Préliminaires méta-logiques
(version chantier quasi-achevée)

Marc SAGE

29 mai 2012

Table des matières

> Because language is misleading, as well as because it is diffuse and inexact when applied to logic (for which it was never intended), logical symbolism is absolutely necessary to any exact or thorough treatment of our subject.
>
> Lord Bertrand Russell, *Introduction to Mathematical Philosophy* (1920).

1 L'acte de substitution ou d'instanciation

On décrit ici un acte fondamental de la pratique mathématique que l'être humain peut décrire dans son langage usuel, reconnaître et effectuer lui-même.

1.1 Instancier

Dans un groupement fini de symboles, remplacer certains de ces symboles chacun par un groupe de symboles est appelé ***instancier***, le résultat de cet acte (l'***instanciation***) est une ***instance***.

Pourquoi cette terminologie ? Une instance d'une formule, c'est la *forme* ***instant****anée* que prend celle-ci à un moment du discours, c'est la forme locale qu'elle revêt dans le contexte considéré – moment ou contexte donné par les substitutions.

Pour pallier d'éventuelles ambigüités, il est conventionnel de mettre des *parenthèses* autour du groupe remplaçant / substitué.

Lorsqu'un symbole σ a été remplacé par un groupe de symboles Σ, on note

$$\sigma \leftarrow \Sigma \qquad \text{et on pourra lire indifféremment : } \begin{cases} \text{à la place de } \sigma \text{ on met } \Sigma \\ \text{remplacer } \sigma \text{ par } \Sigma \\ \text{substituer à } \sigma\ \Sigma \\ \text{substituer } \Sigma \text{ à } \sigma \end{cases}$$

(Attention aux verbes *remplacer* et *substituer* qui échangent les rôles des compléments d'objet direct et indirect.)

Par exemple,

$$\begin{aligned} u_{\varphi(n)} \text{ devient après substitution } n &\leftarrow \psi(m) \text{ l'instance } u_{\varphi(\psi(m))}, \\ \sqrt{\frac{7\square - e}{\pi + \cos\square}} \text{ devient apès substitution } \square &\leftarrow a^2+1 \text{ l'instance } \frac{7\left(a^2+1\right)-e}{\pi+\cos\left(a^2+1\right)}. \end{aligned}$$

On peut tout à fait effectuer *plusieurs* instanciations *successivement* : par exemple, le groupe de symboles $\blacksquare + \square$ devient, après les instanciations $\blacksquare \leftarrow (a+B)^2$ puis $\square \leftarrow \frac{5t}{\Omega}$, l'instance $(a+B)^2 + \frac{5t}{\Omega}$: on observera que l'instance obtenue est la même si l'on effectue les instanciations dans l'ordre inverse. La raison est simple : aucun symbole n'est commun aux termes de ces deux instanciations. Les informaticiens diront que l'algorithme d'instanciation est (dans ce cas) ***confluent*** :

lorsque plusieurs instanciations ne possèdent,
dans leur termes substitués ou remplacés, aucun symbole en commun,
l'instance obtenue en effectuant successivement ces instanciations ne dépend pas de l'ordre choisi.

Il n'en est cependant pas toujours ainsi. Par exemple, instancier $\triangledown$ selon $\triangledown \leftarrow \triangledown^2$ puis selon $\triangledown \leftarrow 18\triangledown$ donnerait $(18\triangledown)^2$ tandis que l'on obtiendrait selon l'ordre inverse l'instance $18\triangledown^2$. De même, instancier $n \leftarrow p(n)$ puis $n \leftarrow q(n)$ dans la suite de symbole a_n donnerait l'instance $a_{p(q(n))}$, à comparer avec l'instance $a_{q(p(n))}$ que l'on aurait obtenue en instanciant selon l'ordre inverse. Prenons un dernier exemple, plus complexe : la suite de symboles $\bigotimes_{\varepsilon}^{\square} \blacksquare^a \divideontimes \bigoplus_{\varepsilon}^{3\square} \mathfrak{Q}^{-a}$ devient après substitutions successives (de haut en bas) $\Big\downarrow \begin{array}{c} \square \leftarrow \omega^2+1 \\ \mathfrak{Q} \leftarrow \blacksquare \diagup_{\ddagger\blacksquare} \\ \blacksquare \leftarrow \aleph \boxtimes \mho \\ \varepsilon \leftarrow a=1 \end{array}$ l'instance

$$\bigotimes_{\alpha=1}^{\omega^2+1} (\aleph \boxtimes \mho)^{\alpha} \divideontimes \bigoplus_{a=1}^{3\left(\omega^2+1\right)} \left(\aleph\boxtimes\mho \diagup_{\ddagger(\aleph\boxtimes\mho)}\right)^{-\alpha}$$

tandis que, si l'on avait instancié dans l'autre sens (de bas en haut), l'on aurait obtenu l'instance

$$\bigotimes_{\alpha=1}^{\omega^2+1} (\aleph \boxtimes \mho)^{\alpha} \divideontimes \bigoplus_{a=1}^{3\left(\omega^2+1\right)} \left(\blacksquare \diagup_{\ddagger\blacksquare}\right)^{-\alpha}.$$

On retiendra donc que la confluence d'instanciations n'est en générale pas assurée :

l'instance obtenue en effectuant successivement plusieurs instanciations dépend a priori *de l'ordre choisi ;*
il conviendra d'être attentif lorsqu'un même symbole apparaît dans deux termes de ces instanciations.

(L'interprétation mathématique de ce fait est que la composition des applications n'est, en général, pas commutative.)

1.2 Sur les mots spécialiser (danger) et évaluer (à proscrire)

L'usage mathématique parle plutôt, au lieu d'instancier, de ***spécialiser***. Mais nous voyons là une opération supplémentaire et d'une autre nature à la substitution : l'assignation d'une valeur (*évaluation*) du symbole substitué et plus généralement l'interprétation de l'expression obtenue.

Il y a également l'usage confondant *spécialiser* avec *évaluer* (dont le sens est *donner une valeur à*). Discutons cet usage en envisageant plusieurs consignes d'évaluation (chacune contournant la difficulté exhibée dans la précédente) :

1. « *Soit r un réel : évaluer l'expression $2 \times r^3 - 1$ en 18* » L'expression n'en est pas une (c'est un réel puisque r est réel).
2. « *Soit r un réel : évaluer le réel $2 \times r^3 - 1$ en 18* » très bien : je prends le réel 1 (j'impose $r = 1$) puis j'évalue le réel 1 (le résultat de $2 \times 1^3 - 1$) en 18 – comment faire ?
3. « *Soit r un symbole de réel : évaluer l'expression $2 \times r^3 - 1$ en $r = 18$* » Un symbole n'étant pas un réel, l'égalité est un non-sens.
4. « *Soit r un symbole de réel : évaluer l'expression $2 \times r^3 - 1^3$ en évaluant r en 18* » : on peut toujours donner la valeur 18 au symbole r mais ce don de valeur ne nous dit pas
   (a) pourquoi il faudra constituer l'expression $2 \times 18^3 - 1$ (c'est justement le rôle de la *substitution* $r \leftarrow 18$) ;
   (b) comment donner une valeur à $2 \times 18^3 - 1$ (c'est le rôle du *calcul*, ce qui nécessite une interprétation des symboles 18, 2, $\times$ et $-$).

Par conséquent, lorsque E est une certaine expression où apparait un certain symbole s, étant donné un symbole σ,

« *évaluer l'expression E en $s = \sigma$* »

est un abus de langage pour dire

« *calculer (selon une interprétation implicitement donnée par le contexte) le résultat de l'expression E obtenue après substitution $s \leftarrow \sigma$* ».

Les non-dits dans cet abus de langage sont :

1. la substitution ;
2. l'interprétation ;
3. le calcul.

L'*évaluation* doit être vue *stricto sensu* comme une règle d'interprétation des symboles – en particulier du symbole substitué. Elle *prend* donc *part* à l'interprétation et ne s'y identifie que dans le cas trivial où l'expression E est réduite au symbole substitué, où l'on « évalue » un symbole s après substitution $s \leftarrow \sigma$ (le calcul est vide, on obtient la valeur du symbole σ). Mais l'évaluation *ne peut prendre aucunement part* à la substitution car cette dernière reste au niveau syntaxique – tandis que l'attributon d'une valeur passe du niveau syntaxique au niveau sémantique.

La *spécialisation* quant à elle doit être vue comme la substitution suivie de l'interprétation (points 1 et 2 ci-dessus).

Le *calcul* enfin est un jeu dont les règles sont données par l'interprétation des symboles de l'instance de E obtenue (interprétation constituant le *contexte* du calcul) et permettent de transformer cette dernière en une expression plus adéquate à nos volontés (qui peuvent être de toutes sortes). Le calcul peut être automatique lorsque l'on possède un algorithme pour le conduire mais il a bien plus souvent un caractère artisanal, artistique, divinatoire, qui témoigne de l'adresse (*craftsmanship*) de celui qui le mène – homme ou machine guidée par l'homme. C'est toute la différence entre un jeu dont on connaît une stratégie gagnante (morpion) et un jeu où l'on joue avec intuition et essais (go).

1.3 Sur le mot variable (à proscrire)

La terminologie traditionnelle parle de symbole ***de variable*** pour souligner que l'interprétation d'un tel symbole peut *varier* dans un certain ensemble. La souplesse de ce mot fait qu'on l'utilise abusivement en sciences dans en nombreuses situations – tout en étant (heureusement) compris.

En ce début de cours, nous n'avons pas l'expérience pour justifier et clarifier ces abus ; la confusion qu'ils portent en eux nous semble donc trop dangereuse pour que nous y frottions. Nous préférons d'ailleurs nous en tenir à l'écart en toute circonstance. On se préservera ainsi d'autre déconvenues, à savoir confondre une variable avec une *inconnue* (objet dans une relation – appelée alors *équation* – dont on cherche les valeurs réalisant cette relation), un *argument* (ce qu'on donne à manger à une fonction), une *indéterminée* (originellement un symbole instanciable, maintenant objet polynomial décrivable par une certaine propriété universelle).

Le hiatus terminologique éclate lorsque que l'on veut « *fixer une variable* » (pour pouvoir raisonner dessus) car un *objet variable* est à proprement parler une chimère : aucun objet considéré en mathématique n'est variable puisque, une fois considéré, il est déterminé et ne peut plus varier. Parler donc de symbole d'objet variable (ou, pour abréger, de symbole de variable) est donc tout aussi chimérique – autant à ce titre parler de symbole d'objet *fixable*. Or il n'y a absolument rien qui puisse varier ou être fixé : le symbole d'objet ne demande pas à *varier* mais il demande exclusivement à ce qu'on lui *affecte/assigne une valeur*, à *être interprété* en un objet singulier, à *être incarné par* un tel objet spécial, il est en attente de *spécialisation*.

S'il vous restait quelques velléités à utiliser un adjectif pour désigner un symbole d'objet, oubliez *variable* (qui devrait alors être remplacé par *fixable*) et réfléchissez plutôt à l'usage de :

incarnable ou *spécialisable*

(pas *affectable* ni *assignable* car on affecte/assigne du sens à un symbole et non l'inverse (problème de compléments direct/indirect))

(pas *attribuable* car ce qu'on attribue à un objet sont plutôt des propriétés)

(pas *désignable* ni *dénotable* ni *interprétable* (tautologique !) car c'est le role d'un symbole de dénoter/désigner ou d'être interprété)

(pas *représentable* car mauvais sens : on représente un objet par un symbole)

(pas *instanciable* ni *substituable* car ce serait rester sur le même terrain, symbolique, alors que l'on passe au sémantique)

(pas *traduisible* car deux sens possibles : modéliser ou interpréter).

2 Sur l'ambiguïté du langage et les h-entiers

> Les propositions mathématiques sont d'abord des phrases françaises ; mais pas seulement des phrases françaises, puisque toute proposition mathématique entretient une ressemblance avec certaines propositions non-mathématiques. – Les mathématiciens, lorsqu'ils se mettent à philosopher, commettent toujours l'erreur qui consiste à négliger la différence de fonction entre les propositions mathématiques et les propositions non-mathématiques.
>
> Ludwig WITTGENSTEIN, *Cours sur les fondements des mathématiques* (Cambridge, 1939).

2.1 Les niveaux 0, -1 et -2 de langage

REVOIR AVEC GONSETH, PAS DE META, QUE DU 0 ! !§ NIVEAU 1 OBSCUR, NV 2 FICTIO, AUTANT LES EXPEDIER AU DéBUT

Ces lignes que vous lisez participent d'un certain langage – le langage usuel, peut-être votre langue maternelle – que nous utilisons pour présenter le langage logique, son objet, ce dont il parle. De la même façon, le langage logique *parle des* objets mathématiques[1]. Nous voyons apparaître ici une *hiérarchie de langages* dont chacun parle du suivant. Ne pas avoir conscience de cette hiérarchie, c'est l'aplatir, aplatissement menant droit aux paradoxes de BERRY et de RICHARD (*cf.* cours d'introduction).

[1] Cette phrase peut être prise comme une *définition* des objets mathématiques. Cette définition minimale possède l'avantage d'éviter tout ingrédient de nature théologique.

Afin de distinguer relativement ces niveaux de langage, il nous faut en prendre un comme point de repère. Nous choisirons le langage usuel, qui s'adresse à l'être humain et qui prend sens grâce à son *entendement*, ce dernier lui permettant surtout d'appliquer sa *capacité à juger*. Ce niveau 0 va permettre de présenter le langage logique, le niveau -1, posant ainsi le cadre *méta-logique*.

(Par le préfixé *-méta*, nous signifions un niveau au-dessus. Ainsi, le niveau méta-logique est celui situé juste au-dessus du niveau logique, juste au-dessus du niveau -1, à savoir le niveau 0, ce qui devrait éclairer notre terminologie.)

Le niveau -1 va quant à lui parler de la mathématique (ses objets, ses phénomènes, situés au niveau -2), constituant ainsi le cadre *méta-mathématique*. Quitte à nous répéter, cette phrase peut être considérée comme *définition* (minimale) du monde mathématique : ce dont traite le langage logique.

Ainsi, lorsque nous prétendons utiliser notre capacité de jugement au niveau 0 pour trancher d'une question de mathématique, c'est en fait à un niveau *méta-méta-mathématique* que nous exerçons cette faculté.

Le nombre de préfixes « -méta » ne doit pas nous faire perdre de vue l'*axe* à distinguer dans ce qui précède, à savoir *le niveau où nous pouvons appliquer notre capacité à juger*. Afin de favoriser cette dernière, toute démarche algorithmique sera profitable de par la facilité à vérifier chaque étape de l'algorithme (ou de demander à une machine de le faire).

2.2 Réalité physique et monde du sens

Chaque élément d'un langage possède un double visage :

1. son *signifiant* : une partie de la réalité physique, par exemple des graphèmes ou des phonèmes ;
2. son *signifié* : le sens qu'il porte.

S'il est difficile de douter de la réalité physique des signifiants, il est légitime de se demander *comment* un signifiant peut-il au juste *signifier*. L'acteur qui permet de mettre du sens dans des données (physiquement) sensibles[2], nous l'appellerons notre *entendement*.

Écoutons Stella Baruk nous en parler dans cet extrait de *C'est-à-dire* :

> l'entendement, c'est cette possibilité, cette potentialité constitutives du sujet humain de recevoir et de produire du sens à partir de la pratique de sa langue maternelle. Et que nous ayons le même mot, en français, pour dire « entendre », c'est-à-dire « ouïr », et « entendre », c'est-à-dire « comprendre », ne me paraît pas procéder du simple hasard.

Outre le *plaisir* qu'on peut éprouver à découvrir et à communiquer du sens, ce dernier nous permet

1. de *voir* : au sens de « porter un regard critique sur », de *juger*, de reconnaître, de valider ;
2. d'*agir* – grâce à notre jugement – en retour sur la réalité physique : se donner rendez-vous, demander un service, monter un meuble suivant un mode d'emploi, suivre une recette de cuisine...

Notre entendement nous permet donc, à travers le sens auquel il nous donne accès, d'exercer nos capacités

1. de *jugement* ;
2. d'*action* (à la lumière de notre jugement).

Afin d'illustrer ce qui précède, regardons ce que permet notre entendement dans les domaines respectifs des nombres, de la géométrie, de la logique ou des probabilités :

	entiers	géométrie	logique	
jugement	les pâtes sont cuites, il manque une personne	ce cube ne rentrera pas dans ce trou, je vois le chemin le plus court pour y aller, vous aller forcément vous croiser	détecter une arnaque rhétorique, repérer une faille dans un raisonnement	j'ai
action	carreler une pièce (combien de carreaux ?), organiser un repas (combien de quantité ?)	construire un cadran solaire, focaliser des rayons lumineux en un point, séparer équitablement une pièce rectangulaire en deux sachant qu'un seul mur fournit en lumière,	blinder ou détruire une argumentation, défendre ou combattre une prise de position, rejeter une décision	joue et pl

[2] Nous parlons ici des cinq sensibilités *physiques* (toucher, ouïe, vue, odorat, vision) à l'exclusion d'éventuelles sensibilités intellectuelle et empathique.

[3] « On n'a rien à redouter du calcul [des probabilités], lorsqu'on est décidé à ne pas régler sa conduite sur ses indications sans les avoir au préalable pesées à leur juste valeur : c'est une illusion singulière de penser que l'indépendance individuelle est accrue par l'ignorance. » (Émile Borel, *Le calcul des probabilités et la mentalité individualiste*, Revue du mois 6 (1908), 641–560)

Signalons tout de suite que notre entendement n'est pas le seul mode de jugement / d'action : il suffira d'évoquer l'empathie ou toute sensibilité (pas la sensiblerie) (non nécessairement intellectuelle) à l'art, l'amour, la vie... lesquelles permettent un autre type de communication.

Toutes les actions qui précèdent se déroulaient dans la réalité physique, dans le monde des sens.

L'action qui se meut uniquement dans le sens, nous la nommerons *acte de penser*. Si l'on cherche à calquer notre duo jugement/action ci-dessus, on se demande naturellement quel est l'acteur de la vision, du jugement, dans le monde du sens : nous l'appellerons *intuition*, dont la terminologie anglaise *insight* évoque bien plus qu'en français la composante « vision »[4]. S'il devait y avoir un créateur de cette vision intérieure, nous ne sommes pas en mesure de le cerner et préférons garder le mystère qui l'entoure.

Question : ce que l'entendement crée, l'être humain le *nomme* : mais que peut-il en *dire* ? Pourquoi même *pourrait*-il en dire quoi que ce soit ? (? ? ? ?tractacus ! ! ! !) (Weyl ! ! !)

Problème : le sens est cristallisé dans une réalité sensible : le *symbole* du langage. Pour communiquer du sens, on communique les *porteurs* de sens, *i. e.* les symboles ; la pensée tend à se confondre avec ce qui l'échafaude – ainsi l'entendement s'égare-t-il.

En effet, le symbole à lui tout seul permet de parler de choses qui dépassent la réalité sensible : des oxymores (« lumière noire »), des contradictions (« oui et non à la fois »), des absurdités (« je mange car je n'ai pas faim »), des paradoxes (le crétois qui affirme « Je mens », l'énoncé vrai de GÖDEL qui affirme « Je ne suis pas démontrable »)... Certaines de ces choses peuvent être très belles et porteuses de sens (par exemple poétique) mais d'autres sont au contraire de véritable monstres, à l'instar (rappelons BERRY) du plus petit entier non-définissable en moins de cents mots ou encore (appelons RUSSELL) du barbier qui décide de raser tous ceux qui ne se rasent pas eux-mêmes et qui n'arrive pas à trancher s'il doit se raser ou non.

? ? ? ?*De la certitude* ! ! ! ! "cette fourchette à est gauche de mon couteau"

L'entendement régit (une partie de) la réalité physique, *a fortiori* chaque regroupement de symbole que rien n'empêche de voir comme un langage vierge de toute interprétation et sans retour sur lui-même. Mais de quel droit l'entendement régirait-il le monde du sens, soumis au langage qui s'incarne dans le monde des sens ? Par une confusion/extension qui se fait sentir plus (trop ?) tard, (? ? ?Métaphore de la Terre avec ou sans gravité, analogue du monde des sens et du monde du sens une fois la gravité coupée, on ne s'en pas compte tout se suite mais on peut partir dans l'espace, prendre du recul sur le monde du sens dont on vient (qui se confondait alors avec le monde ses sens) ? ? ?), à savoir l'*interprétation* de ce langage vierge, là, dans la subjectivité de l'interprétation, se perd la certitude. (Gonseth ? ? ?)

2.3 Le préfixe « h- »

Ce serait mettre la charrue avant les bœufs que de prétendre utiliser les outils logiques et mathématiques que nous présentons (situés au niveau -1 voire -2) afin de définir, raisonner et prouver au sein de la présentation sus-évoquée (faite au niveau 0). Nos « définitions », « théorèmes » et « preuves » n'auront pas encore la rigueur mathématique qu'elles vont permette de définir. Pour rappeler que nous parlerons au niveau 0, celui où l'être ***h***umain *peut juger*, nous mettrons souvent (suivant notre ami Gilles TAUZIN) un préfixe

h- (comme « être ***h***umain »)

devant les terme du langage usuel (niveau 0) possédant une acception en logique ou mathématique (qui fera sens au niveau -1 ou -2) : entier, ensemble, preuve, théorème...

Afin d'alléger la rédaction, on pourra utiliser des synonymes de ces termes participant à plusieurs niveaux de langage : un h-ensemble sera appelé *collection*, une h-suite une *liste*, une h-démonstration une *justification*.

Nous parlerons ainsi de ***h-entiers*** ou de ***h-nombres*** pour parler de « nombres entiers usuels, ceux que l'on utilise pour compter les tomates que l'on achète au marché ou la quantité de carreaux nécessaire pour carreler une pièce. Sur les propriétés des h-entiers, tout le monde peut se mettre d'accord et appliquer sa capacité de jugement.

[4] « William Hamilton utilise une comparaison intéressante : la construction d'un tunnel dans une couche sablonneuse. « Dans cette opération, il est impossible de réussir à moins que chaque mètre – non, chaque centimètre – de notre avance soit assuré par une arche de maçonnerie avant de pousser l'excavation plus avant. Or le langage est exactement pour l'esprit ce que l'arche est pour le tunnel. Le pouvoir de penser et le pouvoir de creuser ne dépendent pas de mots dans un cas ou de maçonnerie dans l'autre ; mais sans ces processus subsidiaires, on ne pourrait aller au-delà d'un commencement rudimentaire. » » (Jacques HADAMARD, *Essai sur la psychologie de l'invention dans le domaine mathématique*)

Les h-entiers sont muni d'un objet singulier – le ***zéro*** – et d'une h-opération unaire – l'***incrémentation*** – tels que chaque h-entier peut être obtenu en incrémentant le zéro un nombre *fini* de fois (principe de *h-finitude* des h-entiers).

Lorsque l'on juxtapose un h-nombre de collections finies, l'on obtient encore une collection *finie* – ainsi peut être définie l'***addition*** des h-entiers. En particulier, incrémenter un h-entier revient à lui ajouter un h-entier singulier nommé ***un***.

L'importance des h-entiers au niveau 0 est capitale : en effet, le jugement humain ne peut traiter *clairement* que de questions d'où l'infini en acte est *exclu* ; or les h-entiers sont certainement les plus à même à permettre un discours sur les questions finitistes.

Au niveau 0*, le mot d'ordre est la* finitude*, véhiculé(e) par les* h-entiers*.*

Sur la modélisation des entiers et l'effondrement de la hiérarchie.

Une fois le cadre logique posé (niveau -1), on pourra *parler* d'objets mathématiques (situés au niveau -2), en particulier d'*entiers* mathématiques, que l'on pourra voir comme un « modèle » des h-entiers usuels (niveau 0). Ainsi, chaque objet logique (situé au niveau -1) qui est h-définissable par les h-entiers (au niveau 0) possède un analogon mathématique (situé au niveau -2) définissable par des énoncés logiques (au niveau -1) arithmétiques (écrits dans le langage des entiers). Cela permet d'utiliser l'attirail démonstratif de ce niveau logique -1 (h-défini au niveau 0 où nous pouvons *juger* de sa validité) pour montrer (toujours à ce niveau -1) des choses sur l'objet logique considéré. De là la possibilité pour des listes de symboles (des preuves) de *prouver* quelque chose sur d'autres listes de symboles (des objets logiques), preuve dont nous sommes pleinement juge. De cette manière, chaque h-théorème portant *sur* la logique (h-théorème énoncé au niveau 0 dont les objets logiques sont situés au niveau -1) peut être « modélisé » par un théorème énoncé *en* logique (au niveau -1) et nous renseigner sur les objets du h-théorème modélisé – c'est la démarche de la *logique mathématique*.

Si l'on escamote l'étape de modélisation, celle qui permet la montée/descente d'un niveau, on fait s'effondrer la hiérarchie des langages qui était le salut de la clarté de notre discours. On comprend ainsi la profonde illégitimité à interpréter des théorèmes *endo*-logiques comme décrivant le cadre *méta*-logique, par exemple des théorèmes modélisant un h-énoncé de prouvabilité typique : « *Il est impossible de montrer que...* ». De là proviennent maint délires philosophiques autour des théorèmes d'incomplétude de Gödel – ces derniers menant pourtant droit à une contradiction[5] si l'on ne dissipe pas cette confusion.

Il semble cependant difficile de concevoir la modélisation des h-entiers autrement que par les entiers mathématiques, de modéliser l'arithmétique d'une autre façon que par les axiomes de Peano, de modéliser la prédication autrement que par la logique des prédicats... Une bonne leçon d'humilité[6].

2.4 h-arithmétique et énumérabilité de listes

> Tout ce que j'essaie en réalité de faire est de scruter la différence entre comptage en mathématique et comptage ordinaire, et la différence entre proposition mathématique et proposition d'expérience.
>
> Ludwig Wittgenstein, *Cours sur les fondements des mathématiques* (Cambridge, 1939).

Au sujet des listes finies génériques.

Il est usuel en mathématique de noter une liste en numérotant ses objets par des h-entiers successifs écrits en indice, par exemple : $a_1, a_2, ..., a_n$ où n est un symbole désignant le h-nombre d'objets dans la liste (et où les virgules séparent les objets). Mais cette indexation est un *artifice* nuisible au niveau 0 de langage où nous

[5] à savoir : l'existence de *h-entiers non finis*. L'argument nécessite des rudiments de sémantique prédicative (présentée dans le cours correspondant) et peut être présenté de la façon suivante.

Soit T une théorie consistante codant l'arithmétique. Le second théorème d'incomplétude de Gödel nous dit que sa consistance C (qui est un énoncé de T) n'est pas prouvable. On peut donc rajouter sa négation et obtenir une théorie $T' := T \cup \{\neg C\}$ qui reste consistante (lemme classique et facile). Par complétude de la logique prédicative, cette théorie T' admet un modèle. Considérons alors les entiers de ce modèle et supposons qu'ils soient finis. L'énoncé $\neg C$ étant vrai dans ce modèle (c'est un axiome de T'), son interprétation fournit une preuve d'une contradiction à partir de T, *a fortiori* à partir de T', ce qui montre que T' est inconsistante. Contradiction !

[6] Le niveau 0, pourvu d'un langage, semble dénué d'objets au-delà de la sphère de la finitude. Au contraire, le langage semble inexistant au niveau -2 tandis que ses objets (mathématiques) s'imposent grâce au langage logique du niveau -1. C'est par écrasement de la hiérarchie langagière que les objets mathématiques remontent au niveau 0, envahissent la sphère de la finitude et déchirent sa frontière de l'intérieur, semant la confusion lorsque le langage vient y réclamer et exercer son contrôle.

sommes : si une liste est formée d'un h-nombre donné d'objets, cela doit se voir *directement* en comptant les objets la composant – et non en lisant les indices. Par exemple, la liste $\square, \lozenge, \triangle, \heartsuit$ est manifestement constituée de quatre objets, tout comme la liste $a_2, a_7, a_{90}, a_{5681903}$ (pas besoin de lire les indices). Ce dernier exemple montre qu'il est plus simple de lister quatre objets sous la forme de quatre symboles « bruts » (par exemple a, b, c, d) plutôt que de les lister à travers une indexation d'un symbole générique (par exemple a_1, a_2, a_3, a_4).

Nous préférerons par conséquent décrire une liste générique d'objets à l'aide d'un alphabet

$$a, b, c, ..., z$$

où les points de succession permettent

1. d'éluder l'écriture des symboles précédant la dernière lettre (ils constituent une *abréviation*) ;
2. de suggérer que cette dernière lettre peut être précédée d'*autant de lettres que voulu* (ils indiquent le caractère *générique*). Le lecteur ne doit par conséquent pas se focaliser sur le fait que l'alphabet français finit par un z et contient vingt-six lettres, on pourrait tout à fait prolonger cet alphabet en s'inspirant des plaques minéralogiques : $..., w, x, y, z, aa, ab, ac, ad...$

Ainsi s'énoncera la h-validité du principe de récurrence qui *indique* le moyen d'obtenir une preuve pour chacun des h-énoncés d'une liste finie donnée.

h-principe (récurrence).

Considérons un certain h-nombre d'énoncés $A, B, C, ..., Z$. On suppose que :

1. *le premier énoncé A est un théorème ;*
2. *dès qu'un énoncé autre que le dernier est prouvé, le prochain par ordre alphabétique l'est également.*

Alors chacun des énoncés $A, B, C, ..., Z$ est un théorème.

Justification.

On part du théorème A (point 1), on en déduit B (point 2), puis C (point 2), puis D (point 2), puis de proche en proche (grâce à la h-finitude du h-nombre d'énoncés) chaque énoncé jusqu'à Z.

Donnons à présent quelques rudiments de ***divisibilité*** pour aboutir à une numérotation possible des énoncés logiques. On dira d'un h-entier qu'il est ***premier*** s'il n'est pas produit de h-entiers strictement plus petits. On pourra vérifier que les h-entiers premiers inférieurs à 100 sont les suivants :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

h-corollaire (décomposition en facteurs premiers).

Chaque h-entier supérieur ou égal à 2 est produit de h-entier premiers.

Justification.

Puisque 2 n'est pas produit de 0 ou de 1, il est premier, ce qui permet d'amorcer une h-récurrence.

Considérons ensuite un h-entier n supérieur ou égal à 2 et supposons (hypothèse de récurrence) chacun des h-entiers successifs $2, 3, 4, ..., n$ décomposable en produit de h-nombres premiers. Alors : ou bien le h-entier $n+1$ est premier (ce qui montre l'énoncé suivant l'hypothèse de récurrence), ou bien il est produit de h-entiers strictement plus petits que l'on peut décomposer (par hypothèse de récurrence) en produits de h-entiers premiers, d'où une décomposition.de $n+1$ en h-entiers premiers en faisant le produit de ces décompositions (en vertu de la stabilité de la h-finitude par juxtaposition), ce qui montre également l'énoncé suivant l'hypothèse de récurrence.

On insistera sur le *caractère algorithmique* de cette h-démonstration, marque de la h-récurrence, même si son efficacité dépend de notre capacité à tester la primalité d'un h-entier donné (il suffit de poser la division par chaque h-entier plus petit, ce qui est aussi trivial que long).

L'unicité de cette décomposition (*cf.* exercices) montre que la numérotation suivante, où les h-entiers apparaissant dans le produit forment les h-entiers premiers, énumère les listes finies de h-entiers :

à une liste finie de h-entiers $a, b, c, d, e...$ associer le numéro $2^a 3^b 5^c 7^d 11^e \cdots$ et réciproquement.

h-corollaire (énumérabilité des h-suites finies).
On peut énumérer les h-suites finies de h-entiers.

Ce h-corollaire a de quoi choquer : il est déjà surprenant que les couples de h-entiers soient énumérables (nous l'avons h-prouvé en introduction à l'aide d'une énumération « en serpent ») ; on peut à la rigueur imaginer étendre l'argument aux triplets de h-entiers, voire aux listes de h-entiers possèdant un h-nombre déterminé d'objets ; mais aux listes possèdent un nombre *arbitraire* d'objets, cela semble très fort.

En revanche, il ne sera pas possible d'énumérer les listes d'h-entiers *infiniment longues*, comme nous l'avons h-montré en introduction par un argument diagonal de CANTOR sur les suites de décimales des nombres de $[0, 1]$.

h-théorème[7] **(non-énumérabilité des h-suites infinies).**
Il est impossible d'énumérer les h-suites infinies[8] *de h-entiers.*

L'intérêt du h-corollaire ci-dessus n'apparaîtra que pour celui intéressé par la logique mathématique, en vue de comprendre ce que signifient au juste les (h-?)théorèmes de cette dernière – qui traitent souvent de (non-)prouvabilité, à l'instar des (h-?)théorèmes de GÖDEL. Le point à retenir est le suivant : une preuve étant fondamentalement quelque chose de *fini*, chaque énoncé parlant de preuve ne parle que d'agencements de listes de symboles. Le h-corollaire dit précisément que ces agencements sont codables *par les entiers* à travers la possibilité d'*énumérer effectivement les formules* écrites dans un langage donné :

les h-énoncés de la logique mathématique (prouvabilité & Co.) peuvent être entièrement modélisés par des énoncés arithmétiques (dans le langage des entiers).

3 Introduction résumée

> Avant de peindre, il faut un fond blanc. Avant d'apprendre, il faut désapprendre.
>
> CONFUCIUS, *Préceptes de vie.*

3.1 Pourquoi réduire les énoncés mathématique à des suites de symboles

> about the reality [...] of propositions. I am entirely unable to exorcise my craving for real propositions, a weakness which is after all only natural in a mathematician, to whom mathematical theorems ought to be the first basic reality of life. But I can find no sort of encouragement wherever I turn.
>
> G. H. HARDY, *Mathematical proof* (publié dans *Mind*, janvier 1929).

Il aura fallu attendre la fin du XIX^{e} siècle avec l'établissement de l'irréductibilité du cinquième postulat aux autres axiomes de la géométrie euclidienne pour admettre la *polysémie* en mathématique. Peu de temps après, le paradoxe de BERRY (ou de RICHARD) nous rappelle la différence de nature entre *signifiant et signifié*[9].

[7] Ce résultat ne nous permet pas à ce stade méta-(méta-)mathématique d'affirmer qu'il existe des infinis plus grands que d'autres car il faudrait pouvoir, d'autre part considérer un infini *en acte*, d'autre part *comparer* les infinis. Cela deviendra possible *dans* la mathématique.

[8] On parle ici d'infini *potentiel* et non actuel, de suites dont chacune est arbitrairement longue.

[9] Un autre paradoxe (attribué à RUSSELL) est souvent associé à celui de BERRY : en considérant la collection C des collections qui ne s'appartiennent pas à elle-mêmes, ce qui s'écrit $c \in C \iff c \notin c$ pour chaque collection c, instancier $c \leftarrow C$ donne une contradiction. Ces deux paradoxes participent en effet tous deux de la limitation de la *séparation* (acte de considérer la collection des objets vérifiant une propriété donnée, les séparant ainsi des autres).

Il est cependant impensable, tant qu'est présente l'identification du symbole $\in$ à son interprétation naïve (l'appartenance), d'imaginer le paradoxe de RUSSELL : quel sens alors un objet aurait-il à s'appartenir à lui-même, tel un serpent mordant sa queue ? C'est seulement une fois le paradoxe de BERRY élucidé (différencier signifiant et signifié) que RUSSELL peut attaquer et mettre en lumière un *tout autre* problème de la séparation : celui de l'univers où l'on sépare (la solution adoptée est de prendre pour ce dernier un ensemble *pré*déterminé).

Ainsi, le véritable paradoxe de RUSSELL vient de la considération de « grosses » collections et non de l'identification abusive du symbole $\in$ avec son interprétation naïve (chair du paradoxe de BERRY où le symbole mésinterprété est le groupe de lettres « définissable »).

Ces deux trivialités linguistiques nous amènent à nous concentrer sur le *signifiant* (les symboles, la logique), le sens étant une affaire de théologie.

Nous *croyons* d'ailleurs personnellement que le sens est le plus éclairant, le plus important à saisir (de même que la pensée prévaut trivialement sur la grammaire) ; mais, face à des hordes d'élèves ne nous comprenant pas sur ce terrain sémantique,

1. nous croyons indispensable de *démystifier* les objets mathématique ainsi que les « preuves » des « vérité » portant sur ces derniers (celui qui ne « voit » pas en maths n'est pas condamné à la stupidité, nous voyons tous la « réalité » à travers nos filtres personnels, nous avons tous des critères de conviction différents). L'élève qui, suite à l'adage professoral « *en maths on prouve tout ce qu'on affirme !* », demande ce qu'*est* au juste une preuve, celui-ci est très intelligent. S'il a l'éclair de demander en outre de *quoi* une preuve parle-t-elle au juste, cet élève sera sans doute très incompris car il aura mis le doigt sur les deux pôles fondamentaux de la mathématique : son *objet*, son *discours*. Bien heureux qui prétendrait lui répondre objectivement sans immiscer dans sa réponse des croyances personnelles.
2. nous croyons possible d'*éclairer ce sens* primordial par un soin accordé au *symbolisme logique*. Ce dernier doit évidemment être accompagné d'*autres ressorts humains* car une étude grammaticale n'a jamais dévoilé une pensée, elle n'en est qu'un outil de compréhension ; cependant, s'il est une displine *discursive* où la syntaxe dévoile au plus haut point la force de conviction d'un discours ainsi que ses objets, c'est bien la mathématique – qui par ce même caractère nous révèle ses limites en matière de vérité.

3.2 Pourquoi réduire les preuves mathématique à des suites de symboles

Le paradoxe de CAROLL nous invite à *oublier le sens* d'une implication (sens qui se résume à une croyance) et à différencier dans une preuve ses *objets* (à ce titre, une implication $a \implies b$ ne se distingue pas d'une conjonction $p \wedge q$) de ses *règles*, à considérer la preuve comme un *jeu*. Écoutons WITTGENSTEIN[10] :

> Il nous faut [...] faire une distinction : entre les configurations de base du calcul (les bases de départ dans le jeu) d'une part, et d'autre part les règles qui indiquent comment nous avons à passer d'une configuration à une autre. C'est ce que Frege a déjà expliqué dans sa critique des théories de Heine et Thomae : « C'est une surprise. Si quelqu'un demandait qu'elles sont les règles du jeu d'échecs, que dirait-il si, pour toute réponse, on lui montrait un groupe de pièces sur l'échiquier ? Probablement qu'il ne peut pas y trouver de règle parce qu'il n'attache aucun sens à ces figures et à leur configuration.»

Selon le parallèle échiquéen ci-dessus, une implication $a \implies b$ est une *position* (tout comme une disjonction $u \vee v$), elle n'aurait aucun sens à être valide, tandis qu'une inférence $a \vdash b$ est une *règle* et non une déduction causale (la position b n'aurait pas de sens à être « causée » par la position a).

3.3 Fondements des mathématiques : le jeu et l'entendement

Rappelons les quatre points fondateurs de la mathématique, qui se résument au *jeu*[11] et à l'*entendement* :

1. pouvoir *juger* si une règle de jeu est respectée/suivie ou non ;
2. pouvoir *appliquer* une règle de jeu ;
3. pouvoir appliquer *successivement* plusieurs règles de jeu ;
4. pouvoir *mettre du sens* dans ce qu'on dit/écrit/lit/entend/fait (témoin : sa langue maternelle).

Les points 2 et 3 concernent l'*acte* du jeu (que l'on pourrait aussi appeler *calcul*) tandis que le point 1 traite de l'*acceptation*, de la *reconnaissance* de cet acte. Le point 4 permet d'interpréter le niveau logique (-1) au niveau mathématique (-2) ? ? ? ? ?.

[10] deuxième appendice des *Remarques philosophiques* éditées chez *tel* GALLIMARD

[11] Nous laissons ici de côté toutes les considérations psychologiques (sans doute les plus importantes) liées au jeu – par exemple leur caractère déterminant et irremplaçable lors du développement de l'enfant – à l'exception d'une : le *plaisir*. Nous espérons ainsi que le mot *jeu* évoquera cette composante indispensable à l'accomplissement de tout travail – fût-il limité à la reconnaissance et l'application de règles.

3.4 Esquisse de plan

> La plupart des raisonnements qui se dont, soit dans la vie courante, soit dans les sciences, ne rentrent pas dans le cadre étroit de la logique rigoureuse et sont mal formalisables, voire absolument non formalisables. Beaucoup de gens, que l'histoire a charitablement oubliés, ont essayé de mettre un peu de formalisme dans ces raisonnements. À chaque « donc », on s'aperçoit que quand on le formalise, on est obligé d'introduire une cascade mineures qui sont beaucoup plus contestables que le « donc ».
>
> La logique mathématique est un noble effort pour formaliser ce qui peut l'être mais, si j'ose dire, la réalité reste en deçà.
>
> Marcel-Paul SCHUTZENBERGER, *Triangle de pensée* (2000).

Pourquoi en mathématique parler de preuve ? Pour atteindre du vrai, on part de vrai puis on raisonne – et l'on escompte bien que tout ce qui soit ainsi obtenu à partir de vrai soit également vrai. La preuve est donc un *pont de vérité*, le pont rationnel par excellence, socle du *principe de cohérence* du discours mathématique.

Comme nous le rappellent les tribunaux et les mystiques, ce pont est cependant loin d'atteindre chaque vérité. Il n'est pas non plus un gage de compréhension globale comme nous l'explique Alain CONNES dans cet extrait de *Matière à pensée* (1989) :

> Les mathématiciens savent bien que comprendre un théorème ne signifie pas comprendre pas à pas une démonstration dont la lecture peut durer plusieurs heures. C'est au contraire voir la totalité de cette démonstration en un temps extrêmement bref. Le cerveau doit être capable de « vérifier », j'ignore comment, cette démonstration en l'espace d'une ou deux secondes. On est certain d'avoir compris un théorème si l'on a ce sentiment-là. Pas si l'on est capable de parcourir la démonstration sans trouver d'erreur, ce qui ne donne qu'une compréhension locale.

Nous considérons une notion de preuve *syntaxique*, *symbolique*, à savoir une suite *finie* de proposition dont chacune est ou bien déjà connue ou bien déduite des précédents par des *règles* à préciser.

En mathématique usuelle, la seule règle d'usage est le *modus ponens* : pouvoir, à partir de A et de $A \Longrightarrow B$, déduire B.

Si l'on peut associer une *valeur de vérité* à chaque proposition, deux questions se posent alors :

1. ***cohérence***[12] (si prouvable, alors vrai) : tout ce qui est prouvé à partir de vrai est-il également vrai ? Il semble impensable de s'en passer car l'on veut préserver la cohérence du discours mathématique ;
2. ***complétude*** (si vrai, alors prouvable) : les preuves suffisent-elles à atteindre tout le vrai ?

Chaque lien entre *prouvable* et *vrai* esquissera un lien entre syntaxique et sémantique, menant à la question fondamentale suivante : « *comment interpréter une suite de symboles ?* ». Un théorème de complétude est ainsi un pont entre sémantique et syntaxique – en fait, vu la cohérence automatique, c'est surtout un retour du sémantique vers le syntaxique.

Illustrons cette démarche en reprenant l'échiquier de FREGE cité par WITTGENSTEIN.

Une partie sera une « preuve », suite de positions dont chacune se déduit de la précédente selon un coup légal (parmi peut-être d'autres possibles) à l'exception de la première qui est érigée en axiome.

Une position est définie comme chaque association d'au plus une pièce (pion, cavalier, fou, tour, dame, roi) par case d'un échiquier carré formé de huit traverses et huit colonnes[13].

On dira qu'une position est valide si :

1. chaque couleur possède au plus seize pièces dont un unique roi et au plus huit points qui sont tous exclus des première et dernière traverses ;
2. les rois ne sont pas en contact.

Il est clair que la position de départ (axiome) est valide et que la validité est préservée lorsqu'un coup est joué (même en cas de prise/promotion), de sorte que chaque position prouvable est valide, d'où la cohérence de notre logique échiquéenne.

Notre définition de la validité n'est cependant pas assez fine pour coïncider avec la prouvabilité (existe-t-il une partie qui mène à la position valide donnée ?) comme le montrent les contre-exemples suivants :

[12] d'autres auteurs (dont Jean-Yves GIRARD) parlent de ***correction***

[13] Pour que notre modélisation soit la plus rigoureuse, il conviendrait de rajouter les trois données suivantes : 1) à qui est le trait ; 2) est-ce que le dernier coup joué est une avancée d'un pion de deux cases et si oui lequel (pour autoriser le cas échéant une prise en passant) ; 3) pour chaque couleur, est-ce que le roi a été déplacé (ce pour interdire le roque le cas échéant).

1. la position de départ où l'on a déplacé une des tours/dames sur l'une des cases du centre ;
2. chaque position avec un double échec fait avec deux tours ;
3. une situation où l'une des couleurs a tous ses pions et ses deux fous de la même couleur.

Par conséquent, notre logique échiquéenne sera incomplète.

Remarquons également un de ses aspects singuliers : en cas de coup(s) forcé(s), la preuve s'écrit *d'elle-même*, ce qui n'arrive jamais dans les logiques classiques où l'on peut toujours incorporer un axiome à n'importe quel moment.

On va (h-)montrer que les logiques des propositions et des prédicats sont complètes (elles seront bien sûr cohérentes). De plus, la possibilité d'une interprétation d'une théorie validant ses axiomes reviendra à sa non-contradiction (un sens seulement est trivial, l'autre est non constructif). En revanche, chaque théorie exprimant l'arithmétique sera incomplète.

4 Présentation des logiques naïve, propositionnelle et prédicative

D'un point de vue très général, une ***logique*** est définie par la donnée :

1. d'un concept de ***formule*** (son objet : de quoi parle la logique) ;
2. d'un concept de ***preuve*** (son acte : que fait-on en logique ? on prouve) ;
3. d'un concept de ***théorème*** (objet particulier : littéralement « digne d'être contemplé ») ;
4. d'un concept d'***interprétation*** (ce qu'elle permet de modéliser, le plus souvent une valeur de vérité).

Ce cours vise à décrire la logique des *prédicats*, dont l'énoncé des axiomes présuppose la logique des *propositions*.

4.1 Logique naïve

En logique naïve, une formule est tout ce dont on peut dire qu'il est vrai ou faux (définition d'une *pensée* chez Frege), fournissant ainsi une interprétation triviale (le vrai ou faux associé à la formule). Une preuve est un *raisonnement* (suite de formules) convainquant. Un théorème est une formule située en conclusion d'une preuve.

On peut construire d'autres formules à l'aide de connecteurs logiques exprimés par le langage usuel : « *et* », « *ou* », « *ou bien* », « *si... alors...* », « *est équivalent à* », « *est incompatible avec* ». Par exemple : « Si je suis un homme, alors j'ai de la barbe et j'allaite mon enfant » (au passage, l'interprétation de cette formule pourra sembler ambigüe si elle est énoncée par une femme).

Nous avons vu en introduction les limites d'une telle logique.

4.2 Logique propositionnelle

La logique propositionnelle ne s'intéresse pas à *ce que disent/énoncent* les formules mais seulement à *la façon dont elle se décomposent* en d'autres formules.

On part ainsi de formules *atomiques* – au sens propre : qui ne peuvent être décomposées –, par exemple les lettres d'un alphabet, puis on les *connecte* avec des symboles dits de connexion logique parmi

$$\neg \ , \quad \wedge \ , \quad \vee \ , \quad \Longrightarrow \ , \quad \Longleftarrow \ , \quad \Longleftrightarrow \quad \text{et} \quad \mid \ .$$

On peut ainsi obtenir la formule

$$[(p \implies q) \wedge \ (\neg\,(q \iff \mathbb{F}) \ \mid s)] \impliedby p.$$

Les parenthèses et crochets sont simplement là pour lever l'ambiguïté de composition : comment savoir sinon si $a \vee b \wedge c$ représente la formule $(a \vee b) \wedge c$ ou la formule $a \vee (b \wedge c)$?

Certaines formules, interprétées naïvement, apparaissent vraies quel que soit le sens de ses atomes : c'est le cas par exemple de $p \wedge q \Longrightarrow p$ (c'est le sens usuel de la *con*jonction, du « *et* »), de $x \Longrightarrow y \vee x$ (sens inclusif du « *ou* »), de $a \Longrightarrow a$ (chaque proposition peut être déduite d'elle-même : il n'y a rien à faire !) ou encore de $(u \Longrightarrow \mathbb{F}) \Longrightarrow \neg u$ (si une proposition entraîne une contradiction, alors elle ne peut être réalisée). On choisit un certain nombre de telles formules naïvement vraies que l'on nommera *axiomes*.

Une *preuve* est alors une suite de formules dont chacune est, ou bien un axiome, ou bien déduite des précédentes par la *règle* suivante : à partir d'une formule a et d'une formule de la forme $a \Longrightarrow b$, on peut déduire la formule b (le *modus ponens*, sens naïf de l'implication). Un *théorème* est la dernière formule d'une preuve.

Pour interpréter une formule, on commence par interpréter ses atomes en leur attribuant une *valeur de vérité* (vrai ou faux) puis l'on se donne un moyen d'obtenir l'interprétation d'une formule $a * b$ connaissant le connecteur $*$ et les interprétations des formules a et b. Une formule qui est vraie quelle que soit l'interprétation de ses atomes est appelée une *tautologie*. Par exemple, chaque axiomes est une tautologie.

Ce qu'il y a à retenir de la logique propositionnelle, c'est que *chaque* tautologie peut être prouvée à partir d'un nombre *fini* de tautologies judicieusement choisies (et dont l'évidence naïve[14] ne fait doute) :

les tautologies sont exactement les théorèmes.

Ces quelques tautologies-axiomes captent donc à elles seules *tout* le vrai que peut énoncer (et prouver) la logique propositionnelle.

4.3 Logique prédicative

Présentons à présent la logique prédicative. La *prédication* (qui n'est pas la *prédiction*) est l'acte d'affirmer que des objets vérifient ou non une certaine condition, appelée *prédicat*.

Un prédicat *atomique* exprimera que ses termes sont dans une certaine *relation*, un *terme* étant construit à partir d'un alphabet (symboles d'objet) et de symboles de composition. On regarde alors les formules créées à partir, d'une part des prédicats atomiques, d'autre part des connecteurs logiques et des quantificateurs (qui jouent le rôle de conjonctions ou disjonctions généralisées). Par exemple :

1. $\forall n,\ \exists a,\ \exists b,\ \mathfrak{p}(a) \wedge \mathfrak{p}(b) \wedge (2n = a + b)$ exprime que chaque objet « double » est somme de deux objets vérifiant chacun le prédicat $\mathfrak{p}$ (dans les entiers supérieurs à 3, c'est l'énoncé de la conjecture de Goldbach lorsque $\mathfrak{p}$ dénote la primalité) ;
2. $\forall D,\ \forall \Delta,\ [\mathfrak{d}(D) \wedge \mathfrak{d}(\Delta) \wedge D \perp \Delta] \Longrightarrow [\exists i,\ \mathfrak{p}(i) \wedge i \in D \wedge i \in \Delta]$ exprime que, étant donnés deux objets quelconques vérifiant la relation $\perp$ et chacun le prédicat $\mathfrak{d}$, il existe un objet vérifiant le prédicat $\mathfrak{p}$ et « appartenant aux » deux objets considérés (en géométrie, lorsque $\mathfrak{d}$ et $\mathfrak{p}$ dénotent respectivement le fait d'être une droite et un point, cette thèse affirme que deux droites orthogonales ont toujours un point en commun – si l'on interprète les symboles $\in$ et $\perp$ comme les relations respectives d'appartenance et d'orthogonalité) :
3. $\exists \Theta,\ \forall o,\ \Theta \geq o$ exprime qu'il y a un objet « plus grand que » chaque autre.

La logique prédicative introduit un nouveau type de formule appelée *invocation*, symbolisant l'invocation d'un objet mathématique par la formule magique

« *Soit o un objet vérifiant...* ».

L'intérêt des invocations est de prouver des énoncés universels : pour pouvoir affirmer $\forall o, P(o)$, il suffit d'invoquer un objet o et de montrer l'énoncé $P(o)$ pour l'objet o invoqué.

Voyons les règles et axiomes. On conserve la règle du *modus ponens*. Chaque tautologie propositionnelle fournit par ailleurs un axiome après remplacement des atomes (propositionnels) par n'importe quels énoncés (prédicatifs). On rajoute d'autres axiomes et règles collant à l'interprétation naïve des quantificateurs et des invocations, par exemple : à partir de « *Soit o tel que* $P(o)$ » et $Q(o)$, pouvoir déduire $\forall z, P(z) \Longrightarrow Q(z)$ (la raison d'être des invocations).

[14] Certains axiomes, à l'instar du tiers-exclu $\neg\neg a \Longrightarrow a$, ne font toutefois pas l'unanimité. On est libre de les rejeter, ce qui conduit à une autre logique, tout aussi respectable – mais beaucoup moins usitée.

Une *preuve* est alors (comme en logique propositionnelle) une suite de formules dont chacune est : ou bien un axiome, ou bien une hypothèse, ou bien déduite des précédentes par une règle. Un *théorème* est la dernière formule d'une preuve – relativement aux hypothèses données.

Quant à l'interprétation, l'architecture des énoncés fait qu'il suffit d'interpréter les symboles d'objets et ceux de relation, les tables d'interprétation des connecteurs et quantificateurs faisant le reste : on trouve au final une valeur de vérité. En attribuer à une invocation serait cependant un non-sens puisque l'interprétation naïve d'une invocation est un *acte* (et non un *énoncé*).

On retiendra de la logique prédicative les points suivants :

1. **Généralisation.** Les invocations servent à prouver des énoncés universels – de la forme $\forall r, \varphi(r)$;
2. **Cohérence.** Lorsque, dans un preuve, les hypothèses sont vraies selon une interprétation, alors les conclusions sont également vraies selon cette même interprétation ;
3. **Polysémie.** La vérité d'un énoncé (prédicatif) dépend *a priori* de l'interprétation de ses termes.
4. **Incomplétude.** Un énoncé *vrai* selon une interprétation peut être faux selon une autre et *peut* ainsi (par cohérence) *ne pas être prouvable.*
5. **Complétude.** Les énoncés vrais selon *chaque* interprétation (les tautologies) sont exactement les énoncés prouvables (les théorèmes). (? ? ? preuve constructive ? ? ?)

5 Exercices de h-arithmétique

On considère deux h-entiers relatifs[15] notés d et m. On dira que d ***divise*** m si l'on peut trouver un h-entier relatif q tel que $m = dq$. On dit alors également que d est un ***diviseur*** de m ou que m est un ***multiple*** de d.

Étant donnés plusieurs h-entiers, ces derniers seront qualifiés d'***étrangers*** si leur seul diviseur (positif) commun est 1.

1. **h-nombres premiers étrangers.** *Considérant deux h-entiers premiers distincts, montrer qu'ils sont étrangers*[16] *.*
2. **Stabilité des multiples par combinaison linéaire.** *Montrer que, dès qu'un même h-entier divise deux h-entiers a et b, il alors divise chaque h-nombre de la forme $\lambda a + \mu b$ avec λ et μ des h-entiers relatifs.*
3. **Division euclidienne.** *On se donne un h-entier a (appelé **dividende**) et un h-entier non nul b (appelé **diviseur**) : montrer que le h-entier a s'écrit comme somme d'un multiple du h-entier b et d'un h-entier (appelé **reste**) compris entre* 0 *(au sens large) et b (au sens strict).*
4. **Invariance de diviseurs.** *On considère une division euclidienne et un h-entier d : montrer qu'il revient au même de dire que d divise le dividende et le diviseur ou que d divise le diviseur et le reste.*
5. **h-théorème de** Bézout**.** *Donnons deux h-entiers étrangers notés # et § . Décrire une construction de deux h-entiers relatifs λ et μ tels que $\lambda\# + \mu\S = 1$. (On pourra effectuer des divisions euclidiennes successives où les diviseur et reste d'une division deviennent les dividende et diviseur respectifs de la suivante puis regarder le dernier reste non nul.) Traiter explicitement le cas des h-entiers* 13 *et* 25*.*
6. **h-lemme d'**Euclide**.** *Considérons un h-entier premier p et un h-entier non nul m multiple de p. Montrer alors que p vaut l'un des facteurs de chaque factorisation de m en produit de h-nombres premiers.*
7. **Unicité de la décomposition en facteurs premiers.** *On considère un h-entier n supérieur à* 1 *et l'on désigne par p un h-nombre premier. On note v_p le plus grand h-entier tel que p^{v_p} divise n. Montrer alors que chaque décomposition de n en produit de premiers contient le facteur p^{v_p}.*

Justifications.

[15] Si la tournure de phrase considère *une* configuration (et en nomme des "éléments", ici d et m), c'est uniquement à fins de clarté de la définition. Il faut bien comprendre que la configuration décrite doit ensuite et immédiatement être pensée comme *générique*, au sens où la terminologie donnée concerne *chaque* configuration rencontrable (ici la donnée de deux h-entiers relatifs). Il serait ridicule de ne pas donner sens à « 3 divise 18 » sous prétexte que, dans notre définition, l'on ne sait pas si d vaut 3 !

[16] Comme pour la définition ci-dessus, la consigne est *générique* : on demande d'établir l'extranéité de *chaques* h-entiers premiers distincts (au nombre de 2).

1. Notons p et q nos h-nombres premiers et considérons-en un diviseur positif commun d. Puisque p est premier, d ne peut valoir que ou bien 1 ou bien p ; de même, la primalité de q impose que d vaille ou bien 1 ou bien q. Or p et q ne sont pas égaux (par hypothèse) et diffèrent de 1 (par primalité), ce que ne laisse qu'un seul cas possible : $d = 1$.

2. Écrivons $a = nu$ et $b = nv$ pour certains h-entiers relatifs u et v, d'où il sort $\lambda a + \mu b = (\lambda u + \mu v)\, n$, ce qui conclut.

3. On soustrait successivement le h-entier b du h-entier a tant que l'on conserve un résultat positif. Cela s'arrête par finitude des h-entiers, appelons q le h-nombre de soustractions ainsi possibles. Alors le h-nombre positif $a - qb$ ne peut être supérieur à b sinon l'on aurait pu effectuer une soustraction supplémentaire.

4. Posons notre division euclidienne sous la forme $a = bq + r$. Supposons que d divise a et b : par le point 3, il divise également la combinaison linéaire $1a + (-q)\, b = r$. Supposons cette fois que d divise b et r : toujours par le point 3, il divise aussi la combinaison linéaire $bq + 1r = a$.

5. Effectuons les divisions euclidiennes suggérées (on note $A, B, C, D...$ les quotients et $a, b, c, d...$ les restes) :

$$\# = \S A + a, \qquad \S = aB + b, \qquad a = bC + c, \qquad b = cD + d, \qquad c = dE + e, \qquad d = eF + f... \tag{1}$$

Observer que l'on peut supposer le premier reste a non nul : dans le cas contraire, le h-entier § divisera #, donc sera un diviseur commun à § et #, ce qui impose (par hypothèse d'extranéité) $\S = \pm 1$, d'où le résultat en écrivant $1 = \pm\S + 0\#$.

Vu les ordinations reliant restes et diviseurs $\S > a > b > c > d > \cdots \geq 0$, la suite des divisions doit s'arrêter en un nombre fini d'étapes. Or elle continuera dès que le reste précédent (le nouveau diviseur) est non nul, ce qui est le cas du premier reste a : on peut donc considérer le dernier reste non nul z :

$$..., \; w = xY + y, \qquad x = yZ + z, \qquad y = z\Omega. \tag{2}$$

Puisque z divise z et 0, le point 3 précédent montre que le h-entier z divise également # et §, donc vaut 1 d'après le point 4. L'avant-dernière égalité de (2) devient donc

$$1 = x - yZ.$$

En récrivant à l'aide des égalités (1) chaque reste $y, x, w, v, u, ..., c, b, a$ comme combinaison linéaire des deux restes précédents, on obtient une instance de l'expression $x - yZ$ dont le résultat est une combinaison linéaire de # et §, d'où les h-entiers relatifs cherchés.

Le procédé algorithmique des divisions euclidiennes et des instanciations assure que la construction est effective.

Dans le cas de 25 et 13, Les divisions successives donnent

$$25 = 13 + 8, \qquad 13 = 8 + 5, \qquad 8 = 5 + 3, \qquad 5 = 3 + 2, \qquad 3 = 2 + 1.$$

On en déduit successivement (on souligne les restes/diviseurs pour les distinguer des coefficients entiers)

$$\begin{aligned} 1 &= \underline{3} - \underline{2} \overset{\text{remplacer } \underline{2}}{=} \underline{3} - (\underline{5} - \underline{3}) = 2 \cdot \underline{3} - \underline{5} \overset{\text{remplacer } \underline{3}}{=} 2\,(\underline{8} - \underline{5}) - \underline{5} = 2 \cdot \underline{8} - 3 \cdot \underline{5} \\ \overset{\text{remplacer } \underline{5}}{=} 2 \cdot \underline{8} - 3\,(\underline{13} - \underline{8}) &= 5 \cdot \underline{8} - 3 \cdot \underline{13} \overset{\text{remplacer } \underline{8}}{=} 5\,(\underline{21} - \underline{13}) - 3 \cdot \underline{13} = 5 \cdot \underline{21} - 8 \cdot \underline{13}. \end{aligned}$$

6. On raisonne par h-récurrence sur le nombre de facteurs premiers des décompositions de m.

Si ce nombre vaut un, alors m est produit d'un h-nombre premier, *a fortiori* est premier, donc le diviseur p vaut ou bien 1 (valeur exclue par primalité de p) ou bien m (ce qu'il fallait démontrer).

Supposons à présent que m se décompose sous la forme $q\pi$ où q est un h-entier premier et π un h-entier non nul. Si $p = q$, on a terminé. Sinon, les points 1 et 5 s'appliquent : on peut écrire $\lambda p + \mu q = 1$ pour certains h-entiers relatifs λ et μ. Alors le h-nombre p divise la combinaison $(\lambda\pi)\, p + \mu\,(q\pi) = \pi$, ce qui permet de conclure par récurrence vu que π a un facteur premier en moins que $q\pi$.

7. Considérons deux décompositions en facteurs premiers d'un même h-entier strictement positif. On simplifie par chaque facteur premier qui apparaît dans les deux décompositions et on note n la valeur du h-nombre ainsi obtenu après simplification : l'unicité cherchée revient précisément à l'égalité $n = 1$. Si cette dernière n'est pas vérifiée, il reste un facteur premier p dans une décomposition de n (donc p divise n) mais pas de l'autre (donc, par le point 6, p ne peut pas diviser n), d'où une contradiction.

Pour répondre à la question posée, il nous suffit d'établir la décomposition de n en produit des p^{v_p} pour p parcourant les h-nombres premiers (produit qui fait sens puisque ses facteurs valent tous $\pi^0 = 1$ au-delà d'une certaine valeur). On a déjà établi qu'il *existait* une décomposition, mettons $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ où les p_i désignent des h-nombres premiers deux à deux distincts. Alors chaque h-nombre de la forme p_i divise n et réciproquement chaque h-premier p tel que $v_p \geq 1$ est un p_i (d'après le point 6). Il s'agit donc de prouver les égalités des exposants $\alpha_i = v_{p_i}$ pour chaque h-entier i compris entre 1 et k. Considérons un tel i : par maximalité de v_{p_i}, il est clair que $\alpha_{p_i} \leq v_{p_i}$; si l'on avait une ordination stricte, alors p_i diviserait $p_i^{v_{p_i} - a_i}$, donc diviserait $\frac{n}{p_i^{\alpha_i}}$, ce qu'interdit le point 6 avec la décomposition $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Remarque. Le dernier point permet de mettre en correspondance bi-univoque les h-entiers non nuls avec les h-suites d'entiers indexées par les h-nombres premiers chacune nulle à partir d'un certain rang :

1. envoyer un h-entier $n \geq 1$ sur la liste des valuations $v_p(n)$;
2. envoyer une h-suite (v_p) sur le produit des p^{v_p} pour p parcourant les h-nombres premiers.

Cette correspondance sera modélisée en mathématique par la bijection suivante (où $\mathbb{P}$ désigne l'ensemble des nombres premiers) :

$$\left\{ \begin{array}{ccc} \mathbb{N}^* & \xrightarrow{\sim} & \mathbb{N}^{(\mathbb{P})} \\ n & \longmapsto & (v_p(n)) \\ \prod_{p \in \mathbb{P}} p^{v_p} & \longleftarrow & (v_p) \end{array} \right. .$$

Elle montrera ainsi que les ensembles $\mathbb{N}$ et $\mathbb{N}^{(\mathbb{N})}$ sont équipotents, dégrossissant notre intuition de la finitude.