on associe les p_k^n où p_k est le $k^{ième}$ nombre premier après 13. Par exemple $G_1(x_1) = 17$, $G_1(z_1) = 23$ ou encore $G_1(y_3) = 19^3$.

Nous devons maintenant l'étendre aux suites de signes primitifs (même si à terme seule la restriction aux formules nous intéresse) puis aux suites de suites de signes primitifs (pour pouvoir projeter la notion de suite de formules qui est utile pour parler de démonstration). Pour cela utilisons l'unicité de la décomposition en facteurs premiers (les s_i sont des signes primitifs et les f_i des suites de signes primitifs) :

$$s_1 s_2 \dots s_n \longmapsto 2^{G_1(s_1)} 3^{G_1(s_2)} \dots p_n^{G_1(s_n)}$$

$$f_1 f_2 \dots f_n \longmapsto 2^{G_1(f_1)} 3^{G_1(f_2)} \dots p_n^{G_1(f_n)}$$

exemples:
$x_2(x_1) \longmapsto 2^{17^2} 3^{11} 5^{17} 7^{13} (\approx 6,9.10^{33})$
$x_2(x_1),\ x_2 \Pi(x_2(f0)) \longmapsto 2^{2^{17^2} 3^{11} 5^{17} 7^{13}} 3^{2^{17^2} 3^9 5^{11} 7^{17^2} 11^{11} 13^3 17^1 19^{13} 23^{13}}$

On appelle $\mathcal{G}$ l'image des signes primitifs, des formules et des suites finies de formules. Les éléments de $\mathcal{G}$ sont appelés les **nombres de Gödel**. A partir de maintenant, tous les entiers manipulés seront des nombres de Gödel.

On constate que tous les éléments de $\mathcal{G}$ (qui ne sont pas des images de signes primitifs) commencent par 2 dans leur décomposition en facteurs premiers ; ceci ajouté à l'unicité de cette décomposition assure l'injectivité[7] de G_1.

De manière plus constructive : si vous me donnez un nombre de Gödel, je peux retrouver sa formule (ou suite de formules) en le décomposant en facteurs premiers, puis en décomposant chacun des exposants en facteurs premiers puis en décomposant les exposants des nouveaux facteurs.

On a ainsi construit une correspondance bi-univoque entre le système $\mathcal{P}$ et les nombres de Gödel.

[7] cf remarque ci-dessous

Remarque: Quand on a défini G_1 sur les signes primitifs on a utilisé que des nombres impairs. Pourquoi ? Simplement pour que les formules et les suites de formules aient des images différentes ; par exemple si on avait codé « f » par 2 alors 2^2 aurait eu deux antécédants : la suite de suite de signe « 0 » et la suite de signe « f ».

4.5.2 Projection de $\mathcal{P}$ sur $\mathcal{G}$

On redéfinit alors sur $\mathcal{G}$ tous les concepts de $\mathcal{P}$. Ces concepts seront définis par les mêmes mots mais écrits en capitales. Par exemple, on dira que 7 (qui code pour $\vee$) est une CONSTANTE, 19 (qui code pour x_2) est une VARIABLE DE TYPE 2, $G_1(\sim (fx_1 = 0))$ est un AXIOME ... ; de même les analogues de Sub, Neg, et Gen seront notés SUB, NEG, et GEN. Il est important de comprendre que tous ces concepts existent dans $\mathbf{N}$ indépendemment de $\mathcal{P}$: par exemple être une VARIABLE DE TYPE 1 signifie exactement être un nombre premier supérieur ou égal à 17.[8].
De plus réécrivons le théorème du sens ; à ce sujet nous noterons désormais $Z(n)$ le nombre de Gödel de f^n0 ($Z(3) = G_1(fff0) = 2^3 3^3 5^3 7^1 = 189000$).

Théorème du SENS
Pour toute relation récursive R à n variables d'entiers il existe un SIGNE DE RELATION à n places r (avec pour VARIABLES LIBRES $u_1, u_2 \dots u_n$) tel que :

$\forall (x_1, \dots, x_n) \in \boldsymbol{N}^n$:

$$R(x_1, \dots, x_n) \Rightarrow DEM[SUB\, r^{u_1 \dots u_n}_{Z(x_1)\dots Z(x_n)}] \tag{4.1}$$

$$\overline{R(x_1, \dots, x_n)} \Rightarrow DEM[NEG(SUB\, r^{u_1 \dots u_n}_{Z(x_1)\dots Z(x_n)})] \tag{4.2}$$

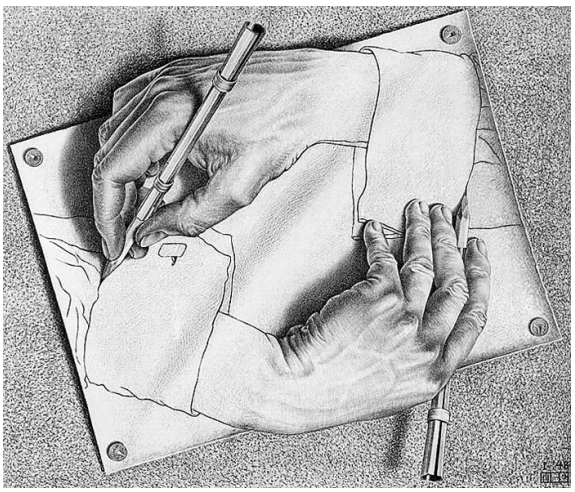


FIG. 4.4 – *Drawing Hands* (Escher 1948)

[8]Pour avoir une idée de la manire dont les autres concepts s'expriment uniquement à l'aide des entiers on peut se référer à 4.7.4 page 73

4.6 La démonstration de Gödel

4.6.1 Système $\mathcal{P}$ étendu et $\omega-$*consistance*

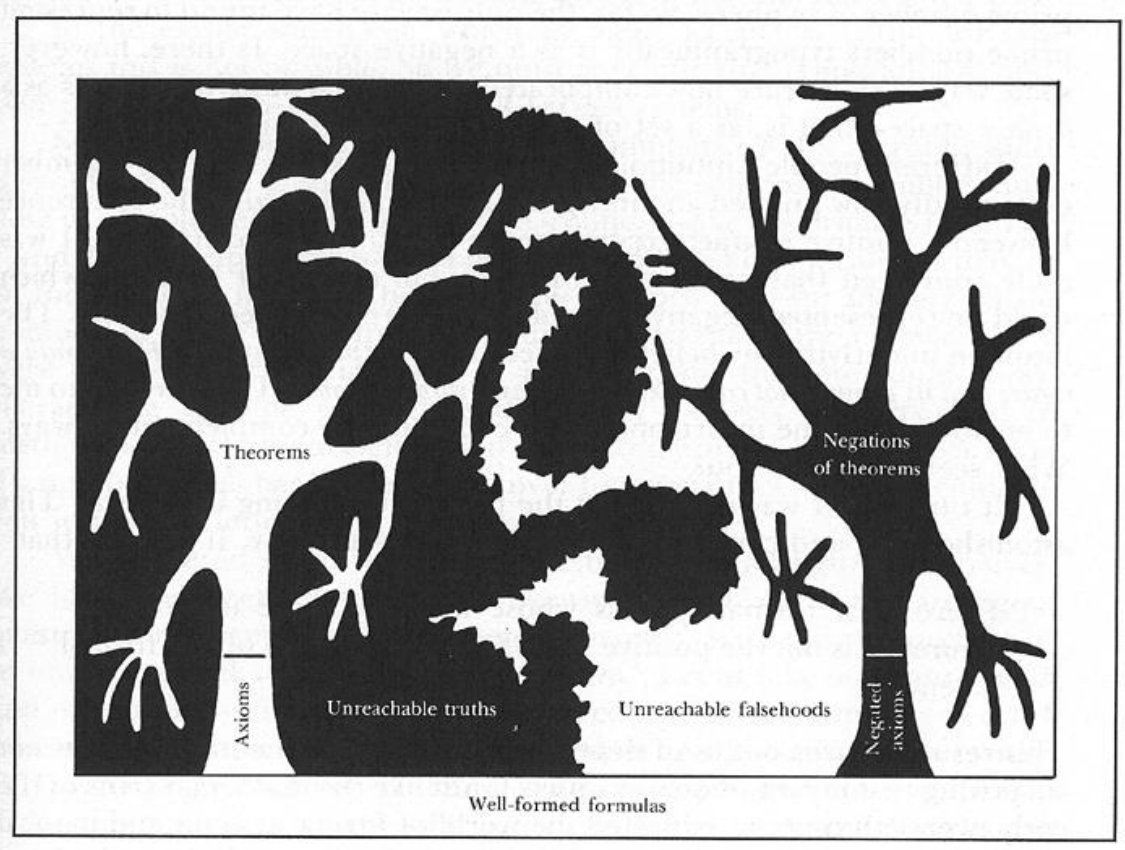
On rappelle que le théorème de Gödel vaut non seulement pour $\mathcal{P}$ mais aussi pour tout système étendu de $\mathcal{P}$. Soit k un ensemble de FORMULES ; on va appeller $Csq(k)$, l'ensemble des FORMULES k-DEMONTRABLES.

Définition 8 *Un ensemble de formules k est dit $\omega-$consistant si et seulement si il n'existe pas de SIGNE DE CLASSE a de VARIABLE LIBRE ν tel que*

$$\forall n\text{:}\ [SUB\ a^{\nu}_{Z(n)} \in Csq(k)]\ \textit{et}\ NEG(\nu\ GEN\ a) \in Csq(k)$$

Cette propriété est plus forte que la consistance. La différence entre les deux notions vient de la remarque suivante : si « $x_1\Pi(a)$ » est démontrable alors d'après l'axiome III.1 (axiome de substitution) « $\forall n \in \mathbf{N}$: $[SUB\ a^{x_1}_{Z(n)}$ est démontrable] » mais comme on le verra plus loin la réciproque n'est pas vraie.

Intuitivement, ce n'est pas parce qu'on a une démonstration de « $P(n)$ » pour chaque entier n (c'est à dire une infinité de démonstrations) que l'on a une démonstration de « $\forall n$: $P(n)$ »[9].



[9]introduire une régle d'inférence pour éliminer cette distinction rendrait le sytème $\mathcal{P}$ contradictoire (car le théorème de Gödel serait faux)

4.6.2 Le théorème de Gödel

Premier théorème d'incomplétude de Gödel(1931)
Pour toute classe ω-consistante et récurive k de $FORMULES$, il existe des $SIGNES\ DE\ CLASSE$ récursifs r tels ni $\nu GENr$ ni $NEG(\nu GENr)$ n'appartiennent à $CSQ(k)$. (ν désigant la $VARIABLE\ LIBRE$ de r)

Démonstration

Supposons k ω-consistant.
L'idée de la démonstration est la suivante : nous allons à l'aide du théorème du SENS exhiber un SIGNE DE CLASSE qui dira, par un processus d'autoréférence, qu'il n'est pas démontrable (en fait c'est un peu plus compliqué).

Soit Q la relation définie sur $\mathbf{N} \times \mathbf{N}$ par

$$Q(x,y) \Leftrightarrow \overline{xDEM_k(SUB\ y^{19}_{Z(y)})}.$$

Supposons Q récursive[10] (ce point sera démontré ultérieurement). On peut alors lui appliquer le théorème du SENS.
Ainsi il existe un SIGNE DE RELATION à 2 PLACES p (avec par exemple pour VARIABLES LIBRES 17 et 17^2) vérifiant :

$\forall (x,y) \in \mathbf{N}^2$:

$$Q(x,y) \ \Rightarrow DEM[SUB\, p^{17,19}_{Z(x),Z(y)}] \tag{4.3}$$

$$\overline{Q(x,y)} \ \Rightarrow DEM[NEG(SUB\, p^{17,19}_{Z(x),Z(y)})] \tag{4.4}$$

Soient :

- $n = 17GENp$
- $q = SUB\ p^{19}_{Z(n)}$
- $r = 17GENq = SUB\ n^{19}_{Z(n)}$ cf note de bas de page[11]

Nous allons montrer que ni r ni $NEG(r)$ ne sont k-DEMONTRABLES.

[10] Gödel démontre également que toute fonction récursive est arithmétique ce qui signifie que le concept indécidable que l'on va construire s'exprime uniquement à l'aide des concepts de la logique classique ($\vee, \sim, \exists \ldots$) et des concepts $=$,$+$ (addition) et . multiplication.

[11] cette égalité se justifie simplement par le fait que la GENERALISATION par rapport à une variable et la SUBSTITUTION d'un signe à une *autre* variable sont des opérations qui commutent sur l'ensemble des formules.

r n'est pas k-DEMONTRABLE :

Si r était k-démontrable comme $r = SUB\ n^{19}_{Z(n)}$ on aurait un x_0 tel que $\overline{Q(x_0, n)}$.

Donc d'après 4.4,

$$DEM[NEG(SUB\, p^{17,19}_{Z(x_0),Z(n)})]$$

donc

$$DEM_k[NEG(SUB\, q^{17}_{Z(x_0)})]^{12}$$

Or ceci contredit la consistance (et donc l'ω-consistance) de k car comme $r = 17GENq$ est k-DEMONTRABLE, l'AXIOME DE SUBSTITUTION nous permet de dire que $SUB\, q^{17}_{Z(x_0)}$ est k-DEMONTRABLE.
Donc r n'est pas k-DEMONTRABLE.

$NEG(r)$ n'est pas k-DEMONTRABLE :

Comme on vient de le voir r n'est pas k-DEMONTRABLE. Donc comme $r = SUB\ n^{19}_{Z(n)}$:

$$\forall x \in \mathbf{N} : Q(x, n)$$

Donc d'après 4.3 on a que $\forall x$**:** $DEM_k[NEG(SUB\, q^{17}_{Z(x_0)})]$ ce qui avec l'ω-consistance montre que $r = 17GENq$ n'est pas k-DEMONTRABLE.

■

Remarque:
On peut reprendre le schéma de cette démonstration en prenant $Q(y) = DEM[SUB\, y^{19}_{Z(y)}]$ et en supposant que le relation $y \mapsto DEM$ ($\equiv$ être DEMONTRABLE) est récursive... et on arrive a une contradiction. Donc $y \mapsto DEM\, y$ n'est pas récursive.

[12] en effet être DEMONTRABLE implique être k-DEMONTRABLE

4.7 Les fonctions récursives

Le but de cette section est définir les fonctions récursives, de montrer que la relation utilisée dans la démonstration du théorème de Gödel ($\equiv Q(x, y)$) est récursive et enfin de démontrer le théorème du sens.
Toutes les fonctions considérées sont des fonctions arithmétiques c'est à dire qu'elles sont définies sur $\mathbf{N}^n$ à valeur dans $\mathbf{N}$. On appelera $\mathcal{F}_n$ l'ensemble des fonctions arithmétiques à n variables. On supposera de plus $\mathcal{F}_n \subset \mathcal{F}_{n+1}$.

4.7.1 Définitions

Définition 9 (Fonctions récursivement définies) *Soient $\phi \in F_n, \psi \in F_{n-1}, \mu \in F_{n+1}$*[13].
On dira que ϕ est récursivement définie à partir de μ et ψ si
$\forall (k, x_2, \ldots, x_n) \in \boldsymbol{N}^n$*:*

$$\begin{aligned} \phi(0, x_2, \ldots, x_n) &= \mu(x_2, \ldots, x_n) \\ \phi(k+1, x_2, \ldots, x_n) &= \psi(k, \phi(k, x_2, \ldots, x_n), x_2, \ldots, x_n) \end{aligned}$$

Définition 10 *Une fonction ϕ sera dite récursive si il existe une suite $\phi_1, \ldots, \phi_n$ de fonctions vérifiant les propriétés suivantes :*

- $\phi_n = \phi$
- $\forall i$*:* ϕ_i *est*
  - *(a) une fonction constante ou*
  - *(b) une fonction qui ajoute 1 à une de ses variables ou*
  - *(c) récursivement définies à partir de deux ϕ_k antérieures ou*
  - *(d) obtenue à partir de deux ϕ_k antérieures par substitution d'une des fonctions à une variable de l'autre de l'autre fonction.*

On appelera degré de ϕ la taille minimale d'une telle suite.

Définition 11 *Une relation R entre n entiers naturels est dite récursive si il existe une fonction récursive ϕ dans $\mathcal{F}_n$ telle que :*

$$\forall (x_1, \ldots, x_n) \in \boldsymbol{N}^n\text{: } R(x_1, \ldots, x_n) \Leftrightarrow \phi(x_1, \ldots, x_n) = 0$$

exemples:

- $(x_1, x_2) \mapsto x_1 + 1$ (a)
- $(x_1, x_2) \mapsto 35$ (b)
- $Id : x_1 \mapsto x_1$ (c)
- $(x_1, x_2) \mapsto x_1 + x_2$ (récursivement définie à partir de Id et de $(x_1, x_2) \mapsto x_1 + 1$)

[13] certaines variables peuvent être muettes (notemment x_1 ou x_2 dans ψ) ; on n'écrira pas de telles variables ce qui explique que ψ n'aura pas toujours une variable de plus que ϕ.

4.7.2 Comment construire des fonctions (relations) récursives ?

4.7.2.1 Par substitution et définition récursive

I/**Corrollaire immédiat de la définition :**
Toute fonction (relation) obtenue à partir d'une fonction (relation) récursive par substitution d'une variable par une fonction récursive est récursive ; de même si une fonction est récursivement définie par deux fonctions récursives alors elle est récursive.

exemples:

- $(x_1, x_2) \mapsto x_1.x_2$
- $(x_1, x_2, x_3) \mapsto x_1^{x_2}$
- $(x_1, x_2, x_3, x_4) \mapsto x_3^{x_2} + x_1.(x_3 + 2) + 7$

4.7.2.2 Avec les opérateurs logiques

II/**Théorème :**
Si R et S sont récursives alors $\overline{R}$, $R \vee S$ (et donc R&S) sont récursives. On en déduit notemment que si ψ_1 et ψ_2 sont récursives, la fonction suivante l'est aussi :

$$(x_1, \ldots, x_n) \quad \mapsto \quad \begin{array}{l} \psi_1(x_1, \ldots, x_n) \; si \; R \\ \psi_2(x_1, \ldots, x_n) \; sinon \end{array}$$

Démonstration

Par abus on notera c_k toutes les fonctions constantes égales à k quelque soit le nombre de variables.
Soient α, β les indicatrices respectives des ensembles suivants :

$$\{0\} \; , \; \mathbf{R}^* \times \mathbf{R}^*$$

α et β sont récursives :
$\alpha(0) = c_1()$
$\alpha(k+1) = c_0(k)$

$\beta(0, x) = c_0(x)$
$\beta(k+1, x) = \alpha(x)$

Les relations $R \vee S$ et $\bar{R}$ se déduisent directement de R, S et de ces deux fonctions (regarder la définition).

La seconde partie du théorème se montre en remarquant que la fonction recherchée est égale à $(\alpha \circ \psi).\psi_1 + (\alpha \circ \alpha \circ \psi).\psi_2$ où ψ est une fonction arithmétique telle que $R(x_1, \ldots, x_n) \Leftrightarrow \psi(x_1, \ldots, x_n) = 0$.

■

On notera en gras les variables de n-uplets (quelque soit n).

III/**Théorème :**
Si les fonctions ϕ et ψ sont récursives alors la relation $\phi(\boldsymbol{r}) = \psi(\boldsymbol{n})$ est récursive.

Démonstration

Soit γ la fonction indicatrice de $\{(x,y)/x \neq y\}$.

On commence par construire une fonction $x \mapsto x-1$ appelée r_{-1} :
$r_{-1}(0) = 0$
$r_{-1}(k+1) = k$ on pourrait écrire $r_{-1}(0) = c_0()$ et $r_{-1}(k+1) = Id(k)$ pour vraiment coller à la définition

Ensuite, on déduit la récursivité de γ ainsi :

$$\begin{array}{rll} \gamma(0,x) = & \alpha(\alpha(x)) & (\alpha \circ \alpha \text{ est la fonction indicatrice de } \mathbf{R}^*) \\ \gamma(k+1,x) = & c_1(x) & si\ Id(x) = 0 \\ = & \gamma(k, r_1(x))) & sinon \end{array}$$

$\phi(\mathbf{r}) = \psi(\mathbf{n}) \Leftrightarrow \gamma(x,y) = 0$
D'où le résultat...

■

4.7.2.3 Avec les quantificateurs et la fonction minimum

IV/**Théorème :**
Si la fonction $\boldsymbol{r} \mapsto \phi(\boldsymbol{r})$ et la relation $(x, \boldsymbol{n}) \mapsto R(x, \boldsymbol{n})$ sont récursives alors les deux relations et la fonction suivantes le sont aussi :

$$S(\boldsymbol{r}, \boldsymbol{n}) \Leftrightarrow \exists x \leq \phi(\boldsymbol{r})/\ R(x, \boldsymbol{n})$$

$$T(\boldsymbol{r}, \boldsymbol{n}) \Leftrightarrow \forall x \leq \phi(\boldsymbol{r}):\ R(x, \boldsymbol{n})$$

$$\psi : (\boldsymbol{r}, \boldsymbol{n}) \mapsto min\{x \leq \phi(\boldsymbol{r})/\ R(x, \boldsymbol{n})\}^{14}$$

Démonstration

Soit θ définie de la manière suivante :

$$\begin{array}{rll} \theta(0, \mathbf{n}) & = c_0(\mathbf{n}) & \\ \theta(k+1, \mathbf{n}) & = \theta(k, \mathbf{n}) & si\ \overline{R(k+1, \mathbf{n})}\ ou\ \theta(k, \mathbf{n}) \neq 0 \\ & = k & sinon \end{array}$$

Ainsi θ (en tant que fonction de k) vaut 0 jusqu'à ce qu'au premier k_0 tel que $R(k_0, \ldots, \mathbf{n})$ puis vaut k_0 après. Elle est récursive d'après II/.
Il suffit alors de prendre ψ et S ainsi :

$$\psi(\mathbf{r}, \mathbf{n}) = \theta(\phi(\mathbf{r}), \mathbf{n})$$

[14] si l'ensemble est vide on prend 0 (et non pas $+\infty$) pour la valeur du minimum

$$S(\mathbf{r}, \mathbf{n}) = R(\psi(\mathbf{r}, \mathbf{n}), \mathbf{n})$$

T s'obtient de la même façon que S mais en considérant $\overline{R}$ à la place de R.

■

4.7.3 Q est récursive

Comment construire des fonctions récursives ?

I/ *Toute fonction (relation) obtenue à partir d'une fonction (relation) récursive par substitution d'une variable par une fonction récursive est récursive ; de même si une fonction est récursivement définie par deux fonctions récursives alors elle est récursive.*

II/ *Si R et S sont récursives alors $\overline{R}$, $R \vee S$ (et donc $R\&S$) sont récursives. On en déduit notemment que si ψ_1 et ψ_2 sont récursives, la fonction suivante l'est aussi :*

$$(x_1, \ldots, x_n) \mapsto \begin{array}{l} \psi_1(x_1, \ldots, x_n) \text{ si } R \\ \psi_2(x_1, \ldots, x_n) \text{ sinon} \end{array}$$

III/ *Si les fonctions ϕ et ψ sont récursives alors la relation $\phi(\boldsymbol{r}) = \psi(\boldsymbol{n})$ est récursive.*

IV/ *Si la fonction $\boldsymbol{r} \mapsto \phi(\boldsymbol{r})$ et la relation $(x, \boldsymbol{n}) \mapsto R(x, \boldsymbol{n})$ sont récursives alors les deux relations et la fonction suivantes le sont aussi :*

$$S(\boldsymbol{r}, \boldsymbol{n}) \Leftrightarrow \exists x \leq \phi(\boldsymbol{r})/\ R(x, \boldsymbol{n})$$

$$T(\boldsymbol{r}, \boldsymbol{n}) \Leftrightarrow \forall x \leq \phi(\boldsymbol{r}) \boldsymbol{:}\ \ R(x, \boldsymbol{n})$$

$$\psi : (\boldsymbol{r}, \boldsymbol{n}) \mapsto min\{x \leq \phi(\boldsymbol{r})/\ R(x, \boldsymbol{n})\}^{15}$$

Pour montrer que Q[16] est récursive il nous suffit désormais de montrer que $(x, y) \mapsto xDEM_k y$, SUB et Z[17] sont récursives.
Cela prend 45 étapes. Nous allons en effet définir successivement 45 concepts du SYSTEME $\mathcal{P}$; il sera évident à l'aide du théorème précédent que chacun d'entre eux est récursif et le quarante-cinquième sera $(x, y) \mapsto xDEM_k y$.
Vous remarquerez que dans la définition de certains de ces concepts apparaissent des bornes supérieurs qui semblent superflus (pour la définition) après les quantificateurs existenciels ; elles servent juste à montrer que le concept en question est récursif.

[15] si l'ensemble est vide on prend 0 (et non pas $+\infty$) pour la valeur du minimum
[16] $Q(x, y) \Leftrightarrow \overline{xDEM_k(SUB\ y^{19}_{Z(y)})}$
[17] $Z(n) = G_1(\underbrace{f \ldots f}_{n\ fois})0$

4.7.4 Les 45 concepts récursifs de Gödel

1. $x/y \equiv \exists z \leq x \big/\ x = y.z$
   x est divisible par y.

2. $Prim(x) \equiv x > 1$ **et** [$\nexists z \leq x \big/\ (z \neq 1$ **et** $z \neq x$ **et** $x/z)$]
   x est un nombre premier.

3. $0\ Pr\ x \equiv 0$
   $(n+1)\ Pr\ x \equiv min\{y \leq x \big/\ Prim(y)$ **et** x/y **et** $y > n\ Pr\ x\}$
   $n\ Pr\ x$ est le $n^{\text{ième}}$ nombre premier (par ordre croissant) divisant x.[18]

4. $0! \equiv 1$
   $(n+1)! \equiv (n+1).n!$

5. $Pr(0) \equiv 0$
   $Pr(n+1) \equiv min\{y \leq [Pr(n)]! + 1 \big/\ Prim(y)$ **et** $y > Pr(n)\}$
   $Pr(n)$ est le $n^{\text{ième}}$ nombre premier par ordre de grandeur croissant.

6. $n\ Tr\ x \equiv min\{y \leq x \big/\ x/(n\ Pr\ x)^y$ **et** $\overline{x/(n\ Pr\ x)^{y+1}}\}$
   $n\ Tr\ x$ est le $n^{\text{ième}}$ exposant dans la suite (croissante) des facteurs premiers de x c'est à dire le $n^{\text{ième}}$ terme de la suite de nombre associée à x.

7. $l(x) \equiv min\{y \leq x \big/\ y\ Pr\ x > 0$ **et** $(y+1)Pr\ x = 0\}$
   $l(x)$ est le nombre d'entiers premiers qui divisent x c'est à dire la longueur de la suite de nombres associée à x.

8. $x * y \equiv min\{z \leq Pr(l(x) + l(z))^{x+y} \big/\ [\forall n \leq l(x),\ n \neq 0$**:** $n\ Tr\ z = n\ Tr\ x]$ **et** $[\forall n \leq l(y),\ n \neq 0$**:** $(n + l(x))Tr\ z = n\ Tr\ y)\}$
   $x * y$ correspond à la concaténation des deux suites finies de nombres associées à x et y.

9. $R(x) \equiv 2^x$
   $R(x)$ correspond à la suite de nombres qui consiste en x tout seul.

10. $E(x) \equiv R(11) * x * R(13)$
    E correspond à l'opération de mettre entre paranthèses (11 et 13 sont les nombres Gödel de (et)).

11. $n\ VAR\ x \equiv n \neq 0$ **et** $\exists z, 13 < z \leq x \big/\ Prim(z)$ **et** $x = z^n$
    x est une VARIABLE DE TYPE n.

12. $VAR(x) \equiv \exists n \leq x \big/\ n\ VAR\ x$
    x est une VARIABLE.

13. $NEG(x) \equiv R(5) * E(x)$
    $NEG(x)$ est la NEGATION de x.

14. $x\ DIS\ y \equiv E(x) * R(7) * E(y)$
    $x\ DIS\ y$ est la DISJONCTION de x et y.

[18] pour n plus grand que le nombre de facteurs de x on trouve 0

15. $x\ GEN\ y \equiv R(x) * R(7) * E(y)$
$x\ GEN\ y$ est la GENERALISATION de y par rapport à x.

16. $0\ N\ x \equiv x$
$(n+1)N\ x \equiv R(3) * (n\ N\ x)$
$n\ N\ x$ correspond à l'action de placer n fois le signe f devant ce que représente x.

17. $Z(n) \equiv n\ N\ R(1)$
$Z(n)$ est le nombre de Gödel de $\underbrace{f \ldots f}_{n\ fois} 0$.

18. $Typ'_1(x) \equiv \exists m, n \leq x \Big/ (m = 1$ **ou** $1\ VAR\ m)$ **et** $(x = n\ N[R(m)])$
x est un SIGNE DE TYPE 1.

19. $Typ_n(x) \equiv [n = 1$ **et** $Typ'_1(x)]$ **ou** $[n > 1$ **et** $\exists v \leq x \Big/ n\ VAR\ v$ **et** $x = R(v)]$
x est un SIGNE DE TYPE n.

20. $Elf(x) \equiv \exists y, z, n \leq x \Big/ Typ_n(y)$ **et** $Typ_{n+1}(z)$ **et** $x = z * E(y)$
x est une FORMULE ELEMENTAIRE.

21. $Op(x, y, z) \equiv (x = NEG(y))$ **ou** $(x = y\ DIS\ z)$ **ou** $(\exists v \leq x \Big/ VAR(v)$ **et** $x = v\ GEN\ y)$
x s'obtient à partir de y par NEGATION ou GENERALISATION ou à partir de y et z par CONJONCTION.

22. $FR(x) \equiv l(x) > 0$ **et** $\forall n \leq l(x), n \neq 0$**:** $[Elf(n\ Tr\ x)]$ **ou** $[\exists p, q < n, \neq 0 \Big/$
$Op(n\ Tr\ x, p\ Tr\ x, q\ Tr\ x)]$
x est une SUITE DE FORMULES, dont chacune est une FORMULE ELEMENTAIRE ou bien résulte des précédentes par le procédé Op.

23. $Form(x) \equiv \exists n \leq (Pr([l(x)]^2))^{x.[l(x)]^2} \Big/ FR(n)$ **et** $x = l(n)Tr\ n$
x est une FORMULE c'est à dire, le dernier terme d'une SUITE DE FORMULES n. [19]

24. $v\ Lie\ n, x \equiv VAR(v)$ **et** $Form(x)$ **et** $\exists a, b, c \leq x \Big/ l(a) + 1 \leq n \leq l(a) + l(v\ GEN\ b)$
et $x = a * (v\ GEN\ b) * c$ **et** $Form(b)$
La VARIABLE v est LIEE en x à la $n^{\text{ième}}$ place.

25. $v\ Lib\ n, x \equiv n \leq l(x)$ **et** $VAR(v)$ **et** $Form(x)$ **et** $v = n\ Tr\ x$ **et** $\overline{v\ Lie\ n, x}$
La VARIABLE v est LIBRE en x à la $n^{\text{ième}}$ place.

26. $v\ Lib\ x \equiv \exists n \leq x \Big/ v\ Lib\ n, x$
v est une VARIABLE LIBRE dans x.

27. $Su\ x^n_y \equiv min\{z \leq [Pr(l(x) + l(y))]^{x+y} \Big/ \exists u, v \leq x \Big/ n = l(u) + 1$ **et** $x = u * R(n\ Tr\ x) * v$ **et** $z = u * y * v\}$
$Su\ x^n_y$ est la formule résultant de x après substitution de y au $n^{\text{ième}}$ terme de x (si $0 < n \leq l(x)$).

[19] Justifions que $n \leq (Pr([l(x)]^2))^{x.[l(x)]^2}$ est une borne acceptable : la longueur du n minimal est bornée par le nombre de SOUS-FORMULES de x ; or il y a au plus $l(x) - k$ SOUS-FORMULES de longueur k ($\forall k \leq l(x)$) et donc au plus $\frac{l(x).l(x)+1}{2} \leq l(x)^2$ SOUS-FORMULES de x ; dès lors on compte au plus $l(x)^2$ nombre premiers divisant n ; ces nombres premiers sont de plus inférieurs à $Pr(l(x)^2)$ et leur exposant vaut au plus x d'où la majoration annoncée.

28. $0\ St\ v,x \equiv min\{n \leq l(x)\big/\ v\ Lib\ n,x$ **et** $\nexists p;\ n < p \leq l(x)\big/\ v\ Lib\ p,x\}$
$(k+1)St\ v,x \equiv min\{n < k\ St\ v,x$ **et** $v\ Lib\ n,x$ **et** $\nexists p;\ n < p < k\ St\ v,x\big/\ v\ Lib\ p,x\}$
$k\ St\ v,x$ est la $(k+1)^{\text{ième}}$ place dans x (à partir de la droite de la FORMULE) où v est LIBRE; si une telle place n'existe pas $k\ St\ v,x = 0$.

29. $A(v,x) \equiv min\{n \leq l(x)\big/\ n\ St\ v,x = 0\}$
$A(v,x)$ est le nombre de places où v est LIBRE dans x.

30. $SUB_0 x^v_y \equiv x$
$SUB_{k+1} x^v_y \equiv Su(SUB_k x^v_y)^{k\ St\ v,x}_y$
$SUB_k x^v_y$ est la formule obtenue à partir de x où on a substitué y à v au niveau de ses k premières (à partir de la droite) OCCURENCES LIBRES.

31. $SUB\ x^v_y \equiv SUB_{A(v,x)} x^v_y$
enfin... le concept SUB (qui est égal à l'identité si x n'est pas une FORMULE ou si v n'est pas une VARIABLE)

32. $c\ IMP\ y \equiv [NEG(x)]DIS\ y$
$x\ CON\ y \equiv NEG[\ NEG(x)\ DIS\ NEG(y)\ ]$
$x\ EQU\ i \equiv (x\ IMP\ y)CON(y\ IMP\ x)$
$v\ EX\ y \equiv NEG(v\ GEN[NEG(y)])$
Il s'agit des concepts IMPLIQUE, CONJONCTION, EQUIVAUT et IL EXISTE.

33. $n\ Th\ x \equiv min\{y \leq x^{(x^n)}\big/\ \forall k \leq l(x)$**:** $[k\ Tr\ x \leq 13$ **et** $k\ Tr\ y = k\ Tr\ x]$ **ou** $[k\ Tr\ x > 13$ **et** $k\ Tr\ y = (k\ Tr\ x).(1\ Pr\ (k\ Tr\ x))^n]$
$n\ Th\ x$ est la $N^{\text{ième}}$ ELEVATION DE TYPE de x (si x et $n\ Th\ x$ sont des formules)

Soient z_1, z_2 et z_3 les nombres de Gödel respectifs des trois Axiomes de Peano (I.1,2,3).

34. $Z-Ax(x) \equiv (x = z_1$ **ou** $x = z_2$ **ou** $x = z_3)$
x est un AXIOME DE PEANO.

35. $A_1-Ax(x) \equiv \exists y \leq x\big/\ Form(y)$ **et** $x = (y\ DIS\ y)IMP\ y$
x est une FORMULE qui résulte du schéma d'axiome II.1. On définit de manière analogue $A_2-Ax(x)$ $A_3-Ax(x)$ et $A_4-Ax(x)$ pour les schémas axiomes II.2,3,4.

36. $A-Ax(x) \equiv A_1-Ax(x)$ **ou** $A_2-Ax(x)$ **ou** $A_3-Ax(x)$ **ou** $A_4-Ax(x)$
x est un AXIOME DE LA LOGIQUE PROPOSITIONNELLE.

37. $Q(z,y,v) \equiv \nexists n \leq l(y), m \leq l(z), w \leq z\big/\ w = m\ Tr\ z$ **et** $w\ Lie\ n,y$ **et** $v\ Lib\ n,y$
z ne contient aucune VARIABLE LIEE EN y à une place où v est LIBRE.

38. $L_1-Ax(x) \equiv \exists v,y,z,n \leq x\big/\ n\ VAR\ v$ **et** $Typ_n(z)$ **et** $Form(y)$ **et** $Q(z,y,v)$
et $x = (v\ GEN\ y)IMP(SUB\ y^v_z)$
x est une FORMULE qui résulte du schéma d'axiomes III.1.

39. $L_2-Ax(x) \equiv \exists v,q,p \leq x\big/\ VAR(v)$ **et** $Form(p)$ **et** $\overline{v\ Lib\ p}$ **et** $Form(q)$
et $x = [v\ GEN\ (p\ DIS\ q)IMP[p\ DIS(v\ GEN\ q)]$
x est une FORMULE qui résulte du schéma d'axiomes III.2.

40. $R-Ax(x) \equiv \exists u,v,y,n \leq x\big/\ n\ VAR\ v$ **et** $(n+1)VAR\ u$ **et** $u\ Lib\ y$ **et** $Form(y)$ **et** $x = u\ Ex\ [v\ GEN([R(u) * E(R(v))]\ EQU\ y)]$
x est une FORMULE qui résulte du schéma d'axiomes IV.1.

Soit z_4 le nombre de Gödel du premier axiome IV.2 [20].

41. $M{-}Ax(x) \equiv \exists n \leq x \Big/ \; n \; Th \; z_4$
x est une FORMULE qui résulte du schéma d'axiomes IV.2.

42. $Ax(x) \equiv Z{-}Ax(x)$ **ou** $A{-}Ax(x)$ **ou** $L_1{-}Ax(x)$ **ou** $L_2{-}Ax(x)$ **ou** $R{-}Ax(x)$ **ou** $M{-}Ax(x)$
x est un AXIOME.

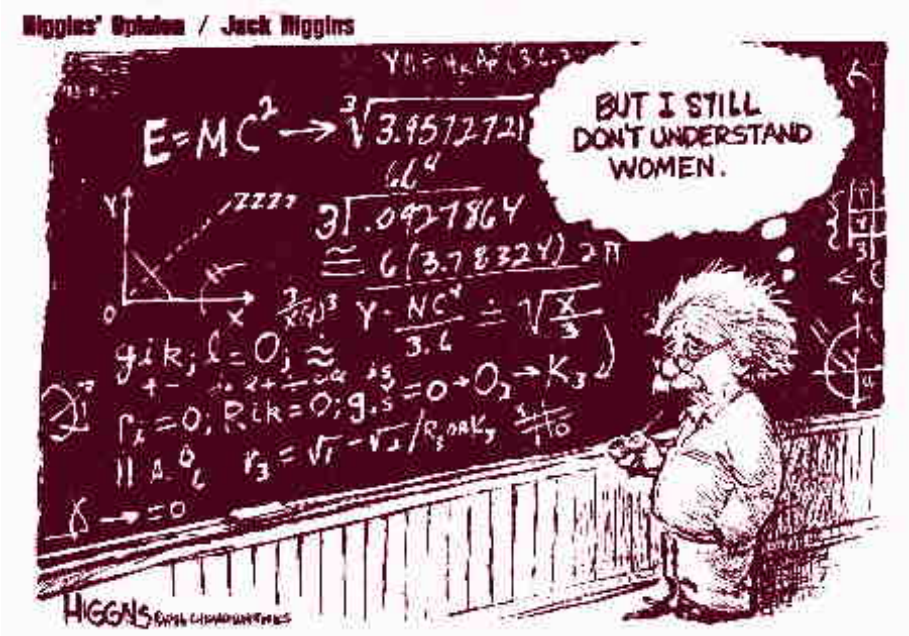
43. $Cs(x,y,z) \equiv y = z \; IMP \; x$ **ou** $\exists v \leq x \Big/ \; VAR(v)$ **et** $x = v \; GEN \; y$
x est une CONCEQUENCE IMMEDIATE de y et z.

44. $Dm(x) \equiv l(x) > 0$ **et** $\forall n \leq l(x), n \neq 0$**:** $Ax(n \; Tr \; x)$ **ou** $[\exists p,q; 0 < p,q < n \Big/$
$Cs(n \; Tr \; x, p \; Tr \; x, q \; Tr \; x)]$
x est une FIGURE DE DEMONSTRATION c'est à dire une suite finie de FORMULES dont chacune est soit un AXIOME soit une CONCEQUENCE IMMEDIATE de deux FORMULES PRECEDENTES.

45. $x \; DEM \; y \equiv Dm(x)$ **et** $[l(x)]Tr \; x = y$
x DEMONTRE y.

bonus $Dem(x) \equiv \exists y \Big/ \; y \; DEM \; x$
x est une FORMULE DEMONTRABLE. Attention, comme il n'y a pas de borne associée au quantificateur existenciel rien ne permet d'affirmer que ce concept est récursif. D'ailleurs, comme on l'a déjà remarqué sa récursivité est incompatible avec la consistance du système $\mathcal{P}$ (cf remarque en fin de 4.6.2 page 67) .

On peut également définir un concept Dm_k puis DEM_k en rajoutant la possibilité d'appartenir à k dans la définition du concept Dm_k ; ces concepts seront récursifs si k est récursif (i.e $x \in k$ est une relation récursive).



[20] $x_1 \Pi(x_2(x_1) \equiv y_2(x_1)) \supset x_2 = y_2$

4.7.5 Démonstration du théorème du sens

Théorème du sens
(Théorème V dans l'article de Gödel)
Pour toute relation récursive R à n variables d'entiers il existe un signe de relation à n places r (avec pour variables libres $x_1, y_1 \ldots \nu_1$) tel que :

$\forall(m_1, \ldots, m_n) \in \boldsymbol{N}^n$:

$$R(m_1, \ldots, m_n) \Rightarrow Dem[Sub\, r^{x_1 \ldots \nu_1}_{f^{m_1}0 \ldots f^{m_n}0}] \tag{4.5}$$

$$\overline{R(m_1, \ldots, m_n)} \Rightarrow Dem[\sim (Sub\, r^{x_1 \ldots \nu_1}_{f^{m_1}0 \ldots f^{m_n}0})] \tag{4.6}$$

Démonstration

Nous allons démontrer le théorème pour toute les relations R de la forme $x_0 = \psi(x_1, \ldots, x_n)$ avec ψ récursive. Il sera alors valable pour toutes les relations récursives Q.
En effet, soit Q récursive et ψ la fonction récursive associée ; alors :

$$Q(x_1, \ldots, x_n) \Leftrightarrow R(0, x_1, \ldots, x_n)$$

où R est définie par

$$R(x_0, \ldots, x_n) \Leftrightarrow x_0 = \psi(x_1, \ldots, x_n).$$

Or si le théorème est vrai pour R, il existe r vérifiant 4.5 et 4.6 ; et alors $Sub\ r^{x_1}_0$ convient car il vérifie 4.5 et 4.6 pour Q.

Soit donc R définie par $x_0 = \psi(\textit{certaines variables})$ avec ψ récursive. Nous allons démontrer le théorème par récurrence sur le degré de ϕ. [21]

Si ϕ est de degré un (c'est à dire une fonction constante n ou une fonction $+1$: par exemple $x_1 \mapsto x_1 + 1$) alors l'un des deux signes de relations à n places suivant convient :

$$(x_0 = f^n 0).(x_1 = x_1).(x_2 = x_2) \ldots (x_n = x_n)$$

$$(x_0 = f x_1).(x_2 = x_2) \ldots (x_n = x_n)^{22}$$

Si ϕ est de degré $m > 1$ alors elle résulte de deux fonctions récursives μ et ψ de degré inférieurs par substitution ou définition récursive.

[21] Nous prendrons quelque libertés avec les notations très strictes du systme $\mathcal{P}$; en effet pour simplifier nous noterons les variables de type 1 par des minuscules $(x_1, y, z_n \ldots)$ et les variables de type 4 (notemment les ensembles d'ensembles de couples) par des capitales $(A, B \ldots)$. Nous veillerons bien entendu à ce que chaque minuscule (en tant que signe primitif) coincide avec la variable d'entier qu'elle est censée représenter.

[22] les égalités triviales ont été rajoutées pour que les nombres de variables de la fonction récursive et du signe de relation soient égaux ; pour les deux signes de relations qui suivent on ne les a pas écrit pour simplifier la discussion

Premier cas : $\phi = \psi(\mu(y_1, \ldots, y_{n_1}), \ldots, x_{n_2})$ [23]

Soit r un signe de relation à n_1 places associé à $x_0 = \psi(x_1, \ldots, x_{n_1})$ (hypothèse d'induction).
Soit s un signe de relation à n_2 associé à $y_0 = \mu(y_1, \ldots, y_{n_2})$ (hypothèse d'induction).
Exhibons un signe de relation à $n_1 + n_2$ places associé à $x_0 = \psi(\mu(y_1, \ldots,$
$y_{n_1}), \ldots, x_{n_2})$. Le signe suivant convient :

$$x\Pi(SUB\ s_x^{y_0} \supset SUB\ r_x^{x_1})$$

On déduit des procédés habituels de démonstration (ceux qu'un Mathématicien utilisent tous les jours et qui ont été formalisés dans les Principia Mathematica) qu'il vérifie bien 4.5 et 4.6 pour R (en fait il suffit de comprendre que ce signe de relation signifie $\phi = x_0$).

Second cas : définition récursive

$$\phi(0, x_2, \ldots, x_n) = \mu(x_2, \ldots, x_n)$$

$$\phi(k+1, x_2, \ldots, x_n) = \psi(k, \phi(k, x_2, \ldots, x_n), x_2, \ldots, x_n)$$

Soit r un signe de relation à $n+1$ places associé à $x_1 = \psi(k, l, x_2 \ldots, x_n)$ (hypothèse d'induction).
Soit s un signe de relation à n_2 associé à $x_1 = \mu(x_2, \ldots, x_n)$ (hypothèse d'induction).
Exhibons un signe de relation à n places associé à $x_0 = \psi(k, x_2, \ldots, x_n)$. Le signe suivant convient :[24]

$(E\ A)(\ (E\ k_0)(\ A(k_0, x_0).$
$[\ x\Pi(\ x(A) \equiv (SUB\ s_x^{x_1} \vee (E\ y, z)(A(y, z).x = SUB\ r_{y,z}^{k,l}))\ )\ ]\ )\ )$

On déduit des procédés habituels de démonstration qu'il vérifie bien 4.5 et 4.6 pour R.

La philosophie de cette démonstration est que les procédés de substitution et de définition récursive s'exprime (et se démontre le cas échéant) dans le système $\mathcal{P}$. Selon les propres termes de Gödel : « *Ce théorème, bien sûr est une concéquence du fait que dans le cas d'une relation récursive R, on peut décider pour tout n-uplé de nombres, et sur la base des axiomes du système $\mathcal{P}$, si la relation R vaut ou non.* »

■

[23] On ne présente ici qu'un cas particulier de substitution . En effet, un autre exemple de substitution serait $\phi(x_1, \ldots, x_n, y_1, \ldots, y_n) = \psi(y_3, x_n, \mu(x_3, y_n, \ldots, x_1), \ldots, x_n)$. Cependant cette démonstration ne prétend ni à la rigueur ni à l'exhaustivité : une étude complète prendrait une dizaine de pages et serait complètement inintéréssante ; « on comprend bien » que les signes de classes pour les autres méthodes de substitutions sont complètement analogues à celui proposé.

[24] (a, b) est une abréviation pour le couple (a, b) ; de même $A(a, b)$ est une abréviation pour « le couple (a, b) est dans l'ensemble de couple A ». On n'écrira pas explicitement ses abréviations car elles sont très longues (A est un signe de type 4)

Chapitre 5

L'explosion convergente

« Le silence éternel de ces espaces infinis m'effraie. »
Blaise Pascal

Cette partie décrit la construction d'une famille d'ensembles purs particuliers : les ordinaux. On y montre que les ordinaux sont munis d'un bon ordre et constituent un prolongement de la suite des entiers naturels.
Dans la première partie, on s'attache à l'étude des ensembles bien ordonnés. On définit les opérations d'addition, de multiplication, et d'exponentiation de bons ordres et on montre le théorème de comparaison entre deux bons ordres.
La deuxième et la troisième partie sont consacrées à la construction des ordinaux proprement dite. Munie des opérations précédentes, la suite des ordinaux prolonge la suite des entiers naturels. On touchera du doigt dans les démonstrations les besoins d'une théorie des ensembles axiomatisée.
Dans la quatrième partie, on utilise les ordinaux pour montrer un résultats surprenant : le théorème de Goodstein, qui affirme la convergence paradoxale des suites du même nom.

5.1 Bons ordres

Ce qui légitime les démonstrations par récurrence sur les entiers est la propriété que tout ensemble non vide d'entiers possède un plus petit élément. Le principe de récurrence s'étend à tous les ordres qui ont la même propriété : les bons ordres. Ce sont ces ordres particuliers qu'on étudie ici.

5.1.1 Définitions

Définition 1.1.1
Un ordre $\leq$ sur un ensemble A est dit bon si toute partie non vide de A possède un plus petit élément.

En particulier, un ensemble bien ordonné possède un plus petit élément, que l'on peut noter 0.

Convention
Si $\leq$ est un ordre on notera $<$ l'ordre strict associé, c'est-à-dire la relation « $x \leq y$ et $x \neq y$ », qui est antiréflexive ($x < x$ est toujours faux) et transitive. Inversement, si $<$ est un ordre strict, on notera $\leq$ l'ordre large associé, c'est-à-dire la relation « $x < y$ ou $x = y$ », qui est bien réflexive, antisymétrique, et transitive.

La propriété suivante démontre le principe d'induction généralisé aux bons ordres.

Proposition 1.1.2
Supposons que $<$ est un bon ordre sur A et soit $P(x)$ une propriété pour laquelle le principe de séparation est valide. Si P(0) est vraie et que $P(x)$ est vraie dès que $P(y)$ est vraie pour tout $y < x$, alors $P(x)$ est vraie pour tout x dans A.

La démonstration de ce principe d'induction est simple.

Démonstration
Le principe de séparation permet de considérer l'ensemble B des éléments de A qui ne satisfont pas P. Par l'absurde, supposons B non vide. $0 \notin B$ et B possède un élément minimum m. Mais alors, $P(x)$ est vraie pour tout $x < m$, donc $P(m)$ est vraie. D'où la contradiction. Donc $B = \oslash$ c'est-à-dire que P est vraie pour tout x dans A.

Exemples
L'ordre usuel sur **N** est un bon ordre. De ce fait sa restriction à tout sous-ensemble de **N** est également un bon ordre.
Par contre, l'ordre sur **Z** ou **Q** n'est pas un bon ordre : dans les deux cas, la partie **Z** n'a pas de plus petit élément. Dans le deuxième cas on peut aussi considérer l'ensemble des rationnels strictement positifs.

On a les propriétés suivantes sur les bons ordres.

Proposition 1.1.3
Soit $\mathcal{A} = (A, <)$ un ensemble bien ordonné.

(i) S'il est non vide, il possède un plus petit élément, et tout élément de A qui n'est pas maximal possède un plus petit majorant.

(ii) Il n'existe pas de suite infinie strictement décroissante dans A.

(iii) Si B est un sous-ensemble de A, alors la restriction de $<$ à B est un bon ordre.

5.1.2 Rigidité des bons ordres

On s'intéresse aux morphismes de bons ordres.
La notion de morphisme pertinente pour les ensembles ordonnés est celle d'application strictement croissante : si (A,<) et (B,<) sont deux ordres stricts, une applica-

tion f de A dans B est un morphisme si $x < y$ entraîne $f(x) < f(y)$. Si de plus f est bijective, on dit que f est un isomorphisme.

Le lemme-clé pour la rigidité des bons ordres est le suivant :

Lemme 1.2.1
Soit (A,<) un ensemble bien ordonné et f une application strictement croissante de A dans lui-même. On a pout tout $a \in A$, $a \leq f(a)$.

Démonstration
Soit $X = \{x \in A; f(x) < x\}$. Si X est non vide, il admet un plus petit élément m. Alors $f(m) < m$. De la stricte croissance de f, on tire $f(f(m)) < f(m)$. Mais $f(m)$ n'est pas dans X. Contradiction.

Proposition 1.2.2
Si (A,<) et (B,<) sont deux ensembles bien ordonnés, il existe au plus un isomorphisme de A sur B. En particulier, l'identité est le seul automorphisme de A.

Démonstration
Soient f et g deux isomorphismes de A sur B. Alors, par le lemme 2.2.1, g^{-1} est un isomorphisme de B vers A, puis $g^{-1} \circ f$ est un automorphisme puis par le lemme 2.2.2, $a \leq g^{-1} \circ f(a)$ pour tout a de A donc $g(a) \leq f(a)$. Par symétrie, $f(a) \leq g(a)$ donc $f = g$.

5.1.3 Comparaison de bons ordres

Définition 1.3.1
Supposons que $<$ est un ordre sur A. Pour $a \in A$, on appelle segment initial déterminé par a, et on note $I_<(a)$ ou $I(a)$ l'ensemble $\{x \in A; x < a\}$.

Une relation d'ordre étant transitive, un segment initial d'un ensemble ordonné est toujours clos par minorant, c'est-à-dire qu'un minorant d'un élément de $I(a)$ est encore dans $I(a)$. La réciproque est en général fausse : en effet dans $\mathbf{Q}$, l'ensemble $\{x \in \mathbf{Q}; x < \sqrt{2}\}$ est clos par minorant sans être un segment initial de $\mathbf{Q}$. Par contre, dans le cas des bons ordres, on a la réciproque.

Lemme 1.3.2
Supposons que $<$ est un bon ordre sur A et soit X un sous-ensemble de A clos par minorant. Alors X est A tout entier, ou un segment initial de A.

Démonstration
Soit $Y = A - X$. Ou bien Y est vide, ou bien soit a son plus petit élément. Par construction $I(a) \subseteq X$. Réciproquement, soit x dans X. Si on avait $a \leq x$ alors

comme X est clos par minorant, on aurait $a \in X$, ce qui n'est pas le cas. Donc $X = I(a)$.

Lemme 1.3.3
Si $<$ est un bon ordre sur A, alors A n'est isomorphe à aucun de ses segments initiaux, et deux segments initiaux distincts de A ne sont jamais isomorphes.

Démonstration
Soit a élément de A et f une application de A dans I(a) : on a $f(a) < a$ ce qui , par le lemme 1.2.1, interdit à f d'être strictement croissante.
Soient maintenant a, a' distincts dans A : par exemple $a < a'$. $I(a')$ est bien ordonné et $I(a)$ en est un segment initial, donc par le résultat précédent, $I(a)$ et $I(a')$ ne peuvent être isomorphes.

Proposition 1.3.4
Soient $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, <)$ deux ensembles bien ordonnés. Alors un des trois cas suivants se présente :

(i) $\mathcal{A}$ et $\mathcal{B}$ sont isomorphes.

(ii) $\mathcal{A}$ est isomorphe à un segment initial de $\mathcal{B}$.

(iii) $\mathcal{B}$ est isomorphe à un segment initial de $\mathcal{A}$.

Démonstration
On définit une correspondance F de A dans B par :

$$F(a) = b \Leftrightarrow I(a) \text{ est isomorphe à } I(b)$$

Le lemme précédent montre que F est fonctionnelle, c'est-à-dire que, pour chaque a dans A, il existe au plus une valeur b de B telle que b=F(a). Par ailleurs, on a, pour la même raison que F est injective. Pour le moment, on ne peut affirmer que F est définie sur tout A, ou qu'elle est bijective.
Montrons que le domaine Dom(F) est clos par minorant. Soit $a' < a$ avec $a \in A$. Par définition, il existe un isomorphisme $f : I(a) \to I(F(a))$. Soit alors f' la restriction de f au segment initial $I(a')$. f' est alors strictement croissante. Donc l'image de f' est incluse dans $I(f(a'))$. Inversement, soit y dans $I(f(a'))$. Par surjectivité de f, il existe x dans $I(a)$ tel que $f(x) = y$. Et comme $y < f(a')$, il vient $x < a'$. Donc l'image de f' est $I(f(a'))$. Puis F est définie en a' et $F(a') = f(a') < F(a)$.
Donc F est strictement croissante et que son domaine est clos par minorant dans A. De même, l'image de F est close par minorant dans B : si b est dans Im(F) et $b' < b$ $b' \in Im(F)$.
Donc quatre cas sont possibles :

(i) $Dom(F) = A$ et $Im(F) = B$. Alors A est isomorphe à B.

(ii) $Dom(F) = A$ et Im(F) est un segment initial de B : alors A est isomorphe à un segment initial de B.

(iii) Dom(F) est un segment initial de A et Im(F)=B alors B est isomorphe à un segment initial de A.

(iv) $Dom(F) = I(a)$ et $Im(F) = I(b)$. Mais alors,par définition, on devrait avoir $b = F(a)$. Contradiction.

5.1.4 Addition de bons ordres

On définit la somme de deux ordres, et on montre que la somme de deux bons ordres est un bon ordre.

L'idée pour définir la somme de deux ensembles ordonnés $(A, <)$ et $(B, <)$ est de juxtaposer ces ensembles : on place les éléments de B après ceux de A. Pour éviter d'éventuels problèmes liés aux éléments communs à A et B, on introduit la notion d'union disjointe.

Définition 1.4.1(union disjointe, somme)

(i) Soient A et B deux ensembles. On définit la somme disjointe $A \oplus B$ de A et B par

$$A \oplus B = (A \times \{1\}) \cup (B \times \{2\})$$

(ii) Soient $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, <)$ deux ensembles ordonnés. On appelle somme de ces ensembles, notée $\mathcal{A} + \mathcal{B}$ le couple $(A \oplus B, <)$ où la relation $<$ est définie par

$$(a, i) < (b, j) \Leftrightarrow ((i < j) \text{ ou } ((i = j) \text{ et } (a < b)))$$

Exemple
Soient p, q deux entiers. La somme des intervalles $\{1..p\}$ et $\{1..q\}$, munis de l'ordre usuel est isomorphe à $\{1...p + q\}$ muni de l'ordre usuel.

Pour une preuve des propositions suivantes, on renvoie au cours de Dehornoy [6] (chapitre 2).

Proposition 1.4.2
La somme de deux ensembles ordonnés (resp. totalement, resp. bien ordonnés) est un ensemble ordonné (resp. totalement, resp. bien ordonné).

Proposition 1.4.3
A isomorphisme près, l'addition des ordres est associative ; pour tous $\mathcal{A}, \mathcal{B}, \mathcal{C}$, $(\mathcal{A} + \mathcal{B}) + \mathcal{C}$ est isomorphe à $\mathcal{A} + (\mathcal{B} + \mathcal{C})$.

5.1.5 Multiplication des bons ordres

Définition 1.5.1
Soient $(A, <)$ et $(B, <)$ deux ensembles ordonnés. On appelle produit de $(A, <)$ et $(B, <)$ le couple $(A \times B, <)$ où $<$ est définie par

$$(a, b) < (a', b') \Leftrightarrow ((b < b') \text{ ou } ((b = b') \text{ et } (a < a')))$$

Exemple
Soient p, q deux entiers. Alors le produit de $\{1..p\}$ et $\{1..q\}$ équipés de l'ordre usuel, est isomorphe à $\{1..pq\}$ muni de l'ordre usuel.

Proposition 1.5.2
Le produit de deux ensembles ordonnés (resp. totalement, resp. bien ordonnés) est un ensemble bien ordonné (resp. totalement, resp. bien ordonné).

Proposition 1.5.3
A isomorphisme près, la multiplication des ordres est associative et distributive à gauche par rapport à l'addition. $(\mathcal{A}\times\mathcal{B})\times\mathcal{C}$ *est isomorphe à* $\mathcal{A}\times(\mathcal{B}\times\mathcal{C})$ *et* $\mathcal{A}\times(\mathcal{B}+\mathcal{C})$ *est isomorphe à* $(\mathcal{A}\times\mathcal{B})+(\mathcal{A}\times\mathcal{C})$.

5.1.6 Exponentiation de bons ordres

Définition 1.6.1
Soient $(A,<)$ *et* $(B,<)$ *deux ensembles ordonnés. On suppose que A possède un plus petit élément noté 0.*

(i) Pout toute suite s d'éléments de A on appelle support de s l'ensemble $\{i; s(i)\neq 0\}$*, et on note* $A^{(B)}$ *l'ensemble des suites de* A^B *à support fini.*

(ii) On appelle exponentiation de A par B le couple $(A^{(B)},<)$ *où* $<$ *est définie par*

$$f<g \Leftrightarrow (\exists\ i \text{ tel que } f(i)<g(i) \text{ et } f(j)=g(j) \text{ pour tout } j>i)$$

Exemple
Soient p, q deux entiers. Alors l'exponentielle des intervalles $\{1...p\}$ et $\{1...q\}$ équipés de l'ordre usuel est isomorphe à $\{1...p^q\}$.

Proposition 1.6.2
Soient $(A,<)$ *et* $(B,<)$ *deux ensembles totalement (resp. bien ordonnés) tels que A a un plus petit élément. Alors l'exponentielle de A par B est un ensemble totalement (resp. bien) ordonné.*

Proposition 1.6.3
Si $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ *sont trois ensembles totalement ordonnés tels que A ait un élément minimal,* $\mathcal{A}^{\mathcal{B}+\mathcal{C}}$ *est isomorphe à* $\mathcal{A}^{\mathcal{B}}\times\mathcal{A}^{\mathcal{C}}$ *et* $\mathcal{A}^{\mathcal{B}\times\mathcal{C}}$ *est isomorphe à* $(\mathcal{A}^{\mathcal{B}})^{\mathcal{C}}$.

5.2 Construction des ordinaux

Dans cette section, nous allons construire une famille d'ensembles bien ordonnés particuliers, les ordinaux. Les ordinaux se rangent en une suite bien ordonnée, mais

ne forment pas un ensemble. On montre que tout ensemble bien ordonné est isomorphe à un unique ordinal.

La construction présentée ci-dessous est due à John von Neumann. Mais, il existe d'autres constructions possibles des ordinaux : Cantor les définissait comme classe d'isomorphisme de bons ordres.

5.2.1 Ensembles transitifs

Avant d'introduire les ordinaux, on introduit une classe particulière d'ensembles, les ensembles transitifs.

Définition 2.1.1
Un ensemble d'ensembles A est dit transitif si tout élément d'un élément de A est élément de A.

Notation
Si A est un ensemble d'ensembles on notera $\bigcup A$, l'union de A, c'est-à-dire la réunion des éléments de A, et $\bigcap A$ l'intersection de A, c'est-à-dire l'intersection des éléments de A.

Ainsi, un ensemble A est transitif si et seulement si on a

$$x \in a \in A \Rightarrow x \in A$$

ie si $a \in A$ entraîne $a \subseteq A$, ie $A \in \wp(A)$, ie $\bigcup A \subseteq A$.

La notion d'ensemble transitif n'est pas familière, et il est clair que la plupart des ensembles ne sont pas transitifs. Cependant le lemme suivant montre qu'il existe des ensembles transitifs.

Lemme 2.1.2

(i) L'ensemble vide est transitif.

(ii) Si A est transitif, il en est de même de $A \cup \{A\}$, de $\wp(A)$, et de $\bigcup A$.

(iii) Toute union et toute intersection d'ensembles transitifs est transitive.

Démonstration

(i) L'ensemble vide n'ayant pas d'élément, il est transitif.

(ii) Supposons A transitif. Soit $a \in A \cup \{A\}$. On a donc soit $a \in A$, et alors $a \subseteq A$,par transitivité de A, soit $a = A$. Dans tous les cas, $a \subseteq A \cup \{A\}$.
Soit $x \in a \in \wp(A)$ alors $x \in A$ donc par transitivité de A, $x \in \wp(A)$.
Soit $a \in \bigcup A$, alors il existe $b \in A$ tel que $a \in b \in A$. Donc par transitivité de A, $a \in A$ puis $a \subseteq A$.

(iii) Soit $(A_i)_{i\in I}$ une famille d'ensembles transitifs. Supposons $x \in a \in \cup(A_i)$. Alors il existe i tel que $x \in a \in A_i$ donc $x \in A_i$ puis $x \in \bigcup_{i\in I} A_i)$.

Il existe donc une infinité d'ensembles transitifs, puisqu'au moins tous les ensembles obtenus inductivement à partir de $\oslash$ et des opérations $A \mapsto A \cup \{A\}$ et $A \mapsto \wp(A)$ sont transitifs.

5.2.2 Ordinaux

Définition 2.2.1
On dit qu'un ensemble α est un ordinal si α est transitif et que la restriction de $\in$ à α est un bon ordre strict.

Autrement dit α est un ordinal si et seulement si les 4 conditions suivantes sont vérifiées :

(i) pour tout x dans α, on a $x \subseteq \alpha$.

(ii) pour tout x dans α, on a $x \notin x$.

(iii) pour tous x,y,z dans α, si $x \in y \in z$ alors $x \in z$.

(iv) pour tout sous-ensemble non vide A de α, A admet un plus petit élément.

Lemme 2.2.2

(i) L'ensemble vide est un ordinal.

(ii) Si α est un ordinal, $\alpha \notin \alpha$.

(iii) Si α est un ordinal, alors $\alpha \cup \{\alpha\}$ en est un.

Démonstration

(i) L'ensemble vide n'ayant pas d'élément, et donc aucun sous-ensemble non vide, les quatre conditions sont satisfaites.

(ii) Par définition, si α est un ordinal, on a $x \notin x$ pour tout élément x de α. Donc, si α était élément de lui-même, ie $\alpha \in \alpha$ on aurait, $\alpha \notin \alpha$. Contradiction. Donc $\alpha \notin \alpha$.

(iii) Soit α un ordinal et $\beta = \alpha \cup \{\alpha\}$. Déjà, le lemme 3.1.2 affirme que β est transitif.
Supposons $x \in \beta$. Ou bien $x \in \alpha$ ou bien $x = \alpha$. Dans les deux cas, on a que $x \notin x$.
Soit $x, y, z \in \beta$ avec $x \in y \in z$. Si x,y,z appartiennent à α, on en déduit que $x \in z$. Supposons $x = \alpha$. On ne peut avoir $y = \alpha$ donc on est dans la situation $\alpha \in y \in \alpha$. Mais alors on aurait $\alpha \in \alpha$, ce qui est exclus. On montre de même que le cas $y = \alpha$ est impossible. Enfin, si $z = \alpha$, on a bien $x \in z$.
Donc la relation $\in$ est un ordre strict.
Montrons que cet ordre est un bon ordre. Soit A un sous-ensemble non vide de β.

Supposons d'abord $A \cap \alpha$ non vide. α étant un ordinal, $A \cap \alpha$ a un plus petit élément, x. Cet élément est encore un minorant de α donc x est le plus petit élément de A.
Si A est non vide et que $A \cap \alpha$ l'est, alors $A = \{\alpha\}$ et donc α est son élément minimum.

Il existe donc une infinité d'ordinaux, à savoir au moins $\oslash$ et tous les ensembles obtenus en répétant l'opération $\alpha \mapsto \alpha \cup \{\alpha\}$.

Notation
Pour tout ensemble A, on pose $S(A) = A \cup \{A\}$. Pour tout entier naturel n, on note $\underline{n} = S^n(\oslash)$.

Ces notations permettent de constater que pour tout $n \in \mathbf{N}^*$ on a $\underline{n} = \{\underline{0}...\underline{n-1}\}$.

Proposition 2.2.3
Pour tout entier n, l'ordinal $\underline{n}$ a exactement n éléments : les $\underline{k}$ pour $k < n$.

Démonstration
La démonstration se fait par récurrence sur n. $\underline{0} = \oslash$. Supposons le résultat acquis au rang n-1. $\underline{n} = \underline{n-1} \cup \{\underline{n-1}\}$ donc par hypothése de récurrence, $\underline{n} = \{\underline{0}...\underline{n-1}\}$.

Lemme 2.2.4
Tout élément d'un ordinal α est un ordinal strictement inclus dans α.

Démonstration
Soit α un ordinal et $x \in \alpha$. Alors $x \subseteq \alpha$ donc x est un ensemble d'ensembles. Soit $z \in y \in x$, par transitivité de la relation d'ordre $\in$, on a $z \in x$, donc x est transitif. Comme x est inclus dans α, la relation $\in$ restreinte à x est toujours un bon ordre strict donc x est un ordinal.
Enfin, comme $\alpha \notin \alpha$, $x \neq \alpha$.

Lemme 2.2.5
Si A est un ensemble non vide d'ordinaux, $\bigcap A$ est un ordinal.

Démonstration
Posons $a = \bigcap A$. Le lemme 3.1.2 assure que a est un ensemble transitif. Soit α un ordinal de A. Alors, $a \subseteq \alpha$ donc la restriction de $\in$ à a est un bon ordre. Donc a est un ordinal.

5.2.3 L'ordre sur les ordinaux

Nous allons montrer que les ordinaux se rangent en une suite bien ordonnée.

Lemme 2.3.1
La restriction de $\in$ aux ordinaux est un ordre strict.

Démonstration
Pour tout ordinal α, $\alpha \notin \alpha$. Par ailleurs soient $\beta \in \gamma \in \alpha$, on a $\beta \in \alpha$, ie la relation $\in$ est bien antiréflexive et transitive.

Définition 2.3.2
On notera $<$ la relation d'appartenance entre ordinaux.

Exemple
On a toujours $\alpha < S(\alpha) = \alpha \cup \{\alpha\}$. Pour m, n entiers, $m < n$ équivaut à $\underline{m} < \underline{n}$.

Proposition 2.3.3

(i) Tout ordinal coïncide avec l'ensemble des ordinaux strictement plus petits que lui.

(ii) L'ordre large associé à la restriction de $\in$ aux ordinaux est l'inclusion.

(iii) Pour chaque ordinal α l'ordinal $S(\alpha)$ est successeur immédiat de α. De plus S est strictement croissante.

Démonstration

(i) Soit α un ordinal : tous ses éléments sont des ordinaux strictment plus petits que α. Et, par définition, un ordinal strictement plus petit que α est dans α.

(ii) Supposons $\alpha \leq \beta$. Alors ou bien $\alpha < \beta$ ou bien $\alpha = \beta$. Dans tous les cas $\alpha \subseteq \beta$. Réciproquement supposons $\alpha \subseteq \beta$. Ou bien $\alpha = \beta$ ou bien $\alpha \subset \beta$ et alors $\beta - \alpha$ est une partie non vide de β, donc admet un plus petit élément α', qui est un ordinal. On va montrer que $\alpha' = \alpha$, ce qui donne $\alpha < \beta$.
Soit $\gamma \in \alpha$. Donc $\gamma \in \beta$. Puis γ est comparable avec α'. Ou bien $\gamma \in \alpha'$, ou bien $\gamma = \alpha'$, ou bien $\alpha' \in \gamma$. Si $\gamma = \alpha'$, alors $\gamma \in \beta - \alpha$, ce qui est exclus. Si $\alpha' \in \gamma$, alors, $\alpha' \in \alpha$ ce qui est exclu. Nécessairement $\alpha \subseteq \alpha'$.
Inversement soit $\gamma \in \alpha'$. Alors $\gamma \in \beta$. Alors α' étant le plus petit élément de $\beta - \alpha$, on a $\gamma \in \alpha$. $\alpha = \alpha'$.

(iii) $\alpha < S(\alpha)$ par définition. Supposons $\alpha < \beta$. Alors $\alpha \in \beta$ donc $\{\alpha\} \subseteq \beta$. Par ailleurs $\alpha \subseteq \beta$ donc $S(\alpha) \leq \beta$.

Proposition 2.3.4
Tout ensemble non vide d'ordinaux A possède un plus petit élément, à savoir $\bigcap A$.

Démonstration

Posons $a = \bigcap A$. a est un ordinal. Par construction $a \subseteq \beta$ pour tout $\beta \in A$. Supposons par l'absurde que pour tout $\beta \in A$ on ait $a \in \beta$. Alors $a \in \bigcap A$ soit $a \in a$, ce qui est exclus.

Appliquant ce qui précède à toute paire $\{\alpha, \beta\}$ d'ordinaux, on en déduit que l'ordre sur les ordinaux est un ordre total.

Comme l'ordre sur les ordinaux est un bon ordre, on en déduit la possibilité de faire des démonstrations inductives, en vertu de la proposition 1.1.2.

5.2.4 Borne supérieure ; ordinaux limites

Proposition 2.4.1
Tout ensemble A d'ordinaux possède une borne supérieure, à savoir $\bigcup A$.

Démonstration
Posons $a = \bigcup A$. On a que a est transitif. Soient $\alpha, \beta, \gamma \in a$. On a $\alpha \in \alpha$ et $\alpha \in \beta \in \gamma$ entraîne $\alpha \in \gamma$. Donc la restriction de $\in$ à a est un ordre strict.
Soit X une partie non vide de A. Posons $\alpha = \bigcap X$. Puisque X est un ensemble d'ordinaux, la proposition précédente entraîne que α est le plus petit élément de X. Donc $\in$ est un bon ordre sur a.
Pour tout α dans A, on a $\alpha \subseteq a$. Donc a est un majorant de A. Soit par ailleurs β un autre majorant de A. On a par définition, pour tout α de A, $\alpha \subseteq \beta$. Donc $a = \bigcup A \subseteq \beta$. Ce qui montre que a est le plus petit des majorants de A.

En revanche, l'ordinal $\bigcup A$ peut très bien ne pas être dans A.

Une conséquence directe est que les ordinaux ne forment pas un ensemble.

Proposition 2.4.2 (paradoxe de Burali-Forti)
Aucun ensemble ne contient tous les ordinaux.

Démonstration
Supposons qu'il existe un ensemble contenant tous les ordinaux. Alors, soit l'ensemble Ω de tous les ordinaux. Dans ce cas $\bigcup \Omega$ est un ordinal qui majore tous les ordinaux. En particulier $S(\bigcup \Omega) \leq \bigcup \Omega$, ce qui est absurde.

Définition 2.4.3
On note ω *la borne supérieure des ordinaux* $\underline{n}$ *pour n entier.*

ω est donc le premier ordinal infini. En particulier il n'est égal à aucun des $\underline{n}$ pour n entier.

On va partitionner les ordinaux non nuls en deux familles : les ordinaux limites et successeurs.

Lemme 2.4.4

Pour tout ordinal α non nul :

(i) ou bien $\beta < \alpha$ entraîne $S(\beta) < \alpha$ pour tout ordinal β, et alors on a la relation $\alpha = \bigcup \alpha$. On dit alors que α est un ordinal limite.

(ii) ou bien il existe un ordinal β tel que $\alpha = S(\beta)$, auquel cas $\bigcup \alpha = \beta$. On dit alors que α est un ordinal successeur.

Démonstration

Soit α un ordinal non nul, on a $\bigcup \alpha \subseteq \alpha$, et pour tout ordinal β, $\beta < \alpha$ implique $S(\beta) \leq \alpha$. Donc soit $S(\beta) < \alpha$ pour tout tel ordinal, soit il existe β tel que $\alpha = S(\beta)$.
Dans le premier cas, $\beta < \alpha$ entraîne $\beta \in S(\beta) \in \alpha$. Donc $\beta \in \alpha$ entraîne $\beta \in \bigcup \alpha$. Puis $\bigcup \alpha = \alpha$.
Dans le second cas, $\gamma \in \beta$ entraîne $\gamma \in \bigcup \alpha$. Donc $\beta \subseteq \bigcup \alpha$. Inversement, comme $\alpha = \beta \cup \{\beta\}$, on a $\bigcup \alpha = \bigcup \beta \cup \beta = \beta$.

Exemple

Les ordinaux $\underline{1}, \underline{2}...$ sont des ordinaux successeurs tandis que ω est un ordinal limite.

5.2.5 Le théorème de comparaison

Proposition 2.5.1

Tout ensemble bien ordonné est isomorphe à un unique ordinal.

« Démonstration »

L'idée de la démonstration est dans la proposition 1.3.4. Si $(A, <)$ est un ensemble bien ordonné, le théorème de comparaison nous dit que ou bien $(A, <)$ est isomorphe à la suite des ordinaux, ou bien la suite des ordinaux est isomorphe à un segment initial de A, ou bien $(A, <)$ est isomorphe à un segment initial de la suite des ordinaux. Les deux premiers cas sont exclus car la suite des ordinaux n'est pas un ensemble, donc $(A, <)$ est isomorphe à un segment initial $I(\alpha)$ c'est-à-dire à α.
Toutefois nous avons appliqué le théorème 1.3.4 à la suite des ordinaux qui n'est pas un ensemble. Notons qu'en revanche le théorème de comparaison (ou le lemme 1.3.2) permet de démontrer l'unicité de l'ordinal : en effet un bon ordre n'est jamais isomorphe à un de ses segments initiaux.

5.3 Arithmétique ordinale

5.3.1 Un critère

On se donne tout d'abord un critère utile pour démontrer des inégalités entre ordinaux.

Lemme 3.1.1
Supposons que α et β sont deux ordinaux respectivement isomorphes à des ensembles bien ordonnés $(A, <)$ et $(B, <)$.

(i) *$\alpha = \beta$ si et seulement si A et B sont isomorphes.*

(ii) *$\alpha < \beta$ si et seulement s'il existe un isomorphisme de A sur un segment initial de B.*

(iii) *$\alpha \leq \beta$ si et seulement s'il existe une injection strictement croissante de A dans B.*

Démonstration

(i) Le point (i) n'est qu'une reformulation de l'unicité dans le théorème précédent.

(ii) La condition est évidemment nécessaire. Supposons qu'il existe un isomorphisme entre A et un segment initial de B. Alors il existe un isomorphisme entre α et un segment initial de β. Donc il existe $\gamma < \beta$ tel que α soit isomorphe à γ donc par le théorème précédent $\alpha = \gamma$.

(iii) La condition est nécessaire. Supposons qu'il existe une injection strictement croissante de A dans B, alors il existe une injection strictement croissante f de α dans β. Par l'absurde supposons $\beta < \alpha$. Alors f est une injection strictement croissante de α dans lui-même, puis par le lemme 2.2.2, $f(\beta) \geq \beta$, ce qui contredit le fait que $Im(f) \subseteq \beta$. Donc $\alpha \leq \beta$.

5.3.2 Addition ordinale

Définition 3.2.1
Pour α, β ordinaux, on définit $\alpha + \beta$ comme l'unique ordinal isomorphe à $(\alpha, <) + (\beta, <)$

Exemple
Pour n, k entiers, l'ordinal $\underline{n} + \underline{k}$ a n+k éléments : $\underline{n} + \underline{k} = \underline{n + k}$.

Proposition 3.2.2

(i) *On a toujours $\alpha + \underline{0} = \underline{0} + \alpha = \alpha$.*

(ii) *On a toujours $\alpha + \underline{1} = S(\alpha)$. On a $\underline{1} + \alpha = S(\alpha)$ pour α fini et $\underline{1} + \alpha = \alpha$ pour α infini.*

(iii) *L'addition ordinale est associative : on a toujours $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.*

Démonstration
Vérifions par exemple (i). L'application f définie par $f((\theta,1)) = \theta$ est un isomorphisme de $\alpha \oplus \oslash$ sur α. Idem pour $\oslash \oplus \alpha$.

En revanche, l'addition ordinale n'est pas commutative : $\underline{1} + \omega = \omega \neq \omega + \underline{1}$.

Proposition 3.2.3

(i) Pour chaque ordinal α, l'addition de α à gauche est strictement croissante et continue au sens suivant : $\beta < \beta'$ entraîne $\alpha+\beta < \alpha+\beta'$ et pour λ limite, on a $\alpha + \lambda = sup_{\beta<\lambda}\alpha+\beta$.

(ii) Pour chaque ordinal α, l'addition de α à droite est non-décroissante : $\beta \leq \beta'$ entraîne $\beta+\alpha \leq \beta'+\alpha$. Par ailleurs, pour λ limite, on a $\lambda+\alpha \geq sup_{\beta<\lambda}\beta+\alpha$.

Ainsi l'addition ordinale admet la simplification à gauche : $\alpha+\beta = \alpha+\beta'$ entraîne $\beta = \beta'$. En revanche elle n'admet pas la simplification à droite, par exemple, d'après le lemme 3.2.2, on a $\underline{0}+\omega = \underline{1}+\omega$. De même, $\underline{1}+\omega > sup_{\beta<\omega}\underline{1}+\beta$.

5.3.3 Multiplication ordinale

Définition 3.3.1
Pour α, β ordinaux, on définit $\alpha.\beta$ comme l'unique ordinal γ isomorphe à$(\alpha,<) \times (\beta,<)$.

Exemple
Pour n,k entiers, l'ordinal $\underline{n}.\underline{k}$ a nk éléments : on a $\underline{n}.\underline{k} = \underline{nk}$.

[1ex]
Proposition 3.3.2

(i) On a toujours $\alpha.\underline{0} = \underline{0}.\alpha = \underline{0}$, et $\underline{1}.\alpha = \alpha.\underline{1} = \alpha$.

(ii) La multiplication ordinale est associative et distributive à gauche par rapport à l'addition : $\alpha.(\beta.\gamma) = (\alpha.\beta).\gamma$ et $\alpha.(\beta+\gamma) = \alpha.\beta + \alpha.\gamma$.

On en déduit entre autres que pour tout entier n, et tout ordinal α, $\alpha.\underline{n} = \alpha.(\underline{1} + ...\underline{1}) = \alpha + ...\alpha$. En particulier $\omega.\underline{2} = \omega+\omega \neq \underline{2}.\omega$. Donc la multiplication ordinale n'est ni commutative, ni distributive à droite.

Lemme 3.3.3
Pour tout ordinal γ vérifiant $\gamma < \alpha.\beta$ il existe un couple d'ordinaux (ρ,σ) avec $\rho < \alpha$ et $\sigma < \beta$ vérifiant $\gamma = \alpha.\sigma + \rho$.

Démonstration
On peut supposer $\alpha > \underline{0}$. Soit f l'isomorphisme (unique) entre $(\alpha,<) \times (\beta,<)$ et $(\alpha.\beta,<)$. Soit alors $\gamma < \alpha.\beta$, posons $(\rho,\sigma) = f^{-1}(\gamma)$. On a $\rho < \alpha$ et $\sigma < \beta$. Alors le

segment initial $I(\gamma) = \gamma$ de $\alpha.\beta$ est isomorphe au segment initial $I(\rho, \sigma)$. Or $I(\rho, \sigma)$ est l'ensemble des couples (ξ, η) tels que $\eta < \sigma$ ou $\eta = \sigma$ et $\xi < \rho$. Donc $I(\rho, \sigma)$ consiste en les éléments de $I(\alpha, \sigma)$ suivis des éléments de la forme (ξ, σ) avec $\xi < \rho$. Donc $I(\rho, \sigma)$ est isomorphe à $\alpha.\sigma + \rho$ puis $\gamma = \alpha.\sigma + \rho$.

Proposition 3.3.4

(i) Pour chaque ordinal α non nul, la multiplication par α à gauche est une opération strictement croissante et continue au sens suivant : $\beta < \beta'$ entraîne $\alpha.\beta < \alpha.\beta'$ et pour λ limite, on a $\alpha.\lambda = sup_{\beta<\lambda}\alpha.\beta$.

(ii) Pour chaque ordinal α, la multiplication de α à droite est non-décroissante : pour $\beta \leq \beta'$, $\beta.\alpha \leq \beta'.\alpha$ et vérifie : pour λ limite $\lambda.\alpha \geq sup_{\beta<\lambda}\beta.\alpha$.

On en déduit comme dans le cas de l'addition, que la multiplication ordinale admet la simplification à gauche par un ordinal non nul : $\alpha.\beta = \alpha.\beta'$ entraîne $\beta = \beta'$ pour α non nul.

On a alors le résultat de division euclidienne suivant :

Proposition 3.3.5
Pour tout ordinal β et tout ordinal α non nul, il existe un unique couple d'ordinaux (ρ, σ) vérifiant $\beta = \alpha.\sigma + \rho$, avec $\rho < \alpha$. Alors $\sigma \leq \beta$.

Démonstration
Le lemme 3.3.3 assure l'existence.
Reste à prouver l'unicité. Soient $\alpha.\sigma + \rho = \alpha.\sigma' + \rho'$ tels que $\rho, \rho' < \alpha$. Supposons par l'absurde $\sigma < \sigma'$. Alors $\alpha.\sigma + \rho < \alpha.\sigma + \alpha = \alpha.(\sigma + \underline{1}) \leq \alpha.\sigma' \leq \alpha.\sigma' + \rho'$. D'où une contradiction. donc $\sigma = \sigma'$ puis, par simplification à gauche, $\rho = \rho'$. D'où l'unicité.

5.3.4 Exponentiation ordinale

Définition 3.4.1
Pour α, β ordinaux, on définit l'ordinal α^β comme l'unique ordinal isomorphe à $(\alpha, <)^{(\beta,<)}$.

Exemple
Pour n,k entiers, l'ordinal $\underline{n}^{\underline{k}}$ a n^k éléments donc on a la formule : $\underline{n}^{\underline{k}} = \underline{n^k}$.

Proposition 3.4.2

(i) On a toujours $\alpha^{\underline{0}} = \underline{1}$, $\alpha^{\underline{1}} = \alpha$, $\underline{1}^\beta = \underline{1}$, et pour α non nul, $\underline{0}^\alpha = \underline{0}$.

(ii) On a toujours : $\alpha^{\beta+\gamma} = \alpha^\beta.\alpha^\gamma$ et $\alpha^{\beta.\gamma} = (\alpha^\beta)^\gamma$.

Ainsi pour tout entier n : $\alpha^{\underline{n}} = \alpha...\alpha$.

Proposition 3.4.3

(i) Pour chaque ordinal α ($\alpha \neq \underline{0}$ et $\underline{1}$), l'exponentiation de base α est strictement croissante et continue : $\beta < \beta'$ entraîne $\alpha^\beta < \alpha^{\beta'}$ et pour λ limite, on a : $\alpha^\lambda = sup_{\beta<\lambda}\alpha^\beta$.

(ii) Pour tout α, l'exponentiation par α est non-décroissante : $\beta \leq \beta'$ entraîne $\beta^\alpha \leq \beta'^\alpha$ et pour λ limite, $\lambda^\alpha \geq sup_{\beta<\lambda}\beta^\alpha$.

5.4 Théorème de Goodstein

Ce chapitre est consacré aux suites de Goodstein. Pour les définir, introduisons tout d'abord la notion d'écriture en base p itérée d'un entier n.

Ecrire n en base p consiste à trouver les uniques coefficients c_i tels que $n = p^{n_1}.c_{n_1} + ...p.c_1 + c_0$ où chacun des entiers c_i vérifie $0 \leq c_i < p$.
Par exemple, le nombre 59110 s'écrit en base 3 : $59110 = 3^{10} + 2.3^3 + 2.3^1 + 1.3^0$

On peut alors décomposer les exposants eux-mêmes en base p et itérer le processus.
Pour l'exemple : $59110 = 3^{10} + 2.3^3 + 2.3^1 + 1 = 3^{3^2+1} + 2.3^3 + 2.3^1 + 1$

On obtient alors ce qu'on appelle l'écriture en base p itérée. On se convainc facilement que l'écriture est unique.

Définition 4.1 *Pour $q \geq p \geq 2$ on définit la fonction $f_{p,q}$ de $\boldsymbol{N}$ dans $\boldsymbol{N}$ qui à n, fait correspondre l'entier obtenu en décomposant n en base p itérée, puis en remplaçant p par q.*

Exemple Reprenons l'exemple précédent : $59110 = 3^{3^2+1} + 2.3^3 + 2.3^1 + 1$
On a :$f_{3,4}(59110) = 4^{4^2+1} + 2.4^4 + 2.4^1 + 1 = 17179869184$.

Définition 4.2 *Pour chaque entier a, la suite de Goodstein de graine a $(g_p(a))$ est définie de la manière suivante : $g_2(a) = a$ puis pour tout p : $g_{p+1}(a) = f_{p,p+1}(g_p(a)) - 1$ si $g_p(a)$ est non nul et $g_{p+1}(a) = 0$ sinon.*

On est amené à penser que les changements de base successifs vont faire exploser la suite de Goodstein et que le rôle du terme (-1) est négligeable. Regardons sur quelques exemples.

Exemple
Les suites de Goodstein de graines 1,2,3 atteignent très vite la valeur 0 : il suffit de 6 itérations pour la graine 3.

Considérons à présent la suite de Goodstein de graine 4.
$g_2(4) = 4 = 2^{2^1}$

$g_3(4) = f_{2,3}(4) - 1 = 3^{3^1} - 1 = 2.3^2 + 2.3 + 2 = 26$
$g_4(4) = f_{3,4}(4) - 1 = 2.4^2 + 2.4 + 2 - 1 = 2.4^2 + 2.4 + 1 = 41$
$g_5(4) = f_{4,5}(4) - 1 = 2.5^2 + 2.5 + 1 - 1 = 2.5^2 + 2.5 = 60.$
$g_6(4) = 2.6^2 + 2.6 - 1 = 83 = 2.6^2 + 6 + 5$
$g_7(4) = 2.7^2 + 7 + 4 = 109$
$g_8(4) = 2.8^2 + 8 + 3 = 139$
...
$g_{14}(4) = 2.14^2 + 9 = 401$
...
$g_{22}(4) = 2.22^2 + 1 = 969$
$g_{23}(4) = 2.23^2 = 1058$
$g_{24}(4) = 2.24^2 - 1 = 1151 = 24^2 + 23.24 + 23$
...
$g_{47}(4) = 47^2 + 23.47 = 3290$
$g_{48}(4) = 48^2 + 22.48 + 47 = 3407$
...

On est tenté de croire que la suite va croître indéfiniment. Pourtant le théorème de Goodstein affirme que pour tout a, $g_p(a)$ finit par prendre la valeur 0 ! Toutefois, pour des graines a supérieures à 3, le nombre d'itérations est très important. Dans le cas de la graine 4 par exemple, il faut $3^{2402653211} - 3$ itérations !

Pour montrer le théorème, définissons une fonction $f_{p,\omega}$ sur le modèle de $f_{p,q}$:

Définition 4.3
Pour tout entier p, on définit la fonction $f_{p,\omega}$ de $\boldsymbol{N}$ qui à un entier n associe le nombre construit en décomposant n en base p itérée, puis en remplaçant p par ω.

Lemme 4.4
Pout tout p,n on a : $f_{p,\omega}(n) < f_{p,\omega}(n+1)$

Démonstration
Fixons p et démontrons le résultat par récurrence sur n.
Le résultat est trivial pour n=0 ou n=1. Soit donc $n \geq 1$. La décomposition de n en base p fait intervenir des puissances de p au plus (n-1)-ièmes :

$$n = p^{n-1}.c_{n-1} + ...p.c_1 + c_0$$

On a alors : $f_{p,\omega}(n) = \omega^{f_{p,\omega}(n-1)}.\underline{c_{n-1}} + ...\omega^{f_{p,\omega}(1)}.\underline{c_1} + \underline{c_0}$.

Soit m le plus petit entier tel que le coefficient c_m ne soit pas égal à $p-1$ ($m < n-1$).
La décomposition de $n+1$ en base p s'écrit alors : $n+1 = p^{n-1}.c_{n-1} + ...p^m.(c_m + 1)$.
Alors $f_{p,\omega}(n+1) = \omega^{f_{p,\omega}(n-1)}.\underline{c_{n-1}} + ...\omega^{f_{p,\omega}(m)}.\underline{c_m + 1}$.

Soit alors $\alpha = \omega^{f_{p,\omega}(n-1)}.\underline{c_{n-1}} + ...\omega^{f_{p,\omega}(m)}.\underline{c_m}$.
$f_{p,\omega}(n) = \alpha + \omega^{f_{p,\omega}(m-1)}.\underline{c_{m-1}} + ...\underline{c_0}$

et $f_{p,\omega}(n+1) = \alpha + \omega^{f_{p,\omega}(m)}$. Par hypothèse de récurrence $f_{p,\omega}(m) > ...f_{p,\omega}(0)$. Donc par les règles de stricte croissance de la multiplication à gauche, on a : $\omega^{f_{p,\omega}(m-1)}.\underline{c_{m-1}} + ...\omega^{f_{p,\omega}(0)}.\underline{c_0} < \omega^{f_{p,\omega}(m)}$. D'où, par ajout de α à gauche, $f_{p,\omega}(n) < f_{p,\omega}(n+1)$.

On peut alors démontrer la convergence des suites de Goodstein :

Proposition 4.5 (théorème de Goodstein)
Pour toute graine a, la suite $(g_p(a))_{p\geq 2}$ *tend vers 0, ie il existe* $p \in \boldsymbol{N}$ *tel que pour tout* $n \geq p$ *on ait* $g_n(a) = 0$.

Démonstration
Introduisons la suite auxiliaire $(h_p(a))$ définie par : $h_p(a) = f_{p,\omega}(g_p(a))$. Pour tout p tel que $g_p(a)$ soit non nul, on a :

$$h_{p+1}(a) = f_{p+1,\omega}(g_{p+1}(a)) = f_{p+1,\omega}(f_{p,p+1}(g_p(a)) - 1) < f_{p+1,\omega}(f_{p,p+1}(g_p(a))) \\ = f_{p,\omega}(g_p(a)) = h_p(a)$$

Donc par l'absurde, si la suite de Goodstein ne s'annulait pas, on obtiendrait une suite infinie strictement décroissante d'ordinaux, ce qui est impossible car l'ordre sur les ordinaux est un bon ordre. Donc $(g_p(a))$ tend vers 0.

Conclusion

Les propriétés des ordinaux introduites dans ce chapitre ont permis de démontrer le théorème de Goodstein. De manière générale, l'intérêt des ordinaux est qu'ils constituent un prolongement de la suite des entiers, et qu'ils sont munis d'opérations arithmétiques qui prolongent les opérations sur les entiers. Le fait qu'ils se rangent en une suite bien ordonnée permet de définir par induction des suites « plus grandes » que les entiers, ou de faire des démonstrations par induction (pour un autre exemple, voir la démonstration du théorème de Cantor-Bendixson dans [6]).
On peut toutefois se demander si le recours aux ordinaux, dont la construction est basée sur les axiomes de la théorie des ensembles, était nécessaire pour démontrer une propriété sur les entiers. La réponse est positive : le théorème de Kirby-Paris affirme que le théorème de Goodstein ne peut être démontré à partir des seuls axiomes de Peano. Il constitue donc un exemple particulièrement simple d'énoncé indécidable dans l'axiomatique de Peano, contrairement à ceux qui apparaissent dans le théorème d'incomplétude de Gödel (cf *Le chapitre 4 n'est pas démontrable* page 49).

FIG. 5.1 – R.L. Goodstein

```
public class Goodstein {
  static long power(long p, long q){
    if(q==0){
      return 1;
    }
    if(q%2==0){
      long n= power(p,q/2);
      return n*n;
    }
    long n= power(p,q/2);
    return n*n*p;
  }
  static long fpq (long n,long p, long q){
    //2<=p<=q
    //ak*p^k+.....ao->ak*q^fpq(k)+....ao
    if(n<p){
      return n;
    }
    long s=0;
    long ak=0;
    long r=n;
    long k=0;
    while(r!=0){//on calcule les ak
      ak=r%p;//r modulo p
      r=r/p;
      s=s+ak*power(q,fpq(k,p,q));
      k=k+1;
    }
    return s;
  }
  static long goodsteinGraine (long g){
    long i=1;
    long k=2;
    System.out.println(g);
    while(g>0){
      g=fpq(g,k,k+1)-1;
      System.out.println(g);
      i=i+1;
      k=k+1;
    }
    return i;
  }
  public static void main(String[] args) {

   System.out.println(goodsteinGraine(4));
  }
}
```

FIG. 5.2 – programme Java pour calculer les premiers termes de la suite de Goodstein

Chapitre 6

Les mille et un théorèmes

« La logique, c'est comme la loi :
si on l'appliquait parfaitement,
ce serait la mort. »
Claude Roy

6.1 Introduction

La théorie des modèles est une branche de la logique mathématique qui raisonne sur les formules mathématiques. Bien que méconnue, elle a de nombreuses applications en algèbre et en géométrie. L'objet de cette partie est de donner au lecteur un aperçu de la théorie des modèles, des objets manipulés et des raisonnements qu'elle utilise. Dans cet esprit notre but ici sera de démontrer le théorème suivant :

Théorème 6.1 (Ax 1969) *Soit f une application polynômiale de $\boldsymbol{C}^n$ dans $\boldsymbol{C}^n$ injective. Alors f est surjective.*

Par application polynômiale de $\mathbf{C}^n$ dans $\mathbf{C}^n$ on entend une application

$$f : \mathbf{C}^n \to \mathbf{C}^n$$

$$(x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

où les f_i sont des fonctions polynômiales de $\mathbf{C}^n$ dans $\mathbf{C}$.

Il existe une preuve de ce théorème qui utilise la géométrie algébrique, mais l'approche que nous allons développer ici, utilisant des notions de théorie des modèles, est nettement plus simple et plus rapide.

L'idée est la suivante : on va démontrer le théorème d'Ax dans des cas simples de corps $\mathbf{K}$ puis le déduire sur $\mathbf{C}$ par un théorème de transfert.

Tout d'abord, trouvons des corps qui vérifient le théorème d'Ax.

6.1.1 Les corps finis et localement finis

Les corps finis vérifient trivialement le théorème d'Ax. En effet soit $\mathbf{K}$ un corps fini, alors toute application injective de $\mathbf{K}^n$ dans $\mathbf{K}^n$ est surjective.

Définition 6.1 *On appelle* ***corps localement fini*** *tout corps* $\boldsymbol{K}$ *tel que tout sous-corps finiment engendré de* $\boldsymbol{K}$ *(ie engendré par une partie finie) est fini.*

On peut remarquer qu'un tel corps est nécessairement de caractéristique non nulle car sinon son sous-corps $\mathbf{Q}$, engendré par 1, serait fini.

Théorème 6.2 *Les corps localement finis vérifient le théorème d'Ax.*

preuve : Soit $f = (f_1, \ldots, f_n)$ une application polynômiale injective de $\mathbf{K}^n$ dans $\mathbf{K}^n$ et $a = (a_1, \ldots, a_n)$ un élément de $\mathbf{K}^n$. Soit alors $\mathbf{K}_0$ le sous-corps de $\mathbf{K}$ engendré par les a_i et les coefficients des polynômes f_i. $\mathbf{K}_0$ est fini. Considérons la restriction f' de f à $\mathbf{K}_0^n$. Comme pour tout i, $f_i \in \mathbf{K}_0[X]$, on a $f'(\mathbf{K}_0^n) \subset \mathbf{K}_0^n$, et l'application f' étant injective sur un ensemble fini, est surjective. Donc a est dans l'image de f.

6.1.2 Clôture algébrique des $\mathbf{F}_\mathrm{p}$

On rappelle la notation $\mathbf{F}_{p^n}$ qui désigne l'unique corps (à isomorphisme près) de cardinal p^n.

Il existe une extension de $\mathbf{F}_p$ qui est algébrique sur $\mathbf{F}_p$ et algébriquement close. Cette extension, unique à isomorphisme près, est appelée clôture algébrique et est notée $\overline{\mathbf{F}_p}$.

$\overline{\mathbf{F}_p}$ est la réunion des $\mathbf{F}_{p^n}$ et on a $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$ ssi n divise m. Donc $\overline{\mathbf{F}_p}$ est la réunion croissante des $\mathbf{F}_{p^{n!}}$.

On en déduit que si $a_1, \ldots, a_p$ est une famille finie d'éléments de $\overline{\mathbf{F}_p}$, il existe un entier N tel que les a_i sont tous dans $\mathbf{F}_{p^{N!}}$, donc le sous-corps qu'ils engendrent est fini.

Les $\overline{\mathbf{F}_p}$ sont donc localement finis, puis vérifient le théorème d'Ax.

6.1.3 Les théorèmes de transfert

A ce stade, la théorie des modèles permet de conclure par le théorème de transfert suivant :

Théorème 6.3 *Si une propriété qui s'exprime par un « énoncé du premier ordre » est vraie dans la clôture algébrique de* $\boldsymbol{F}_p$ *pour tout p premier, elle est vraie dans* $\boldsymbol{C}$*.*

Dans cette présentation nous allons introduire les outils de théorie des modèles qui permettent de démontrer ce théorème. Il nous faudra en particulier définir la notion d'*énoncé du premier ordre* et vérifier que le théorème d'Ax correspond bien à ce type d'énoncé.

6.2 Les formules du premier ordre pour le langage des anneaux

6.2.1 Définition de l'ensemble des formules

R est un **anneau commutatif** muni de l'addition $+ : R \times R \to R$ et de la multiplication $\times : R \times R \to R$.

Définition 6.2 *L'ensemble des* ***formules atomiques*** $\mathcal{F}_0$ *:*
ce sont toutes les formules de la forme $P(x_1, ..., x_n) = Q(x_1, ..., x_n)$ *où* P *et* Q *sont des polynômes dans* $\mathbb{Z}[X_1, ...X_n]$

Définition 6.3 *On dit que la variable* x_i *est* ***libre*** *dans la formule* ϕ*, de la forme* $P(x_1, ..., x_n) = Q(x_1, ..., x_n)$*, ssi* x_i *est de degré* ≥ 1 *dans l'un des deux polynômes* P *ou* Q*.*

Pour une formule ϕ de $\mathcal{F}_0$, on écrit $\phi(x_1, ..., x_n)$ pour indiquer que les variables libres dans ϕ sont parmi les $x_1, ..., x_n$.

Définition 6.4 *Pour* $\phi(x_1, ..., x_n)$ *dans* $\mathcal{F}_0$*, on dit que* R ***satisfait*** *la formule* $\phi(a_1, ...a_n)$*, ou que la suite* $a_1, ..., a_n$ *satisfait la formule* $\phi(x_1, ..., x_n)$ *dans* R*, ssi dans* R *on a* $P(a_1, ..., a_n) = Q(a_1, ..., a_n)$*. On note* $R \models \phi(a_1, ..., a_n)$

Définition 6.5 $\phi \in \mathcal{F}_{n+1}$ *ssi :*
- *soit* $\phi \in \mathcal{F}_n$
- *soit* ϕ *est de la forme* $(\phi_1 \wedge \phi_2)$ *pour* $\phi_1, \phi_2 \in \mathcal{F}_n$
- *soit* ϕ *est de la forme* $(\phi_1 \vee \phi_2)$ *pour* $\phi_1, \phi_2 \in \mathcal{F}_n$
- *soit* ϕ *est de la forme* $\neg\psi$ *pour* $\psi \in \mathcal{F}_n$
- *soit* ϕ *est de la forme* $\exists x\psi$ *pour* $\psi \in \mathcal{F}_n$
- *soit* ϕ *est de la forme* $\forall x\psi$ *pour* $\psi \in \mathcal{F}_n$
- *On dit que* x *est une* ***variable libre*** *de* $(\phi_1 \wedge \phi_2)$*, ou de* $(\phi_1 \vee \phi_2)$*, ssi* x *est une variable libre de* ϕ_1 *ou si* x *est une variable libre de* ϕ_2*.*
- x *est une* ***variable libre*** *de* $\neg\psi$ *ssi* x *est une variable libre de* ψ*.*
- x *est une* ***variable libre*** *de* $\exists y\psi$*, ou de* $\forall y\psi$*, ssi* x *est une variable libre de* ψ*, mais* x *n'est* ***jamais*** *une variable libre de* $\exists x\psi$*, ni de* $\forall x\psi$*.*

Définition 6.6 ***Satisfaction*** *d'une formule* $\phi \in \mathcal{F}_{n+1}$ *: soit* $a_1, ..., a_n \in R$*, on a :*
- $R \models \phi_1 \wedge \phi_2(a_1, ..., a_n)$ *ssi* $R \models \phi_1(a_1, ..., a_n)$ *et* $R \models \phi_2(a_1, ..., a_n)$
- $R \models \phi_1 \vee \phi_2(a_1, ..., a_n)$ *ssi* $R \models \phi_1(a_1, ..., a_n)$ *ou* $R \models \phi_2(a_1, ..., a_n)$
- $R \models \neg\phi_1(a_1, ..., a_n)$ *ssi* R *ne satisfait pas* $\phi_1(a_1, ..., a_n)$*, noté* $R \not\models \phi_1(a_1, ..., a_n)$
- $R \models \exists y\psi(y, a_1, ..., a_n)$ *ssi il existe* $b \in R$ *tel que* $R \models \psi(b, a_1, ..., a_n)$
- $R \models \forall y\psi(y, a_1, ..., a_n)$ *ssi pour tout* $b \in R$*, on a* $R \models \psi(b, a_1, ..., a_n)$

Définition 6.7 *L'ensemble des* ***formules du premier ordre*** $\mathcal{F}orm := \bigcup_{n\geq 0} \mathcal{F}_n$

Définition 6.8 *La* ***complexité*** *d'une formule du premier ordre* ϕ *est l'unique* n *tel que* $\phi \in \mathcal{F}_n$ *et* $\phi \notin \mathcal{F}_m$ *pour* $m < n$*.*

Cette notion nous permettra de démontrer des résultats (comme le lemme suivant) par **induction** sur la complexité des formules du premier ordre.

Lemme 3 *Si* f *est un isomorphisme (d'anneau) de* R *sur* R*', si* $\phi(x_1, ..., x_n)$ *est une formule, alors pour tous* $a_1, ..., a_n \in R$*,*

$$R \models \phi(a_1, ..., a_n) \text{ ssi } R' \models \phi(f(a_1), ..., f(a_n))$$

6.2.2 Exemples, théories et modèles

Définition 6.9 *Une formule sans variable libre est appelée un* ***énoncé****. Si l'anneau R satisfait l'énoncé θ, on dira que R est un* ***modèle*** *de θ. Si Σ est un ensemble d'énoncés et si R est modèle de chacun des énoncés de Σ, on dira que R est modèle de Σ, noté $R \models \Sigma$. Un ensemble (éventuellement infini) d'énoncés qui a un modèle sera appelé* ***une théorie****.*

Exemple : Les modèles de l'énoncé $\Theta_c := \forall x(x = 0) \vee (\exists x.y = 1)$ sont exactement les anneaux commutatifs qui sont des corps.

Si p est un nombre premier, les modèles de l'énoncé $\sigma_p := (p = 0)$ sont exactement les anneaux commutatifs de caractéristique p.

Les modèles de l'énoncé « $(\Theta_c \wedge \sigma_p)$ » sont exactement les corps de caractéristique p.

La théorie $\Sigma_0 = \{\neg\sigma_p \text{ , } p \text{ premier}\}$ a pour modèles tous les anneaux de caractéristique zéro.

6.2.3 Théorie des corps algébriquement clos, théorème d'Ax

Il existe une théorie, c'est à dire un ensemble (infini) d'énoncés, dont les modèles sont exactement les corps algébriquement clos.
Soit $n \geq 1$ un entier fixé, on peut écrire un énoncé, θ_n, dont les modèles sont exactement les anneaux p tels que tout polynôme unitaire de degré n à coefficients dans R a une solution dans R :

$$\forall y_0 \cdots \forall y_{n-1} \exists x \, (x^n + \sum_{i=0}^{n-1} y_i.x^i) = 0$$

Les corps algébriquement clos sont alors exactement les modèles de la théorie

$$T_{CAC} := \{\theta_C\} \cup \{\theta_n; n \geq 1\}.$$

Enfin, il nous faut vérifier que le théorème d'Ax s'énonce par une infinité d'énoncés du premier ordre.
Nous allons exprimer, par une formule $J_{n,d}$, que pour n et d fixés, toute application polynômiale de R^n dans R^n, de degré indérieur ou égal à d, qui est injective, est surjective. Comme précédemment il va falloir quantifier sur les coefficients des polynômes, pour dire « pour tout polynôme de degré inférieur ou égal à d ». On l'écrit ici dans un cas simple $f = (f_1, f_2)$, application de degré inférieur ou égal à 2 de $\mathbf{C}^2$ dans $\mathbf{C}^2$.
On a $f_1(x_1, x_2) = \sum_{i+j=2} y_{ij} x_1^i x_2^j$ et $f_2(x_1, x_2) = \sum_{i+j=2} z_{ij} x_1^i x_2^j$.
Soit $I(\bar{y}, \bar{z})$ la formule :

$$\forall x_1 \forall x_2 \forall x_1' \forall x_2' [((\sum_{i+j=2} y_{ij} x_1^i x_2^j = \sum_{i+j=2} y_{ij} {x_1'}^i {x_2'}^j) \wedge$$

$$(\sum_{i+j=2} z_{ij} x_1^i x_2^j = \sum_{i+j=2} z_{ij} {x_1'}^i {x_2'}^j)) \rightarrow (x_1 = x_1' \wedge x_2 = x_2')].$$

Alors $R \models I(\bar{y}, \bar{z})$ ssi f est injective.
Soit $S(\bar{y}, \bar{z})$ la formule :

$$\forall v \forall w \exists x_1 \exists x_2 ((\sum_{i+j=2} y_{ij} {x_1}^i {x_2}^j = v) \wedge (\sum_{i+j=2} z_{ij} {x_1}^i {x_2}^j = w)).$$

Alors $R \models S(\bar{y}, \bar{z})$ ssi f est surjective.
Maintenant soit

$$J_{2,2} := (\forall \bar{y} \forall \bar{z} (I(\bar{y}, \bar{z}) \rightarrow S(\bar{y}, \bar{z}))).$$

Alors $R \models J_{2,2}$ si et seulement si toute application polynômiale de degré inférieur ou égal à 2, de R^2 dans R^2, qui est injective, est surjective.

6.3 Ultraproduits

6.3.1 Filtres et ultrafiltres

Notre but dans cette section est de montrer le Théorème de Los sur lequel la preuve du Théorème d'Ax est basée. Pour cela nous allons construire des structures appelées filtres et ultrafiltres.

Définition 6.10 *Soit I un ensemble non vide, un filtre $\mathcal{F}$ sur I est un sous-ensemble de $\mathcal{P}(I)$ tel que :*
- *$I \in \mathcal{F}$ et $\emptyset \notin \mathcal{F}$*
- *si $X \in \mathcal{F}$ et $Y \in \mathcal{F}$ alors $Y \cap X \in \mathcal{F}$*
- *si $X \in \mathcal{F}$ et $X \subset Z \subset I$ alors $Z \in \mathcal{F}$*

Exemples : 1) Filtre principal Si $\emptyset \neq X_0 \subset I$, $\mathcal{F}_{X_0} := \{Y \subset I; X_0 \subset Y\}$ est un filtre appelé filtre principal.
2) Filtre de Fréchet Si I est un ensemble infini, $\mathcal{FR} := \{X \subset I; X^c \, est fini\}$ est un filtre appelé filtre de Fréchet.

Définition 6.11 *Un filtre $\mathcal{U}$ est appelé ultrafiltre ssi $\forall X \subset I$, soit $X \in \mathcal{U}$, soit $X^c \in \mathcal{U}$.*

Propriété :
Tout filtre est contenu dans un ultrafiltre.

6.3.2 Notations et rappels

Maintenant nous allons fixer quelques notations et faire des rappels sur le produit cartésien des anneaux. Soit $(R_i)_{i \in I}$ une famille d'anneaux commutatifs et R un ultrafiltre sur I. On note $R = \prod_{i \in I} R_i$ le produit cartésien des anneaux R_i, un élément $a \in R$ sera noté $a = (a(i))_{i \in I}$, où $a(i) \in R_i$ est la i-ième coordonnée de a. On rappelle que $\prod_{i \in I} R_i$ est un anneau commutatif lorsque on définit l'addition et la multiplication coordonnées par coordonnées :

$$a + b(i) = a(i) + b(i)$$

$$a \cdot b(i) = a(i) \cdot b(i)$$

avec $1 = (1, \ldots, 1)$ et $0 = (0, \ldots, 0)$.
Si $P(x_1, \ldots, x_n)$ est un polynôme dans $\mathbf{Z}[X_1, \ldots, X_n]$ et $a_1, \ldots, a_n$ éléments de R, on a d'après l'addition et multiplication que nous avons definies, que la coordonnée i-ième de $P(a_1, \ldots, a_n)$ est donnée par :

$$P(a_1, \ldots, a_n)(i) = P(a_1(i), \ldots, a_n(i))$$

6.3.3 Relation d'équivalence

Définition 6.12 *Avec les notations précédentes, on définit $\equiv_{\mathcal{U}}$ comme la relation suivante :*

$$\forall a, b \in R, a \equiv_{\mathcal{U}} b \Leftrightarrow \{i \in I; a(i) = b(i)\} \in U$$

Le fait que $\mathcal{U}$ soit un filtre permet de vérifier que $\equiv_{\mathcal{U}}$ est bien une relation d'équivalence. On notera la classe d'équivalence de $a \in R$ par $a_{\mathcal{U}}$.

6.3.4 Ultraproduits

Définition 6.13 *On appelle l'ultraproduit des R_i (par $\mathcal{U}$) l'ensemble des classes d'équivalence de R par $\equiv_{\mathcal{U}}$ et on le note $R/\mathcal{U}$. $R/\mathcal{U}$ est naturellement doté d'une structure d'anneau commutatif où les opérations sont définies par classes :*

$$\bar{a} + \bar{b} := \bar{c} \Leftrightarrow \{i \in I; a(i) + b(i) = c(i)\} \in U$$

et

$$\bar{a} \cdot \bar{b} := \bar{c} \Leftrightarrow \{i \in I; a(i) \cdot b(i) = c(i)\} \in U$$

Proposition 6.1 *$R/\mathcal{U}$ est un anneau commutatif.*

preuve : Soit $\star$ l'addition ou la multiplication dans l'anneau R. Nous allons montrer que $\equiv_{\mathcal{U}}$ et $\star$ sont compatibles. Soient $a \equiv_{\mathcal{U}} a'$ et $b \equiv_{\mathcal{U}} b'$ et

$$J = \{i \in I;\ a(i) = a'(i)\}$$

$$J' = \{i \in I;\ b(i) = b'(i)\}$$

$$K = \{i \in I;\ a'(i) \star b'(i) = a(i) \star b(i)\}$$

Par définition on a que J et $J' \in \mathcal{U}$, donc $J \cap J' \in \mathcal{U}$ car $\mathcal{U}$ est stable par intersection. De plus $J \cap J' \subset K$ d'où on déduit que $K \in \mathcal{U}$ et donc $a \star b \equiv_{\mathcal{U}} a' \star b'$.

Maintenant nous sommes en mesure d'énoncer et de montrer le Théorème de Los :

6.3.5 Théorème de Los

Soit $(R_i)_{i \in I}$ une famille d'anneaux commutatifs et $\mathcal{U}$ un ultrafiltre sur I.
Si $\phi(x_1, ..., x_n)$ est une formule du premier ordre et $a_1, \ldots, a_n \in R = \prod_{i \in I} R_i$, alors

$$R/\mathcal{U} \models \phi(a_{1_{\mathcal{U}}}, \ldots, a_{n_{\mathcal{U}}}) \ ssi \ \{i \in I;\ R_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$$

Ce qui veut dire que $R/\mathcal{U}$ satisfait la formule ϕ évaluée dans les classes d'équivalence $a_{k_{\mathcal{U}}}$ si et seulement si l'ensemble des i tels que R_i satisfait la formule ϕ évaluée dans les coordonées i-ièmes des a_k, appartient à l'ultrafiltre $\mathcal{U}$.

preuve : La preuve consiste en une induction sur la complexité des formules.
Pour les formules de complexité zéro, on a que $\phi \in \mathcal{F}_0$ ssi ϕ est de la forme $P(x_1, ..., x_n) = Q(x_1, ..., x_n)$, donc :

$$R/\mathcal{U} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) \Leftrightarrow P(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) = Q(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$$

d'après la définition des opérations sur les classes on a que :

$$P(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) = Q(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) \Leftrightarrow P(a_1, \ldots, a_n)_\mathcal{U} = Q(a_1, \ldots, a_n)_\mathcal{U}$$

ce qui veut dire que $P(a_1, ..., a_n)$ et $Q(a_1, ..., a_n)$ appartient à la même classe d'équivalence, donc on a que :

$$\{i \in I;\ P(a_1, ..., a_n)(i) = Q(a_1, ..., a_n)(i)\} \in \mathcal{U}$$

La condition ci-dessus est équivalente à :

$$\{i \in I;\ P(a_1(i), ..., a_n(i)) = Q(a_1(i), ..., a_n(i))\} \in \mathcal{U}$$

qui est, par la définition de la satisfaction d'une formule, équivalente à :

$$\{i \in I;\ R_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$$

Soit maintenant $\phi \in \mathcal{F}_{n+1}$, on sait que ϕ est soit la conjonction ou disjonction de deux formules de complexité n, soit la négation d'une formule de complexité n ou soit la quantification universelle ou existentielle d'une formule de complexité n. Nous allons traiter le cas de la conjonction.
Soit $\phi = \phi_1 \wedge \phi_2$ avec $\phi_1, \phi_2 \in \mathcal{F}_n$. Par définition de la conjonction on a que

$$R/\mathcal{U} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$$
$$\Leftrightarrow R/\mathcal{U} \models \phi_1(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) \textit{ et } R/\mathcal{U} \models \phi_2(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$$

Les formules ϕ_1 et ϕ_2 étant de complexité n, elles satisfont l'hypothèse inductive, donc :

$$R/\mathcal{U} \models \phi_1(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) \textit{ et } R/\mathcal{U} \models \phi_2(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$$
$$\Leftrightarrow S_{1,2} := \{i \in I;\ R_i \models \phi_{1,2}(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$$

$\mathcal{U}$ est un ultrafiltre donc

$$S_1, S_2 \in \mathcal{U} \Leftrightarrow S_1 \cap S_2 \in \mathcal{U}$$

et par définition de S_1 et S_2 on trouve :

$$S_1 \cap S_2 \in \mathcal{U} \Leftrightarrow \{i \in R\,; R_i \models (\phi_1(a_1(i), \ldots, a_n(i)) \textit{ et } \phi_2(a_1(i), \ldots, a_n(i)))\} \in \mathcal{U}$$

finalement en utilisant à nouveau la définition de la conjonction on trouve que :

$$\{i \in R\,; R_i \models (\phi_1(a_1(i), \ldots, a_n(i)) \textit{ et } \phi_2(a_1(i), \ldots, a_n(i)))\} \in \mathcal{U}$$
$$\Leftrightarrow \{i \in R\,; \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$$

Ce que nous voulions démontrer.
Les preuves pour les autres cas sont analogues sauf pour celui de la négation où il faut utiliser la propriété de maximalité des ultrafiltres pour l'inclusion.

6.4 Élimination des quantificateurs et complétude de la Théorie de corps algébriquement clos

6.4.1 Élimination des quantificateurs

Soit ϕ une formule. On dira que ϕ est **sans quantificateur** si elle ne contient ni le symbole $\exists$, ni le symbole $\forall$. Ainsi, l'ensemble des formules sans quantificateurs est donc la clôture de l'ensemble des formules atomiques par négation et par conjonction. Soient T une théorie et θ est un énoncé, on dira que θ est une **conséquence** de T, et on le notera $T \vdash \theta$, si pour tout anneau R modèle de T, R est modèle de θ aussi. On dira que T **admet l'élimination des quantificateurs** ssi pour toute formule $\phi(x_1, \ldots, x_n)$, il existe une formule sans quantificateurs $\theta(x_1, \ldots, x_n)$ (avec la même quantité de variables) telle que

$$T \vdash \forall x_1, \ldots, \forall x_n(\phi(x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n))$$

Étant donnés une formule $\phi(x_1, \ldots, x_n)$ quelconque et un anneau R qui satisfait $\phi(a_1, ..., a_n)$ pour $a_1, ..., a_n$ éléments de R, il n'est pas forcément vrai que tout sous-anneau de R contenant les $a_1, ..., a_n$ satisfait aussi la formule $\phi(a_1, ..., a_n)$. Par exemple si on prend $\phi(x) = (\exists y\, y^2 = x)$ on sait que $\mathbf{R} \models \phi(2)$ mais $\mathbf{Q} \models \neg\phi(2)$ ou encore $\mathbf{C} \models \phi(-1)$ mais $\mathbf{R} \models \neg\phi(-1)$.

Le lemme suivant dit que pour le cas spécial des formules sans quantificateurs, la satisfaction de $\phi(a_1, ..., a_n)$ par un anneau ne dépend pas du sous-anneau où se trouvent les $a_1, ..., a_n$.

Lemme 4 *Si $\phi(x_1, \ldots, x_n)$ est une formule sans quantificateurs, R_2 un anneau, R_1 un sous-anneau de R_2 et $a_1, \ldots, a_n \in R_1$, alors*

$$R_1 \models \phi(a_1, ..., a_n) \text{ ssi } R_2 \models \phi(a_1, \ldots, a_n)$$

preuve : Induction sur la complexité des formules. La propriété est claire pour les formules d'ordre zéro (qui sont des égalités polynômiales) et elle reste vraie par disjonction et par négation (puis par conjonction aussi).

La proposition suivante dit que T élimine les quantificateurs d'une formule si et seulement si la satisfaction de cette formule est invariante par isomorphisme des modèles de T. Elle est, dans une certaine mesure, la réciproque du lemme précédent.

Proposition 6.2 *Soient T une théorie et $\phi(x_1, \ldots, x_n)$ une formule, les deux propriétés suivantes sont équivalentes :*

- *(i) $\exists\, \theta(x_1, \ldots, x_n)$ sans quantificateurs telle que*

$$T \vdash \forall x_1, \ldots, \forall x_n[\phi(x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n)]$$

- *(ii) Pour tous R_1, R_2 anneaux commutatifs modèles de T, pour tous S_1, S_2 sous-anneaux de R_1, R_2, pour tout isomorphisme d'anneau $f : S_1 \to S_2$, pour tous $a_1, \ldots, a_n \in S_1$*

$$S_1 \models \phi(a_1, ..., a_n) \text{ ssi } S_2 \models \phi(f(a_1), \ldots, f(a_n))$$

La preuve de cette proposition étant assez technique, on se réfère à [2].

Maintenant on donne un lemme qui affirme que pour obtenir l'élimination des quantificateurs il suffit d'éliminer le quantificateur existentiel, ce qui ne surprend pas si on se souvient de l'équivalence $\forall x \phi(x)$ ssi $\neg(\forall x \neg \phi(x))$.

Lemme 5 *Soit T une théorie, si pour toute formule $\phi(y, x_1, \ldots, x_n)$ sans quantificateurs, il existe une formule sans quantificateurs $\theta(x_1, \ldots, x_n)$ telle que :*

$$T \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \phi(y, x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n))$$

alors T admet l'élimination des quantificateurs.

preuve : Induction sur la complexité des formules. Si $\phi(y, x_1, \ldots, x_n)$ est de complexité zéro, elle est déjà sans quantificateurs car elle est une formule atomique. Supposons la propriété vraie pour les formules de complexité k et soit $\phi(x_1, \ldots, x_n)$ de complexité $k+1$. On distingue les cinq cas possibles :

- Si $\phi(y, x_1, \ldots, x_n)$ est la négation d'une formule $\psi(y, x_1, \ldots, x_n)$ de complexité k on a par l'hypothèse d'induction qu'il existe une formule $\theta(y, x_1, \ldots, x_n)$ telle que :

  $$T \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \psi(y, x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n))$$

  La negation de $\theta(y, x_1, \ldots, x_n)$ est aussi sans quantificateurs et elle est équivalente à $\phi(y, x_1, \ldots, x_n)$, c-à-d :

  $$T \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \phi(y, x_1, \ldots, x_n) \leftrightarrow \neg\varphi(x_1, \ldots, x_n))$$

- Si $\phi(x_1, \ldots, x_n)$ est de la forme $\psi(x_1, \ldots, x_n) = \forall y \psi(y, x_1, \ldots, x_n)$ avec $\psi(y, x_1, \ldots, x_n)$ de complexité k on a que d'après l'hypothèse d'induction il existe une formule $\varphi(y, x_1, \ldots, x_n)$ sans quantificateurs telle que

  $$T \vdash \forall y \forall x_1, \ldots, \forall x_n (\psi(y, x_1, \ldots, x_n) \leftrightarrow \varphi(y, x_1, \ldots, x_n))$$

  et donc que

  $$T \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \exists y \psi(y, x_1, \ldots, x_n) \leftrightarrow \exists y\, \varphi(x_1, \ldots, x_n))$$

  Comme $\varphi(x_1, \ldots, x_n)$ est sans quantificateurs on peut lui appliquer l'hypothèse du lemme et on a qu'il existe une formule sans quantificateurs $\theta(x_1, \ldots, x_n)$ qui lui est équivalente. On en déduit que :

  $$T \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \phi(y, x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n))$$

- Si ϕ est la conjonction de deux formules $\phi = \phi_1 \vee \phi_2$ avec ϕ_1 et ϕ_2 de complexité inférieure ou égale à k la propriété est claire car par induction ϕ_1 (ϕ_2) est équivalente à une formule sans quantificateurs φ_1 (φ_2) et donc ϕ est équivalente à $\varphi_1 \vee \varphi_2$ qui reste sans quantificateurs.
- Le cas de la disjonction est analogue à celui de la conjonction.
- Le cas de $\phi(y, x_1, \ldots, x_n) = \forall y\, \psi(y, x_1, \ldots, x_n)$ est déduit du fait que $\forall x\, \psi(y, x_1, \ldots, x_n)$ *ssi* $\neg(\forall x\, \neg\psi(y, x_1, \ldots, x_n))$.

Théorème 6.4 *La théorie des corps algébriquement clos T_{CAC} admet l'élimination des quantificateurs dans le langage des anneaux.*

preuve : D'après le lemme précédent il suffit de montrer que T_{CAC} élimine le quantificateur existentiel pour prouver qu'elle admet l'élimination des quantificateurs. Dans cet esprit, on montrera que T_{CAC} satisfait bien les hypothèses du lemme 2.

Soit $\phi(y, x_1, \ldots, x_n)$ une formule sans quantificateurs, comme elle appartient à la clôture de l'ensemble des formules atomiques par négation $\neg$ et par conjonction $\wedge$ elle est équivalente à :

$$(\wedge_{1\leq i\leq m} P_i(y, x_1, \ldots, x_n) = 0\,) \wedge (Q(y, x_1, \ldots, x_n) \neq 0)$$

On peut donc supposer que

$$\phi(y, x_1, \ldots, x_n) = (P(y, x_1, \ldots, x_n) = 0) \wedge (Q(y, x_1, \ldots, x_n) \neq 0)$$

Or on doit montrer qu'il existe une formule sans quantificateurs équivalente à $\exists y\, \phi(y, x_1, \ldots, x_n)$. Pour faire cela on vérifiera que T_{CAC} et $\exists y\, \phi(y, x_1, \ldots, x_n)$ satisfont (ii) de la proposition 2
Soient $K_1(K_2)$ corps algébriquement clos (i.e : un modèle de T_{CAC}) et $R_1(R_2)$ un anneau commutatif contenu dans $K_1(K_2)$. Soit $f : R_1 \to R_2$ un isomorphisme d'anneau. Soient T_1 le corps de fractions de R_1 et L_1 la clôture algébrique de T_1 qui est contenue dans K_1 (de même pour R_2).
D'après le Théorème des plongements f se prolonge en un isomorphisme $f : L_1 \to L_2$. Soient $a_1, \ldots, a_n$ éléments de R_1 et supposons que $K_1 \models \exists y\, \phi(y, x_1, \ldots, x_n)$, il existe donc $b \in K_1$ tel que

$$P(b, a_1, \ldots, a_n) = 0 \wedge Q(b, a_1, \ldots, a_n) \neq 0$$

On distingue deux cas :

- Si $P(x, a_1, \ldots, a_n) \equiv 0$ alors par isomorphisme $P(x, f(a_1), \ldots, f(a_n)) \equiv 0$ puis $P(f(b), f(a_1), \ldots, f(a_n)) = 0$. D'ailleurs, $Q(x, a_1, \ldots, a_n) \not\equiv 0$ donc le polynôme $Q(x, f(a_1), \ldots, f(a_n)) \in R_2[X]$ n'est pas nul et il a un nombre fini de racines dans K_2. Ce dernier étant infini (il est algébriquement clos) $\exists\, c \in K_2$ tel que $Q(c, a_1, \ldots, a_n) \neq 0$. On a prouvé que $K_2 \models \exists y\, \phi(y, x_1, \ldots, x_n)$.
- Si $P(x, a_1, \ldots, a_n) \not\equiv 0$, alors b est algébrique sur R_1 puis $b \in L_1$. L_1 étant isomorphe à L_2 on a que $P(f(b), f(a_1), \ldots, f(a_n)) = 0$
  et que $Q(f(b), f(a_1), \ldots, f(a_n)) \neq 0$. Ce qui prouve $K_2 \models \exists y\, \phi(y, x_1, \ldots, x_n)$.

On a montré que $K_1 \models \exists y\, \phi(y, x_1, \ldots, x_n)\, ssi\, K_2 \models \exists y\, \phi(y, x_1, \ldots, x_n)$ et par symétrie que

$$K_1 \models \exists y\, \phi(y, x_1, \ldots, x_n)\, ssi\, K_2 \models \exists y \phi(y, x_1, \ldots, x_n)$$

c-à-d : T_{CAC} et $\exists y \phi(y, x_1, \ldots, x_n)$ satisfont (ii) de la proposition 2. On en déduit qu'il existe $\theta(x_1, \ldots, x_n)$ sans quantificateurs telle que

$$T_{CAC} \vdash \forall x_1, \ldots, \forall x_n (\exists y\, \phi(y, x_1, \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n))$$

Étant donnée $\phi(y, x_1, \ldots, x_n)$ n'importe quelle formule on a bien montré que T_{CAC} satisfait les hypothèses de la proposition 2, i.e : T_{CAC} admet l'élimination des quantificateurs.

Note sur la notion de langage
Tout ce qu'on a fait dans ce chapitre peut être traité d'une façon plus abstraite, en considérant un langage quelconque à la place du langage des anneaux. Un langage est un ensemble de symboles (symboles de fonction, symboles de relation et symboles constants) qui « modélise » une structure mathématique. On parle du « langage des groupes », du « langage des graphes » et en particulier du « langage des anneaux » qui est $\{+, -, ., 0, 1\}$, où $+$, $-$ et $.$ sont symboles de fonction et 0 et 1 sont symboles constants. D'une façon approximative, une formule dans un langage est une expression obtenue à partir des symboles de relation et des symboles constants en appliquant les symboles de fonctions et les symboles logiques usuels $(\vee, \wedge, \neg, (,), =, \forall, \exists, x, y, z, etc.)$. Par exemple, dans le langage des anneaux une formule atomique est une égalité de polynômes à coefficients dans $\mathbf{Z}$. Le fait que la théorie des corps algébriquement clos T_{CAC} admette l'élimination des quantificateurs dans le langage des anneaux veut dire qu'elle élimine les quantificateurs des formules construites à partir de l'ensemble de symboles $\{+, -, ., 0, 1\}$.

6.4.2 Complétude de la Théorie des corps algébriquement clos de caractéristique fixée

Définition 6.14 *Deux anneaux commutatifs R_1 R_2 sont **élémentairement équivalents** ssi pour tout énoncé σ*

$$R_1 \models \sigma \; ssi \; R_2 \models \sigma$$

*Une Théorie est **complète** ssi tous ses modèles sont élémentairement équivalents*

Théorème 11 (Complétude de la Théorie des corps algébriquement clos de caractéristique fixée)
Deux corps algébriquement clos sont élémentairement équivalents ssi ils ont la même caractéristique.

preuve : La caractéristique d'un corps est définie par l'énoncé $\sigma =$ "$p = 0$" donc, si deux corps corps sont élémentairement équivalents ils ont la même caractéristique. Réciproquement, soient K_1 et K_2 sont deux corps algébriquement clos de même caractéristique, disons p (avec p un nombre premier ou nul). Chacun de ces corps contient une copie du corps k_p engendré par 1. Soit σ un énoncé tel que $K_1 \models \sigma$. La théorie des corps algébriquement clos admettant l'élimination des quantificateurs, on a qu'il existe une formule θ sans quantificateurs telle que $T_{CAC} \vdash (\sigma \leftrightarrow \theta)$. Par ailleurs, d'après le lemme 2 on a que $K_1(K_2) \models \theta \; ssi \; k_p \models \theta$. On en déduit que : $K_1 \models \sigma \; ssi \; K_1 \models \theta \; ssi \; k_p \models \theta \; ssi \; K_2 \models \theta \; ssi \; K_2 \models \sigma$.

6.4.3 Démonstration du théorème de transfert et du théorème d'Ax

Les preuves du théorème de transfert et du théorème d'Ax que nous allons donner ici, reposent sur l'utilisation du théorème de Los et sur la complétude de la Théorie des corps algébriquement clos de caractéristique fixée.

Démonstration du théorème de transfert
Rappelons d'abord le théorème :

Théorème 3
Si une propriété qui s'exprime par un « énoncé du premier ordre » est vraie dans la clôture algébrique de $\boldsymbol{F}_p$ pour tout p premier, elle est vraie dans $\boldsymbol{C}$.

preuve : Définissons pour cela l'ultraproduit suivant. On note P l'ensemble des nombres premiers et soit $\mathcal{U}$ un ultrafiltre non principal sur P, ie un ultrafiltre contenant le filtre de Fréchet sur P. Alors $\mathcal{U}$ contient toutes les parties de P de complémentaire fini. On pose alors $K_p = \overline{\mathbf{F}_p}$ et on définit $K = \prod_{p\in P} K_p$. Quelles sont les propriétés de K ?

(i) K est un corps. En effet, on a vu que l'anneau R était un corps ssi il satisfait à l'énoncé $\theta_c = \forall x(x = 0) \vee (\exists y\ x * y = 1)$. Cet énoncé étant satisfait par tous les K_p, par le théorème de Los,K satisfait θ_c.

(ii) K est de caractéristique 0. Il suffit de montrer que pour tout p premier, K satisfait à l'énoncé $\neg\sigma_p = \neg(p = 0)$. Or, cet énoncé est vrai pour tout K_q où $q \in P - \{p\}$. Et $P - \{p\} \in U$. Donc par le théorème de Los, pour tout p premier, on a $p \neq 0$ dans K donc K est de caractéristique nulle.

(iii) K est algébriquement clos. En effet on a vu qu'il suffisait que K satisfasse pour tout n un certain énoncé θ_n. Or cet énoncé est satisfait par tous les K_p, donc par K. K est algébriquement clos.

Donc par le théorème de Los, si un énoncé du premier ordre est vérifié par tous les $\overline{F_p}$, il est vérifié par K. Ce dernier étant un corps algébriquement clos de caractéristique nulle il est élémentairement équivalent à $\mathbf{C}$, donc tout énoncé du premier ordre vérifié par K est vérifié par $\mathbf{C}$ aussi. Nous avons démontré le théorème de transfert.

Démonstration du théorème d'Ax
Dans la section 2 de ce chapitre nous avons montré que le théorème d'Ax s'énonce par une infinité d'énoncés du premier ordre. Chacun de ces énoncés étant vrai dans la clôture algébrique de $\mathbf{F}_p$ pour tout p premier, d'après le théorème de transfert il sont vérifiés par $\mathbf{C}$ aussi. Nous avons démontré le théorème d'Ax.

Chapitre 7

Une porte doit être ouverte et fermée

« Crois et tu comprendras ; la foi précède, l'intelligence suit. »
Saint Augustin

7.1 Les enjeux de l'informatique quantique

La puissance de calcul des ordinateurs augmente depuis 35 ans avec une régularité spectaculaire. Cette puissance est directement liée aux progrès technologiques constants réalisés dans le domaine de la miniaturisation des composants électroniques : comme l'illustre la loi de Moore, leur taille diminue de manière exponentielle au cours du temps.

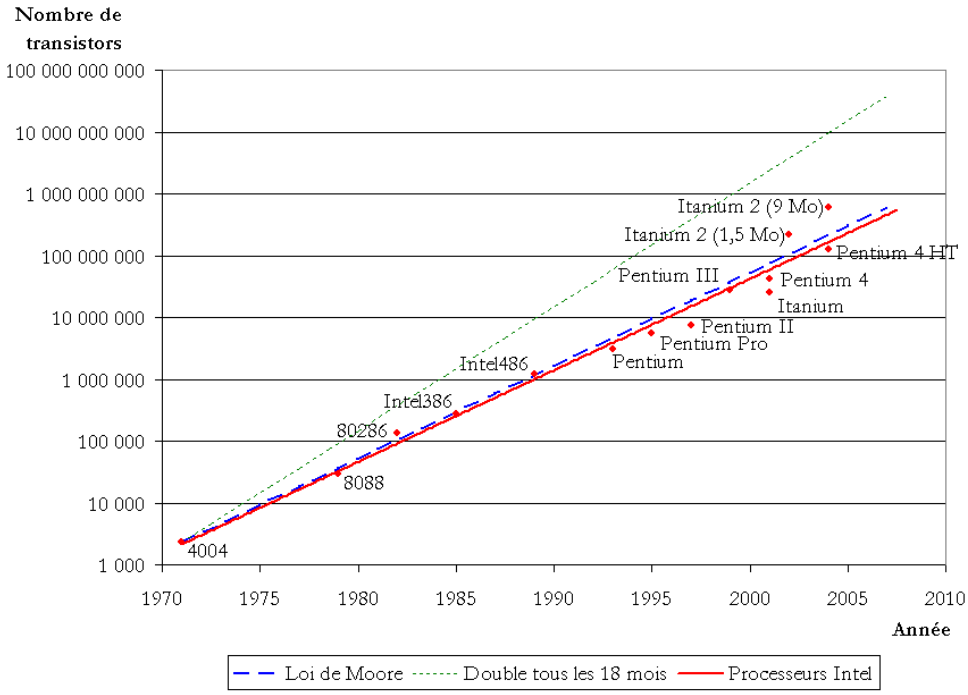


FIG. 7.1 – Loi de Moore : évolution du nombre de transistors dans une puce Intel

Toutefois les transistors auront bientôt atteint leur taille minimale : pour bloquer correctement le courant, une jonction NPN doit faire au moins une vingtaine de

molécules de longueur. De plus des **effets quantiques** apparaissent à ces échelles, qui ne sont pas pris en compte par la théorie de l'informatique actuelle.

En effet celle-ci part du principe que l'information traitée par un processeur, représentée par une série de « bits » (une suite de 0 et de 1), est liée à un support matériel dont l'état ne peut prendre que 2 valeurs. Par exemple un transistor est soit « ouvert » (il laisse passer du courant électrique) et code pour « 0 », soit « fermé » (il ne laisse pas passer de courant) et code pour « 1 ».

En revanche un composant de la taille de quelques molécules, donc relativement isolé de son milieu extérieur, a une forte propension à se comporter comme une particule quantique : il est **au même moment dans plusieurs états à la fois**. Il reste dans cette superposition d'états jusqu'à ce qu'un opérateur extérieur vienne **mesurer** son état, par exemple pour en afficher la valeur à l'écran. Le transistor redevient alors dans un état unique : c'est le phénomène de **décohérence**. Or l'état du transistor à l'issue de cette mesure est **aléatoire** : il est soit ouvert avec probabilité p soit fermé avec probabilité q. Dans ces conditions on comprend qu'il est difficile d'effectuer des calculs sur de l'information qu'on ne retrouve pas toujours dans l'état où on l'avait laissée.

C'est de ce constat que part la théorie de l'informatique quantique : celle-ci prend en compte la superposition des états de l'information quantique, et propose d'effectuer des calculs sur tous ces états en même temps. Ainsi on peut construire, comme nous allons le montrer, des algorithmes beaucoup plus rapides que ceux que nous connaissons.

Cette discipline a déjà 20 ans, mais à l'heure actuelle aucun ordinateur quantique n'est disponible dans nos foyers. La raison est que **l'information quantique est très difficile à contrôler** puisque un objet quantique redevient dans un état unique et aléatoire dès qu'on effectue une mesure sur son état. Or cette mesure est souvent accidentelle : le transistor peut par exemple **interagir avec un objet extérieur** au système quantique du transistor (par exemple un morceau de circuit électronique). Cette interaction constitue une mesure dans le sens où elle **donne de l'information** sur l'état du transistor au milieu extérieur : elle provoque donc la **décohérence** et le transistor redevient dans un état unique (ouvert ou fermé). La moindre perturbation fait donc perdre toute l'information quantique. C'est pourquoi construire un ordinateur quantique a longtemps été jugé irréalisable.

En 1994 la donne change complètement avec la découverte de l'algorithme de Shor : ce protocole quantique décompose les grands nombres en facteurs premiers en un temps logarithmique. Il permet par conséquent de « casser » tous les codes de cryptage de données actuels, basés sur la complexité exponentielle d'une telle décomposition. Pour cette raison l'armée américaine a depuis investi beaucoup d'argent dans des programmes de développement d'ordinateurs quantiques. Depuis les premiers obstacles physiques vers leur réalisation commencent à tomber.

Mais notre objectif ici n'est pas de décrire les supports physiques permettant le calcul quantique. En revanche nous avons l'ambition de faire comprendre les nouveaux concepts de logique mis en oeuvre dans cette théorie et de montrer tout l'intérêt de penser en termes de **logique quantique**.

7.2 Bits quantiques et portes quantiques

Définition 7.1 *Un **bit quantique** (ou « **qubit** ») est un système physique dans une **superposition de 2 états**, sur lequel on peut faire une **mesure** qui renvoie l'un des 2 états de manière **probabiliste**.*

Exemples : • Un photon dont on mesure la polarisation : elle est soit verticale soit horizontale.
• Un électron dont on mesure le spin : il est soit « up » soit « down ».

Description mathématique : Un qubit est représenté par un vecteur de $\mathbf{C}^2$ de norme 1. Cet ensemble sera noté $\mathbf{U}(\mathbf{C}^2)$.
Le vecteur $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ représente le qubit dont la mesure renvoie avec probabilité 1 l'état n°0 : par exemple un spin down ou une polarisation $|\rightarrow\rangle$.
Le vecteur $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ représente le qubit dont la mesure renvoie avec probabilité 1 l'état n°1 : par exemple un spin up ou une polarisation $|\uparrow\rangle$.
Le vecteur $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ représente le qubit dont la mesure renvoie soit l'état $|0\rangle$ avec probabilité $|\alpha|^2$, soit l'état $|1\rangle$ avec probabilité $|\beta|^2$ (et donc $|\alpha|^2 + |\beta|^2 = 1$).

Remarque : Les vecteurs $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ et $\lambda \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ avec $|\lambda| = 1$ représentent le même qubit. Un qubit est donc décrit par une **classe d'équivalence** de $\mathbf{U}(\mathbf{C}^2)/\mathbf{U}(\mathbf{C})$.

Définition 7.2 *Une **porte quantique** est une classe d'équivalence d'isométries de $\boldsymbol{C}^2$ pour la relation $\sim$: $A \in O(\boldsymbol{C}^2), B \in O(\boldsymbol{C}^2)$ alors $A \sim B$ ssi $\exists \lambda \in \boldsymbol{U}(\boldsymbol{C})$, $A = \lambda B$*

Exemples : • $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est un représentant de la porte « **NOT** ». En effet on remarque que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle = |1\rangle$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |1\rangle = |0\rangle$. C'est l'analogue de la porte NOT d'un ordinateur classique.
• $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ est un représentant de l'**Identité**. En effet $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix} \sim \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
• $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ la « **Porte de Hadamard** ». C'est la symétrie orthogonale par rapport à la droite D de direction $\cos(\frac{\pi}{8}) |0\rangle + \sin(\frac{\pi}{8}) |1\rangle$:

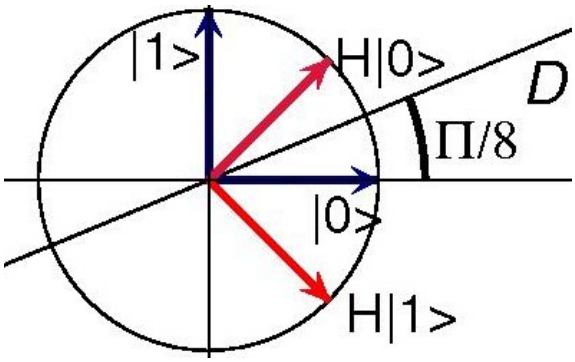


FIG. 7.2 – la porte de Hadamard

On en déduit en particulier que $H^2 = Id$.

La porte de Hadamard peut être construite avec une lame demi-onde d'axe incliné de $\frac{\pi}{8}$ (la lame symétrise la polarisation du photon entrant par rapport à son axe).

• La porte « $\boldsymbol{T}$ », de matrice $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$

Remarquons à ce stade le saut conceptuel effectué : jusqu'alors nous utilisions des opérateurs logiques $(\neg, \vee, \wedge, \Rightarrow, \dots)$ qui agissaient sur des variables booléennes (c'est à dire à valeurs dans $\{vrai, faux\}$ ou $\{0,1\}$) et qui renvoyaient invariablement un booléen.

Ici nous avons complexifié la notion même d'objet logique : nous ne raisonnons plus seulement sur des états « vrais » ou « faux », mais aussi sur des états dans une superposition de « vrai » et « faux ». Nous pouvons ainsi construire des opérateurs beaucoup plus compliqués agissant sur ces états. Par exemple H est une racine carrée de l'identité. De même la porte $\sqrt{NOT} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ est une racine carrée de la négation $(\neg)$.

Définition 7.3 *Un* ***n-qubit*** *est un élément de* $\boldsymbol{U}\left(\boldsymbol{C}^{2\otimes n}\right) / \boldsymbol{U}(\boldsymbol{C})$*, c'est à dire une classe d'équivalence de vecteurs de* $\boldsymbol{C}^{2\otimes n}$ *de norme 1 pour la relation* $\sim$ *:* $U, V \in \boldsymbol{C}^{2\otimes n}$*, alors* $U \sim V$ *ssi* $\exists \lambda \in \boldsymbol{U}(\boldsymbol{C})$, $U = \lambda V$.

Un n-qubit est codé par un ensemble de qubits dont les états sont « **intriqués** », c'est à dire qu'ils forment ensemble un système quantique dans une superposition de 2^n états et dont la mesure renvoie un de ces 2^n états.

Exemple : $\overbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}^{n \text{ fois}}$, noté $\overbrace{|00\dots0\rangle}^{n \text{ fois}}$, représente un n-qubit. C'est le premier des 2^n vecteurs de base de $\mathbf{C}^{2\otimes n}$, numérotés dans l'ordre alphanumérique.

Définition 7.4 *Une* ***n-porte quantique*** *est une classe d'équivalence d'isométries de* $\boldsymbol{C}^{2\otimes n}$.

Exemple : $H^{\otimes n} = \overbrace{H \otimes H \otimes \cdots \otimes H}^{n \text{ fois}}$.

Pour un vecteur de base $|x\rangle$ de $\mathbf{C}^{2\otimes n}$, on vérifie facilement que

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2}^n} \sum_{|y_i\rangle \text{ vecteur de base de } \mathbf{C}^{2\otimes n}} (-1)^{x.y_i} |y_i\rangle$$

avec $x.y$ défini de la manière suivante : pour $|x\rangle = |x_1 x_2 \dots x_n\rangle$, $(x_i)_i \in \{0,1\}^n$ et $|y\rangle = |y_1 y_2 \dots y_n\rangle$, $(y_i)_i \in \{0,1\}^n$ deux vecteurs de base de $\mathbf{C}^{2\otimes n}$ quelconques, on note : $x.y = x_1.y_1 \oplus x_2.y_2 \oplus \dots \oplus x_n.y_n$ où $\oplus$ est l'addition modulo 2.
D'autre part, étant donné que $H^2 = Id$, on remarque que

$$(H^{\otimes n})^2 = Id_{\mathbf{C}^{2\otimes n}}$$

On observe enfin que $H^{\otimes n}$ est symétrique. En effet pour $|u\rangle$ et $|x\rangle$ vecteurs de base de $\mathbf{C}^{2\otimes n}$, en notant $|y_i\rangle$ les 2^n vecteurs de base de $\mathbf{C}^{2\otimes n}$, on vérifie :

$$\left(|u\rangle, H^{\otimes n}|x\rangle\right) = \left(|u\rangle, \frac{1}{\sqrt{2}^n} \sum_{|y_i\rangle} (-1)^{x.y_i} |y_i\rangle\right) = \left(|u\rangle, \frac{1}{\sqrt{2}^n}(-1)^{x.u}|u\rangle\right) = \frac{(-1)^{x.u}}{\sqrt{2}^n}$$

$$\left(H^{\otimes n}|u\rangle, |x\rangle\right) = \left(\frac{1}{\sqrt{2}^n} \sum_{|y_i\rangle} (-1)^{u.y_i} |y_i\rangle, |x\rangle\right) = \left(\frac{1}{\sqrt{2}^n}(-1)^{u.x}|x\rangle, |x\rangle\right) = \frac{(-1)^{u.x}}{\sqrt{2}^n}$$

Exemple : La 2-porte quantique $\mathbf{C}NOT = \begin{pmatrix} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & 0 & 1 \\ |11\rangle & 0 & 0 & 1 & 0 \end{pmatrix}$ (« conditional NOT ») : sur un vecteur de base $|a\rangle \otimes |b\rangle$ de $\mathbf{C}^{2\otimes 2}$ noté $|ab\rangle$ (donc $(a,b) \in \{0,1\}^2$), elle réalise $|a, NOT(b)\rangle$ si $a = 1$ et ne fait rien sinon. Elle réalise donc $|a, b \oplus a\rangle$. Cette définition s'étend par linéarité à tous les vecteurs de $\mathbf{C}^{2\otimes 2}$.

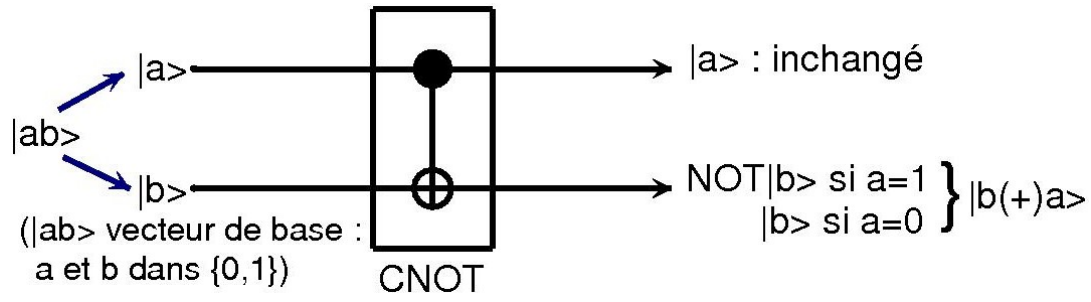


FIG. 7.3 – la porte CNOT

Exemple : la porte de Toffoli

$$Toffoli = \begin{array}{c} \\ |000\rangle \\ |001\rangle \\ |010\rangle \\ |011\rangle \\ |100\rangle \\ |101\rangle \\ |110\rangle \\ |111\rangle \end{array} \begin{array}{c} \begin{array}{cccccccc} |000\rangle & |001\rangle & |010\rangle & |011\rangle & |100\rangle & |101\rangle & |110\rangle & |111\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

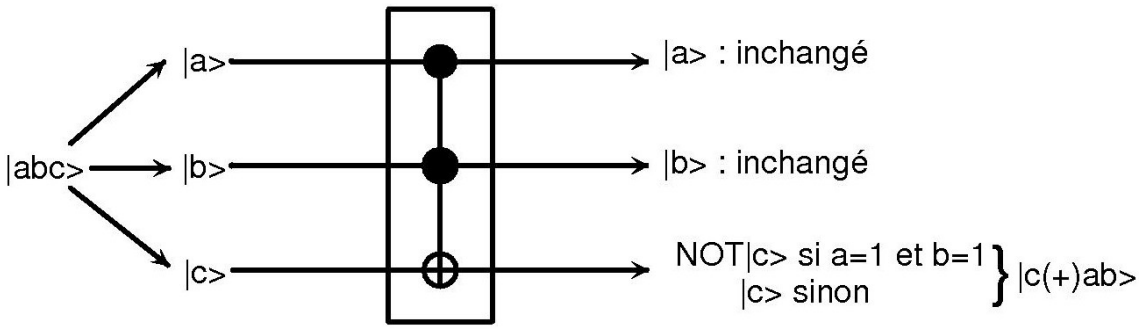
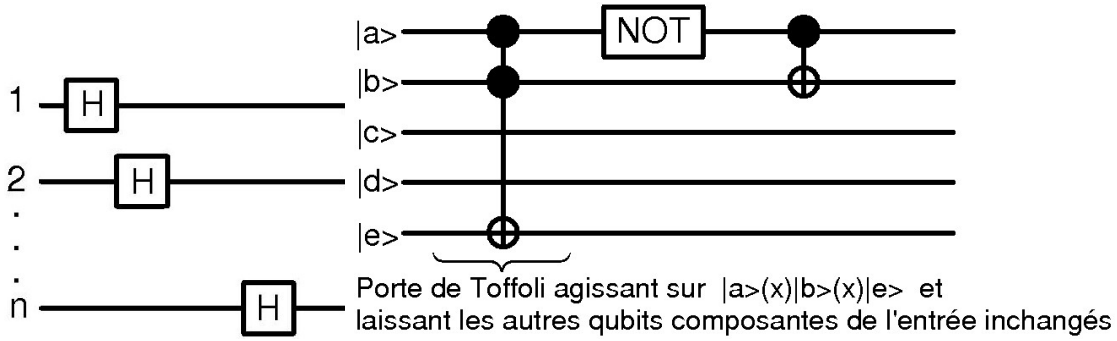


FIG. 7.4 – la porte de Toffoli

Définition 7.5 *Un* ***n-circuit quantique*** *est une succession de 1-portes, de 2-portes ou de 3-portes, prolongées respectivement par* $\otimes id_{\mathbb{C}^2}{}^{\otimes(n-1)}$, $\otimes id_{\mathbb{C}^2}{}^{\otimes(n-2)}$ *et* $\otimes id_{\mathbb{C}^2}{}^{\otimes(n-3)}$ *sur les autres qubits composant le vecteur de base de l'entrée.*

Un n-circuit est donc un produit de plusieurs n-portes quantiques, chaque porte n'agissant que sur 1,2 ou 3 qubits composant le vecteur de base de l'entrée et laissant les autres inchangés.

Exemples : Le n-circuit de gauche « implémente » (c'est à dire effectue) $H^{\otimes n}$.



Remarque : On sait construire un 3-circuit qui implémente la porte de Toffoli uniquement avec des 2-portes.

Définitions 7.1 • *Un n-circuit* $U = U_L \dots U_2 U_1$ ($U_i \in O(\boldsymbol{C}^{2\otimes n})/\boldsymbol{U}(\boldsymbol{C})$) *de longueur* L *calcule une fonction* $F : \boldsymbol{U}(\boldsymbol{C}^{2\otimes k})/\boldsymbol{U}(\boldsymbol{C}) \to \boldsymbol{U}(\boldsymbol{C}^{2\otimes k})/\boldsymbol{U}(\boldsymbol{C})$ *avec* ***erreur*** ϵ *ssi toute entrée* $|x\rangle$ *dans* $\boldsymbol{C}^{2\otimes k}$ *vérifie*

$$\sum_{|z\rangle \text{ vecteur de base de } \boldsymbol{C}^{2\otimes(n-k)}} \left|\left\langle F(x)\otimes z \,|U|\, x\otimes 0^{n-k}\right\rangle\right|^2 \geq 1-\epsilon$$

• *la* ***taille*** *d'un circuit est le nombre de portes utilisées pour le réaliser.*
• *la* ***complexité*** *approchée (resp exacte) d'une fonction est la taille minimale du circuit qui la calcule avec erreur* $1/3$ *(resp 0).*

Remarque : L'erreur peut être arbitrairement réduite à ϵ par $\log(1/\epsilon)$ itérations.

Proposition 7.1 *On peut démontrer que les portes* $(H, CNOT, T)$ *forment une* ***base universelle****, c'est à dire qu'elles permettent de fabriquer pour chaque fonction* $F : \boldsymbol{U}(\boldsymbol{C}^{2\otimes k})/\boldsymbol{U}(\boldsymbol{C}) \to \boldsymbol{U}(\boldsymbol{C}^{2\otimes k})/\boldsymbol{U}(\boldsymbol{C})$ *un circuit qui approche* F *avec une précision arbitraire.*

7.3 Calcul de fonctions

Toute fonction $f : \{0,1\}^n \to \{0,1\}^m$ peut s'implémenter au moyen d'un circuit classique. On définit alors le prolongement de f par linéarité :
$\tilde{f} : \mathbf{U}(\mathbf{C}^{2\otimes k})/\mathbf{U}(\mathbf{C}) \to \mathbf{U}(\mathbf{C}^{2\otimes m})/\mathbf{U}(\mathbf{C})$. On peut donc construire, au moins sur le papier, le circuit quantique qui implémente $\tilde{f}$: il suffit pour cela de récupérer le plan du circuit classique et de remplacer chaque porte par son analogue quantique (c'est à dire par son prolongement par linéarité).
À chaque fonction $f : \{0,1\}^n \to \{0,1\}^n$ on peut associer une opération unitaire

$$\begin{array}{rccc} F: & \{0,1\}^n \times \{0,1\}^m & \to & \{0,1\}^n \times \{0,1\}^m \\ & |x\rangle \times |y\rangle & \to & |x\rangle \times |y \oplus f(x)\rangle \end{array}$$

On sait facilement implémenter F : par exemple au moyen d'une succession de portes CNOT. On remarque en particulier que

$$F\,|x\rangle \times |0\rangle = |x\rangle \times |f(x)\rangle$$

Proposition 7.2 *Pour toute fonction binaire* $f : \{0,1\}^n \to \{0,1\}$ *on peut construire un circuit quantique qui effectue*

$$F'\,|x\rangle := (-1)^{f(x)}\,|x\rangle$$

où F' *est étendue par linéarité à* $\tilde{F'} : \boldsymbol{U}(\boldsymbol{C}^2)/\boldsymbol{U}(\boldsymbol{C}) \to \boldsymbol{U}(\boldsymbol{C})$

preuve : A partir de F, on peut construire $\tilde{F'}$ (notée F' dans la suite) en utilisant

un qubit supplémentaire dans l'état $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$: soit $x \in \{0,1\}$, alors

$$\begin{aligned} F|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= |x\rangle \frac{1}{\sqrt{2}} \left(|f(x)\rangle - \left|\overline{f(x)}\right\rangle \right) \\ &= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ &= F'|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

7.4 Un premier exemple d'algorithme quantique

Algorithme 7.1 (Deutsch) *Problème : étant donné une fonction $f : \{0,1\} \to \{0,1\}$, décider si $f(0) = f(1)$. Solution :*
- *faire $|\psi\rangle = HF'H|0\rangle$*
- *$m = Mesure(|\psi\rangle)$*
- *si $m = 0$ répondre CONSTANTE sinon EQUILIBREE*

Bilan : on n'a effectué qu'un seul « passage » par le circuit qui implémente f. En classique on aurait été obligé de faire appel 2 fois au circuit de f.

preuve :

$$\begin{aligned} |\psi\rangle &= HF'H|0\rangle) \\ &= HF' \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= H(-1)^{f(0)} \frac{1}{\sqrt{2}} \left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \right) \\ &= H \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{f(0)}(-1)^{f(1)}|1\rangle \right) \\ &= H \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle \right) \\ &= (-1)^{f(0)} |f(0) \oplus f(1)\rangle \end{aligned}$$

On obtient donc l'état $|f(0) \oplus f(1)\rangle$ avec probabilité 1. Si $|f(0) \oplus f(1)\rangle = |0\rangle$ alors la foncion est constante ($f(0) = f(1)$), sinon la fonction est équilibrée ($f(0) \neq f(1)$).

Cet algorithme se généralise avec une efficacité spectaculaire (mais on ne refera pas la preuve).

Algorithme 7.2 (Deutsch-Josza) *Problème : Etant donné $f : \{0,1\}^n \to \{0,1\}$, décider si f est constante ($\forall x, y,\ f(x) = f(y)$) ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)|$). Solution :*
- *faire $|\psi\rangle = H^{\otimes n} F' H^{\otimes n} |0\rangle$*
- *$m = Mesure(|\psi\rangle)$*
- *si $m = 0$ répondre CONSTANTE, sinon répondre EQUILIBREE*

Bilan : un seul appel au circuit de f. En classique on aurait été obligé d'en faire $2^{n-1} + 1$!

On pourra trouver sur le site web du PSC un autre exemple simple et parlant d'algorithme quantique : l'algorithme de Grover pour $n = 5$.

7.5 L'algorithme de recherche de Grover

On a une fonction binaire $f : \{0,1\}^n \to \{0,1\}$ qui vaut 1 sur M vecteurs de $\{0,1\}^n$ ($M \ll N$) et 0 sur tous les autres. On cherche les M vecteurs $(|u_i\rangle)_{i\in 1,\dots M}$ vérifiant $f(|u_i\rangle) = 1$ tout en minimisant le nombre d'appels au circuit qui implémente f (pour n grand c'est essentiellement lui qui consomme du temps de calcul).

L'algorithme de Grover permet de trouver la réponse avec $\sqrt{\frac{N}{M}}$ appels à un circuit qui implémente f (en l'occurence le F' de la proposition 7.2).

Exemple : (factorisation d'un grand entier) On cherche à « casser » un grand entier A de taille t bits produit de deux nombres premiers p et q inconnus. On définit f la fonction qui prend comme argument un entier a (codé par un t-bit de $\{0,1\}^t$), qui renvoie 1 si a divise A et 0 sinon. On cherche un unique diviseur entre 0 et $\sqrt{A}$ (sauf si A est un carré), c'est à dire avec nos notations $M = 1$ et $N = \sqrt{A}$.

Le circuit de f « consomme » $O(\frac{N^2}{a})$ additions à chaque appel, soit une moyenne de $2N$ additions pour $a \in \{0, N\}$. Avec un algorithme classique (et naïf) qui essaie tous les diviseurs les uns après les autres, le nombre d'additions moyen à effectuer augmente donc en $O(N^2)$, et donc en $O(2^t)$. L'algorithme de Grover permet de n'effectuer que $\sqrt{N}$ appels à f, soit un nombre d'additions qui croît en $O(N\sqrt{N})$ et donc en $O(2^{\frac{3}{4}t})$. Cet exemple est conceptuellement intéressant, mais l'agorithme de factorisation de Shor est beaucoup plus performant.

Exemple : (l'annuaire inverse) On cherche un nom dans l'annuaire connaissant son numéro de téléphone *num* : avec nos notations $M = 1$. Il y a $N = 2^t$ noms dans l'annuaire, on les code par les 2^t nombres dans $\{0,1\}^t$. Chaque nom (ou t-bit de $\{0,1\}^t$) est associé dans la mémoire de l'ordinateur à un numéro de téléphone. La fonction test f que nous choisirons naturellement est celle qui prend comme argument un t-bit, qui charge en mémoire son numéro de téléphone associé dans l'annuaire, qui le compare avec *num* et qui renvoie 1 s'ils sont égaux et 0 sinon. (Pour plus de détails sur la construction d'une telle « base de données quantique » et sur la manière dont on accède à cette « mémoire quantique » on se référera à [1]).

Classiquement on fera en moyenne $\frac{N}{2}$ consultations d'entrées dans l'annuaire (soit autant d'appels à f) avant de trouver le t-bit cherché. L'algorithme de Grover, lui, permet de ne faire que $O(\sqrt{N})$ consultations (c'est à dire d'appels au circuit F' qui implémente f). La mécanique quantique permet en effet de charger en mémoire une « superposition de numéros de téléphone dans l'annuaire », puis de lui appliquer la fonction de comparaison (le circuit F'), le tout en une seule passe : c'est à dire en autant d'étapes qu'un circuit classique l'aurait fait pour un seul numéro.

Définition 7.6 *l'algorithme de Grover utilise la porte « **phase shift** » :*

$$|x\rangle \to \begin{cases} -|x\rangle \ \ si\ \ |x\rangle \neq \underbrace{|00\dots0\rangle}_{n\ fois} \ (noté\ |0\rangle\ pour\ abréger) \\ |x\rangle \ \ si\ \ |x\rangle = |0\rangle \end{cases}$$

qui réalise donc $2\left|00\ldots0\right\rangle\left\langle 00\ldots0\right| - Id = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$

Algorithme 7.3 (Grover)

$$\left|\phi\right\rangle = \left(H^{\otimes n}\left(2\left|0\right\rangle\left\langle 0\right| - Id\right)H^{\otimes n}F'\right)^{E\left(\sqrt{\frac{N}{M}}\right)} H^{\otimes n}\left|0\right\rangle$$

$$m = Mesure(\left|\phi\right\rangle)$$

m est un état quelconque parmi les $(\left|u_i\right\rangle)_{i\in\{1,\ldots,M\}}$ *états solutions cherchés, avec probabilité* $1 - 4\frac{M}{N}$ *: en répétant l'algorithme on obtient donc toutes les solutions avec une précision qui croît exponentiellement.*

preuve : On rappelle que $H^{\otimes n}$ est hermitien et que $(H^{\otimes n})^2 = Id$.
$H^{\otimes n}\left(2\left|0\right\rangle\left\langle 0\right| - Id\right)H^{\otimes n} = 2H^{\otimes n}\left|0\right\rangle\left|0\right\rangle^{\dagger}\underbrace{H^{\otimes n}}_{=(H^{\otimes n})^{\dagger}} - Id$ par linéarité.
Soit en notant $\left|\psi\right\rangle = H^{\otimes n}\left|0\right\rangle$:

$$2\left|\psi\right\rangle\left|\psi\right\rangle^{\dagger} - Id = 2\left|\psi\right\rangle\left\langle\psi\right| - Id$$

C'est la **symétrie orthogonale d'axe** $\left|\psi\right\rangle$ (en effet $\left|\psi\right\rangle$ est unitaire car $H^{\otimes n}$ est une isométrie). On rappelle que

$$\left|\psi\right\rangle = H^{\otimes n}\left|0\right\rangle = \frac{1}{\sqrt{N}} \sum_{\left|y_i\right\rangle \text{ vecteur de base de } \mathbf{C}^{2\otimes n}} (-1)^{x.y_i}\left|y_i\right\rangle$$

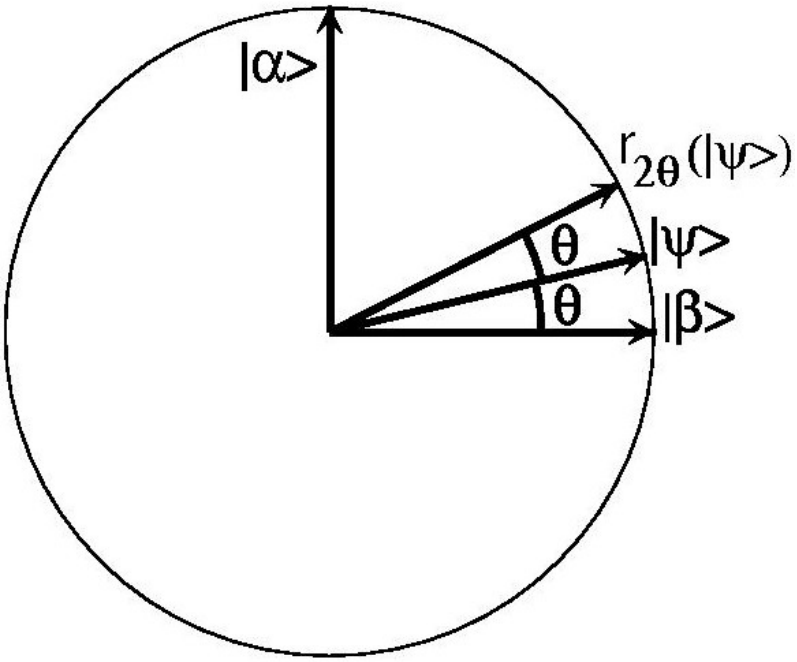
Représentation graphique : On travaille dans le plan des vecteurs

$$\begin{cases} \left|\beta\right\rangle = \frac{1}{\sqrt{M}}\sum_{f(\left|u_i\right\rangle)=1}\left|u_i\right\rangle \text{ superposition des } \left|u_i\right\rangle \text{ cherchés} \\ \left|\alpha\right\rangle = \frac{1}{\sqrt{N-M}}\sum_{f(\left|y_i\right\rangle)=1}\left|y_i\right\rangle \text{ superposition des autres vecteurs de base} \end{cases}$$

Dans cette base (orthonormée), $\left|\psi\right\rangle$ s'écrit :

$$\begin{aligned} \left|\psi\right\rangle &= H^{\otimes n}\left|0\right\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{\left|y_i\right\rangle \text{ vecteur de base de } \mathbf{C}^{2\otimes n}} \left|y\right\rangle \text{ (rappel)} \\ &= \frac{1}{\sqrt{N}}\left(\sqrt{M}\left|\beta\right\rangle + \sqrt{N-M}\left|\alpha\right\rangle\right) \\ &= \sin\theta\left|\beta\right\rangle + \cos\theta\left|\alpha\right\rangle \text{ avec } \sin\theta = \sqrt{\frac{M}{N}} \text{ et } \cos\theta = \sqrt{\frac{N-M}{N}} \end{aligned}$$

Comment s'interprète F' dans ce plan ? F' inverse la composante sur $\left|\beta\right\rangle$ et conserve la composante sur $\left|\alpha\right\rangle$: c'est la **symétrie orthogonale d'axe** $\left|\alpha\right\rangle$.
Donc $(H^{\otimes n}\left(2\left|0\right\rangle\left\langle 0\right| - Id\right)H^{\otimes n}F')$ est le produit de 2 symétries : c'est la **rotation d'angle** 2θ.
Si $M \ll N$ alors $2\theta \approx 2\sin\theta \approx 2\frac{M}{N}$. Donc en appliquant à $\left|\psi\right\rangle$ la rotation d'angle 2θ



un nombre de fois majoré par $\frac{\pi}{4}\sqrt{\frac{N}{M}}$, on fait tourner $|\psi\rangle$ pour l'amener « suffisamment près » de $|\beta\rangle$, au sens où l'écart angulaire est majoré par $2\theta \approx 2\sqrt{\frac{M}{N}}$. Donc la probabilité p que la mesure de $|\psi\rangle$ donne un des états cherchés (superposés dans $|\beta\rangle$) est minorée : $p = |\langle\beta|\ \psi\rangle|^2 = \cos^2(\theta) \geq 1 - 4\frac{M}{N}$.

7.6 Conclusion

La logique quantique est certes une très belle construction de l'esprit qui prolonge naturellement la logique usuelle en mathématiques. Elle permet aussi de faire tourner, sur le papier, des algorithmes beaucoup plus performants que ceux que nous connaissons. Une question subsiste : verrons-nous un jour fonctionner un ordinateur quantique ?

Les obstacles physiques à sa réalisation sont loin d'être résolus mais de nombreuses équipes de recherche y travaillent aujourd'hui dans le monde entier. L'enjeu est d'isoler suffisamment les qubits pour éviter le phénomène de décohérence tout en en manipulant le plus grand nombre possible à la fois. Plusieurs pistes de supports de l'information quantique sont aujourd'hui explorées.

Parlons donc pour finir de deux expériences récentes et médiatiques qui illustrent les progrès dans ce domaine. La première a été réalisée en 2005 dans le laboratoire de Rainer Blatt à Innsbruck : un 8-qubit a été construit au moyen d'ions piégés dans un champ électrique et alignés au moyen d'un champ magnétique.

La deuxième, datant du 13 Février dernier, n'a pas encore été validée par la communauté scientifique : la start-up canadienne D-wave a annoncé avoir réalisé un calcul quantique avec 16 qubits (résolution d'un sudoku). Elle annonce qu'elle va commercialiser en 2008 une première puce quantique conçue pour faire tourner l'algorithme de Grover. Mais la technologie de « calcul quantique adiabatique » mise en

oeuvre est loin d'être grand public : la puce « Orion » a besoin d'un bain d'hélium liquide à -269°C pour fonctionner.

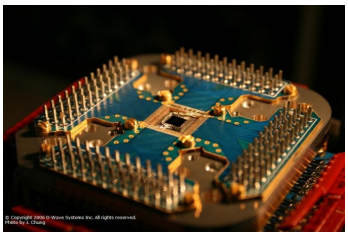


FIG. 7.5 – Orion serait « commercialement viable ».

Si l'ordinateur quantique n'est peut-être pas pour demain, les pays développés y croient : le budget mondial annuel pour ces recherches est de 150 millions d'euros.

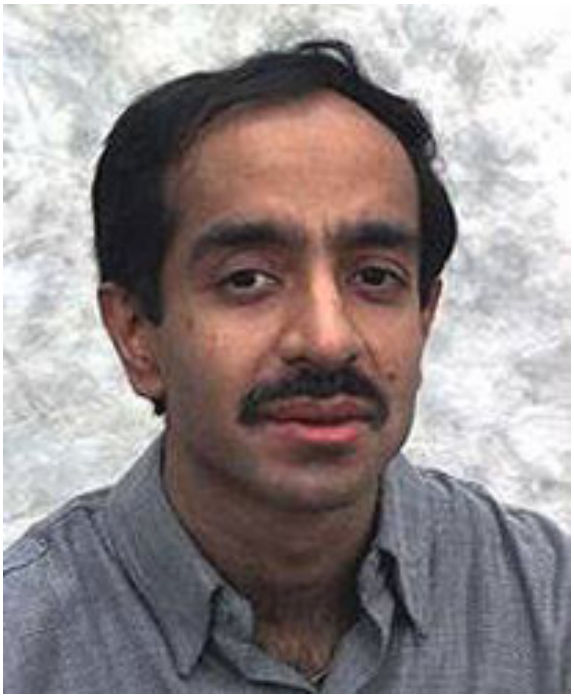


FIG. 7.6 – Dr Lov K. Grover (né en 1961)

Table des figures

Bibliographie

[1] Nielsen et Chuang *Quantum Computation and Quantum Information*. Cambridge, 2003.

[2] E. Bouscaren *Introduction à la théorie des modèles*. Rentrée de Majeure, Ecole Polytechnique, Septembre 2005.

[3] J.-L. Krivine, R. Cori *La Logique*. Masson, 2003.

[4] Kurt Gödel *Sur les propositions formellement indécidables des Principia Mathematica et des systèmes apparentés I*. 1931.

[5] Dahan-Dalmedico et Pfeiffer *histoire des mathématiques - routes et dédales*. Etudes Vivantes, 1982.

[6] P. Dehornoy *Logique et Théorie des Ensembles*. Cours de l'ENS.

[7] Reissman *Théorème de Banach-Tarski*.

[8] P. Dehornoy *Les suites de Goodstein*. Article de Pour la Science n°273.

[9] Brockhaus *Enzyklopedie in 15 Bänden*. 2007.

[10] Philippe Grangier *Les défis de l'ordinateur quantique*. Article de La Recherche, Juin 2006.

[11] Pierre Fima *Portes et circuits quantiques*. Groupe de travail Mathématiques du calcul quantique, ENS Ulm.