Dis Papa, c'est quoi l'arithmétique ?

Médiat

Décembre 2011

Introduction

- Dis Papa, c'est quoi l'arithmétique ?
- C'est un peu compliqué comme question, je t'expliquerai quand tu seras plus grand.
- Dis, Papa, comment on fait les bébés ?
- Bon, alors l'arithmétique c'est l'étude des nombres entiers naturels, tu sais les nombres que tu utilises tous les jours pour compter tes billes ou tes cartes Pokemon ; ce sont ces nombres dont on a l'impression qu'on peut les trouver « dans la nature », d'ailleurs un mathématicien célèbre, Kronecker, disait qu'ils étaient l'œuvre de Dieu (« Dieu fit les nombres naturels ; tout autre est l'œuvre de l'homme »), mais la méthode axiomatique a permis de définir les nombres entiers sans cette hypothèse.
- Mais il y en a beaucoup des nombres entiers, cela va être difficile de les définir tous.
- Aussi ne va-t-on pas chercher à en dresser la liste.
- Mais il y en a vraiment beaucoup beaucoup ?
- Oh oui !
- Plus qu'un milliard ?
- Beaucoup plus !
- Plus qu'un milliard de milliards
- Oui, mais arrête-toi, parce que justement la liste des entiers ne s'arrête pas, chaque entier a un suivant, c'est même une de leurs caractéristiques principales, une caractéristique que nous allons tenter de transformer en définition :

Pour construire les entiers naturels il suffit de se donner un nombre particulier (zéro, bien sûr), puis le suivant, puis le suivant du suivant, puis ... etc. sans s'arrêter.

- Papa, tu te moques là, tu m'avais habitué et appris à être plus rigoureux
- Tu as raison ! Je vais devoir être beaucoup plus rigoureux.

0) Pas encore de l'arithmétique.

Cette rigueur, dont nous avons absolument besoin, nous allons l'introduire en deux étapes :

1. En français, rapidement, mais avec un vocabulaire mathématique
2. En langage purement logique (classique du premier ordre avec égalité).

Définition en langage naturel :

1. On se donne un objet particulier que nous appellerons Marcel (en hommage à Bobby Lapointe)
2. On se donne aussi une application que nous appellerons AuSuivant (en hommage à Jacques Brel) qui à chaque entier fait correspondre un autre entier (et un seul puisque c'est une application) ; cette application est injective (deux nombres différents ne peuvent pas avoir le même AuSuivant), et presque surjective, puisque seul Marcel n'est le AuSuivant d'aucun entier.

Définition formelle :

1. Soit $\mathcal{L}$ le langage constitué d'un symbole de constante (que nous noterons 0 et appellerons « zéro »), et un symbole d'application (que nous noterons s et appellerons « successeur ») : $\mathcal{L} = (0, \mathrm{s})$

Soit la théorie PréA sur $\mathcal{L}$ qui vérifie les axiomes suivants :

$A_1 : \forall x \neg(s(x) = 0)$	Aucun entier n'a 0 pour successeur.
$A_2 : \forall x \exists y(x = 0 \vee x = s(y))$	Tous les entiers différent de 0 sont successeurs (s est une application presque surjective).
$A_3 : \forall x \forall y(s(x) = s(y) \Longleftrightarrow x = y)$	Deux entiers qui ont le même successeur sont égaux ; une autre façon de le dire : deux entiers différents ont des successeurs différents (s est un application injective).

Note : dans l'axiome A_3 peut être remplacé par $\forall x \forall y(s(x) = s(y) \Longrightarrow x = y)$, puisque l'autre sens est garanti par le fait que s est une application.

L'idée de définir les entiers uniquement à partir de la notion de successeur est assez tentante, puisqu'elle est très simple, qu'elle capture bien cette idée qu'après un entier il y a toujours un autre entier, et puis une petite voix, qui vient de l'arrière de la tête, nous souffle que, si cela marche, l'addition ne devrait pas être loin (additionner 1 c'est exactement prendre le successeur, pour additionner n, il suffit d'itérer n fois le successeur), et la multiplication se définit à partir de l'addition. Nous allons voir que tout cela est bien optimiste.

Définition : un modèle d'une théorie est "un monde possible" où l'on peut interpréter les éléments du langage (constantes, fonctions, relations), et tel que les éléments du modèle vérifient les axiomes de la théorie. On peut trouver facilement sur le net de très bons cours sur la théorie des modèles, ainsi qu'une petite introduction là : http ://forums.futura-sciences.com/showthread.php ?p=1395351

Remarque importante : Il n'est pas nécessaire d'avoir une définition formelle des entiers pour utiliser les entiers naïfs, ceux que l'ont apprend à manipuler en maternelle, par exemple il peut paraître abusif d'écrire (dans le cadre de la théorie PréA) $s^2(0)$, puisque 2 n'existe pas dans le langage et n'est pas défini dans PréA (pas plus que la notation exponentielle d'ailleurs), mais il suffit de savoir que $s^2(0)$ est une abréviation pratique pour $s(s(0))$ (abréviation très pratique (pour le scripteur comme pour le lecteur) si je veux parler de $s^{4565465454}(0)$ par exemple).

Il est évidemment formellement interdit d'utiliser les entiers naïfs dans une formule du langage formel sauf comme une abréviation, par exemple écrire :

- $\exists y(y = s^5(0))$ est valide car ce n'est qu'une abréviation pour $\exists y(y = s(s(s(s(s(0))))))$.
- $\exists y(y = s^n(0))$ est valide car ce n'est qu'une abréviation pour $\exists y(y = s(s(s(\ldots(s(0))\ldots)))$ où il y a n occurrences de s, évidemment cet exemple est un peu plus complexe que le précédent puisque n n'est pas fixé.
- $\forall n \, \exists y(y = s^n(0))$ est invalide puisque cette formule ne peut être considérée comme une abréviation d'une formule qui ne contient pas ce n (qui ne fait pas partie du langage utilisé ici).

Pour montrer que cette notion d'abréviation est valide même si n n'est pas fixé, il suffit de comprendre que les deux phrases suivantes (dans le langage adéquat et T une théorie dans ce langage) ne sont pas formellement identiques :

1. Pour tout n et pour tout m je peux démontrer, dans le cadre de la théorie T que : $n \times m = m \times n$.
2. Je peux démontrer dans le cadre de la théorie T que : $\forall n \, \forall m(n \times m = m \times n)$.

Dans le premier cas la démonstration envisagée est un fait un schéma de démonstrations qui permet d'écrire une démonstration pour chaque couple (m, n) d'entiers naïfs.

De la même façon, il sera souvent question du "modèle standard" de l'arithmétique (noté $\mathbb{N}$, bien sur), il y a plusieurs façons de comprendre cette expression, mais elles sont toutes équivalentes (et il suffit d'en comprendre une).

1. L'ensemble des entiers naturels est l'objet initial (unique à isomorphisme près) de la catégorie des diagrammes de Lawvere ($1 \longrightarrow X \longrightarrow^h X$).
2. Le monoïde libre a un générateur (ensemble des « mots » de longueur finie constitués à partir d'un alphabet ne contenant qu'une seule « lettre », auxquels on adjoint le « mot »vide) l'addition est simplement la concaténation des mots, pour la multiplication, on remplace chaque lettre du premier mot par le deuxième mot.

3. L'ensemble des « mots » de longueur finie sur l'alphabet 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 ne commençant pas par 0, plus le mot 0, pour définir l'addition et la multiplication ... il suffit de retourner en cours préparatoire.
4. Dans le cadre de la théorie des ensembles (ZF supposé consistante) ω (le plus petit ordinal limite), avec les opérations habituelles.
5. Si on sait compter (ou écrire en lettres) jusqu'à 999 alors on sait le faire de 1000 jusqu'à 999 999, il suffit d'intercaler le mot « mille » entre les deux groupes, pour les millions et les milliards, c'est le même principe, au delà de 999 999 999 on coupe en paquets de 9 chiffres et on ajoute « milliards » ou « milliards de » entre chaque groupes autant de fois qu'il y a de groupes à droite (cette définition ne respecte pas toutes les règles de la grammaire française, et elle n'est certainement pas facile à manipuler, mais c'est le point de départ de la question de mon fils qui a déclenché chez moi l'envie d'écrire ce petit document).
6. Le segment initial infini commun (à isomorphisme près) à tous les modèles de l'arithmétique de Peano supposé consistante (mais là on se mord la queue, d'ailleurs ce point sera démontré dans le chapitre sur l'arithmétique de Peano).

Tout d'abord nous allons tenter de décrire les modèles possibles de la théorie PréA, et pour se faire nous allons nous pencher sur les « composantes connexes » (au sens de la fonction successeur, bien sûr) de ces modèles.

Définition : Une composante connexe pour la fonction successeur est un sous ensemble d'un modèle qui est clos pour la fonction successeur et telle que pour tout couple d'éléments de la même composante connexe x et y, il existe un entier (naïf) tel que $x = s^n(y)$ ou $y = s^n(x)$ ($s^n(x)$ est une abréviation pour $s(s(s...(x)...)$ avec s appliqué n fois).

Par un simple argument de tiers exclu, il ne peut y avoir que quatre types de composantes connexes possibles :
CC1) Contient le 0 et est infini
CC2) Contient le 0 et est fini (cas, en fait, impossible)
CC3) Ne contient pas le 0 et est infini
CC4) Ne contient pas le 0 et est fini

Exercice 1 (PréA)**.** *Montrer que le cas CC2 est vraiment impossible.*

Exercice 2 (PréA)**.** *Montrer qu'un modèle contient une et une seule composante connexe de type CC1.*

On déduit immédiatement du résultat précédent que la théorie PréA n'a pas de modèle fini.

La structure suivante va nous permettre de construire des modèles de la théorie PréA.
$\mathbb{Z}/p\mathbb{Z}$ représente le groupe additif des classes résiduelles modulo p (qui, donc, contient exactement p éléments).

$$\mathbb{M} = \mathbb{N} \biguplus \alpha \times \mathbb{Z} \biguplus \beta_p \times \mathbb{Z}/p\mathbb{Z}$$

J'utilise le symbole $\biguplus$ pour l'union disjointe, et $\times$ pour le produit cartésien
α et les β_p sont de cardinal quelconque ($\leq \aleph_0$ pour les modèles dénombrables) et p parcourt les entiers strictement positifs.
Par la suite $\mathbb{Z}_i$ sera la i-ième composante égale à $\mathbb{Z}$ et $\mathbb{Z}_i/p\mathbb{Z}_i$ sera la i-ième composante égale à $\mathbb{Z}/p\mathbb{Z}$
Remarque : Les unions étant disjointes, il faut noter que les "0" que l'on trouve dans chacune des copies de

$\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ sont tous distincts et que le seul "0" qui sera intéressant est celui qui va interpréter le 0 du langage.

On définit 0 et s dans la structure $\mathbb{M}$ de la façon suivante :
$0_{\mathbb{M}} = 0_{\mathbb{N}}$

$s_{\mathbb{M}}$ est défini de la façon suivante :
si $x \in \mathbb{N}$ alors $s_{\mathbb{M}}(x) \in \mathbb{N} \wedge s_{\mathbb{M}}(x) = x + 1$

si $x \in \mathbb{Z}_i$ alors $s_{\mathbb{M}}(x) \in \mathbb{Z}_i \wedge s_{\mathbb{M}}(x) = x + 1$

si $x \in \mathbb{Z}_i/p\mathbb{Z}_i$ alors $s_{\mathbb{M}}(x) \in \mathbb{Z}_i/p\mathbb{Z}_i \wedge s_{\mathbb{M}}(x) = x \oplus 1$ (où $\oplus$ est l'addition dans $\mathbb{Z}/p\mathbb{Z}$ c'est-à-dire $s_{\mathbb{M}}(x) < p \wedge s_{\mathbb{M}}(x) \equiv x + 1[p]$)

On peut désormais noter $\mathfrak{M} = (\mathbb{M}, 0_{\mathbb{M}}, s_{\mathbb{M}})$

Exercice 3 (PréA)**.** *Montrer que les modèles de la forme $\mathfrak{M}$ sont des modèles de PréA*

Exercice 4 (PréA)**.** *Pourquoi n'est-ce pas gênant d'utiliser $\mathbb{N}$ ici (ainsi que $\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$) alors que le but est justement de trouver une axiomatisation de $\mathbb{N}$?*

Nous allons montrer que tous les modèles de PréA sont de la forme $\mathfrak{M}$ décrite ci-dessus.

Soit cc1 **la** composante connexe de type CC1 et f la fonction $\mathbb{N} \longrightarrow cc1$ définie par :
$f(0_{\mathbb{N}}) = 0_{\mathbb{M}}$ (qui existe bien dans cc1)
$f(x + 1) = s_{\mathbb{M}}(f(x))$.
Dans la suite nous omettrons les indices lorsqu'aucune confusion n'est possible.
Remarque : Soit $x \in cc1$, c'est-à-dire que x est dans la composante connexe contenant 0, c'est-à-dire qu'il existe n tel que $x = s^n(0)$ (rappelons que $s^n(0)$ est une abréviation pour $s(s(s...(0)...))$ avec s appliqué n fois).
Nous allons montrer que f est injective :
$f(x) = f(y) \Longleftrightarrow s^n(0) = s^m(0)$ si n = m alors x = y (puisque s est une application) et la démonstration est terminée ; sans perte de généralité on peut supposer que $n < m$, en appliquant $m - n$ fois l'axiome A_3 on obtient : $f(x) = f(y) \Longleftrightarrow 0 = s^{m-n}(0)$ ce qui est impossible d'après l'axiome A_1.

Exercice 5 (PréA)**.** *Montrer que f est une application surjective donc bijective*

On déduit de l'exercice précédent que f est un isomorphisme, c'est-à-dire que dans tous les modèles de PréA, la composante connexe contenant 0 est isomorphe à $\mathbb{N}$.

Soit cc3 une composante connexe non vide de type CC3 et f la fonction $\mathbb{Z} \longrightarrow cc3$ définie par :
$f(0_{\mathbb{Z}}) = a$ (un élément quelconque de cc3, qui n'est pas vide)
$f(x + 1) = s_{\mathbb{M}}(f(x))$.
Nous savons que pour tout x dans $\mathbb{Z}$ il existe y tel que $s_{\mathbb{M}}(y) = f(x)$ (axiome A_2), on pose :
$f(x - 1) = y$.

Exercice 6 (PréA)**.** *Montrer que f est un isomorphisme (même chose que pour cc1 a peu de chose près)*

Soit cc4 une composante connexe de cardinal $p > 0$ de type CC4 et f la fonction $\mathbb{Z}/p\mathbb{Z} \longrightarrow cc4$ définie par :
$f(0_{\mathbb{Z}/p\mathbb{Z}}) = a$ (un élément quelconque de cc4, qui n'est pas vide)
$f(x + 1) = s_{\mathbb{M}}(f(x))$.

Exercice 7 (PréA)**.** *Montrer que f est un isomorphisme, la subtilité ici ne réside pas dans la démonstration que f est bijective, mais que f est une application.*

Ce qui termine la preuve que les modèles de la forme $\mathfrak{M}$ sont les seuls modèles de la théorie PréA.
Ce résultat est assez décevant car nous obtenons des modèles très différents de ce que l'on attendait.
Mais une petite lueur d'espoir pointe son nez mutin : la théorie PréA n'est pas complète, comme nous allons le voir, il va donc être possible d'ajouter un ou des axiomes afin d'améliorer les choses.

Théorème 1 (PréA)**.** *La formule $\exists x(s(x) = x)$ est indécidable dans PréA*

Démonstration :
La formule $\exists x(s(x) = x)$ est valide dans le modèle $\mathbb{N} \biguplus \mathbb{Z}/1\mathbb{Z}$ (l'élément de $\mathbb{Z}/1\mathbb{Z}$ vérifie cette formule), alors que le modèle $\mathbb{N}$ ne la vérifie pas (puisqu'elle est équivalente à x + 1 = x)
La théorie PréA contenant une formule indécidable, n'est donc pas complète.

Quel(s) axiome(s) ajouter ? On pourrait envisager de rajouter la négation de la formule précédente, mais ce serait clairement insuffisant, puisqu'il faudrait ajouter la négation de $\exists x(s(s(x)) = x)$, et en fait tous les axiomes de la forme $\neg(\exists x(s^n(x) = x))$ (qui peuvent aussi s'écrire $\forall x \neg(s^n(x) = x)$; il faudrait donc ajouter un

schéma d'axiomes (cf. infra l'exemple d'extension No 1) ; tant qu'à ajouter un tel schéma, messieurs Dedekind et Peano (et avant eux Grassmann) ont pensé à un schéma légèrement plus compliqué et plus puissant :

(cf. en fin de chapitre pour d'autres extensions)

Pour chacune des formules $\Phi(x)$ de $\mathcal{L}$ à une variable libre on ajoute l'axiome :

$A_\Phi : (\Phi(0) \wedge \forall x(\Phi(x) \Longrightarrow \Phi(s(x))) \Longrightarrow \forall x \Phi(x)$.

On reconnaît le schéma d'induction ou de récurrence. Comme nous nous plaçons dans la logique du premier ordre qui n'autorise pas la quantification des formules, il s'agit bien ici d'un schéma d'axiomes (que l'on peut instancier pour chaque formule bien formée du langage) et non d'un axiome ; ce que l'on peut noter cependant, c'est que le processus qui permet de créer une formule bien formée du langage (dénombrable) est récursif (ce qui peut se traduire par : il existe un programme d'ordinateur qui peut, sans boucle infinie, décider si une chaîne de caractères est une formule bien formée ou non).

Nous baptiserons cette nouvelle théorie PréA' ; d'abord vérifions que nous avons bien avancé dans la direction choisie.

Soit $\psi_p(x)$ la formule $\neg(s^p(x) = x)$ (pour $p > 0$)

Exercice 8 (PréA). *Montrer que $\forall x\, \psi_p(x)$ n'est pas valide dans un modèle de PréA contenant $\mathbb{Z}/p\mathbb{Z}$*

Théorème 2 (PréA'). *PréA' $\vdash \neg(s^p(0) = 0)$*

Démonstration :
Trivial, c'est l'axiome A_1

Théorème 3 (PréA'). *PréA $\vdash \forall x(\neg(s^p(x) = x) \Longrightarrow \neg(s^p(s(x)) = s(x))$ (Attention, il s'agit bien de PréA et non de PréA', car le schéma d'induction n'est pas utile pour ce point, mais le résultat est a fortiori vrai pour PréA')*

Démonstration :
$(s^p(s(x)) = s(x)) \Longleftrightarrow (s(s^p(x)) = s(x))$ (parce que s est une application)
$(s(s^p(x)) = s(x)) \Longleftrightarrow (s^p(x) = x)$ (grâce à l'axiome A_3), cqfd

Théorème 4 (PréA'). *PréA' $\vdash \forall x \psi_p(x)$*

Démonstration :
Le théorème 2 + le théorème 3 + l'axiome A_{ψ_p}

On en déduit que les modèles de PréA' sont de la forme $\mathfrak{M} = (\mathbb{M}, 0_\mathbb{M}, s_\mathbb{M})$, où $\mathbb{M} = \mathbb{N} \biguplus \alpha \times \mathbb{Z}$, où α est de cardinal quelconque.

Peut-on aller plus loin, c'est-à-dire trouver une théorie PréA* ayant les mêmes modèles, sans les copies de $\mathbb{Z}$?

La réponse est malheureusement non ! En effet cette théorie n'aurait qu'un seul modèle (à isomorphisme près) infini (ici dénombrable), ce qui est contradictoire avec le théorème de Löwenheim-Skolem.

Définition : Une théorie T est dîte κ-catégorique si elle ne possède qu'un seul modèle de cardinal κ à isomorphisme près.

Théorème 5 (PréA'). *La théorie PréA' est $\aleph_1$-catégorique*

Démonstration :
La structure sous-jacente à un modèle de PréA' est de la forme $\mathbb{N} \biguplus \alpha.\mathbb{Z}$, pour que cette structure soit de cardinal $\aleph_1$, il faut que α soit de cardinal $\aleph_1$; en effet le cardinal de $\mathbb{M}$ est $\aleph_0 + |\alpha|.\aleph_0 = \aleph_1$ ce qui implique $|\alpha| = \aleph_1$ (l'unicité à isomorphisme près s'en déduit facilement)

Rappel de logique classique du premier ordre :

Théorème 6 (de Los-Vaught). *Une théorie n'ayant que des modèles infinis et catégorique pour un cardinal est complète.*

Théorème 7 (PréA'). *PréA' est complète.*

Démonstration :
Conséquence immédiate du théorème 5 et du théorème de Los-Vaught.

Résumé de ce qui précède : Nous avons trouvé une théorie complète modélisant bien la notion de successeur, incluant le schéma d'induction, mais n'ayant pas $\mathbb{N}$ comme seul modèle dénombrable (néanmoins, tous les modèles vérifient les mêmes formules).

Constatation très importante : la notion d'équivalence élémentaire (deux modèles sont élémentairement équivalents s'ils vérifient les mêmes formules) ne recouvre donc pas la notion d'isomorphisme (mais isomorphisme $\Longrightarrow$ équivalence élémentaire)

Les choses semblent bouchées puisqu'à l'évidence, on ne peut pas compléter une théorie complète (qui est une notion liée au langage utilisé), heureusement, on peut enrichir le langage ...

Remarque douloureuse : on peut penser que dans toute théorie candidate au nom d'arithmétique on doit pouvoir trouver l'addition et le 0, et par conséquent on doit pouvoir définir, la relation $<$:

$\forall x \forall y (x < y \Longleftrightarrow (\exists z (z \neq 0 \wedge x + z = y))$

Or si T est une théorie acceptable pour l'arithmétique (donc ayant $\mathbb{N}$ pour modèle), la théorie T' définie par $T' = T \bigcup_{n \in \mathbb{N}} \exists x (x > n)$ est consistante par compacité, donc elle admet au moins un modèle qui contient un élément plus grand que tous les entiers, donc qui n'est pas isomorphe à $\mathbb{N}$; on peut en conclure :

Théorème 8 (Arithmétique)**.** *Aucune théorie arithmétique du premier ordre ne peut être $\aleph_0$-catégorique.*

Rapide description de deux extensions possibles de PréA :

Exemple 1) Soit la théorie PréA" définie sur le même langage que PréA, avec les mêmes axiomes, plus le schéma suivant (pour tout entiers plus grand que 1) :

$S_n : \forall x \neg (s^n(x) = x)$

Dont les modèles sont $\mathfrak{M} = (\mathbb{M}, 0_{\mathbb{M}}, s_{\mathbb{M}})$, où $\mathbb{M} = \mathbb{N} \biguplus \alpha \times \mathbb{Z}$, où α est de cardinal quelconque.

Théorème 9 (PréA")**.** *PréA" est complète (par élimination des quantificateurs, technique que nous verrons en détail dans le chapitre suivant).*

Remarque : PréA" est une théorie complète ayant beaucoup de modèles dénombrables non isomorphes (PréA" n'est pas $\aleph_0$-catégorique), elle possède $\aleph_0$ modèles non-isomorphes (ce qui est loin du maximum).

Exercice 9 (PréA")**.** *Montrer que PréA" a bien $\aleph_0$ modèles non isomorphes, en les exhibant*

Exemple 2) Soit la théorie PréA"' définie sur le langage $\mathcal{L} = (0, s, <)$ avec les axiomes suivant :

$O_1 : \forall x (\neg (x = 0) \Longrightarrow \exists y (x = s(y)))$

$O_2 : \forall x \forall y ((x < s(y)) \Longleftrightarrow ((x < y) \vee (x = y)))$

$O_3 : \forall x \neg (x < 0)$

$O_4 : \forall x \forall y ((x < y) \Longrightarrow \neg (y < x))$

$O_5 : \forall x \forall y \forall z (((x < y) \wedge (y < z)) \Longrightarrow (x < z))$

$O_6 : \forall x \forall y ((x < y) \vee (x = y) \vee (y < x))$

Les axiomes O_4 à O_6 sont ceux d'un ordre total strict.

Exercice 10 (PréA"')**.** *Montrer que les axiomes de PréA sont des théorèmes de PréA"'.*

Théorème 10 (PréA"')**.** *PréA"' est complète (par élimination des quantificateurs).*

Nous verrons plus loin un exemple de démonstration de l'élimination des quantificateurs

1) Arithmétique de Presburger

L'arithmétique de Presburger est une théorie du premier ordre dont le langage est $\mathcal{L} = (0, s, +)$
Ses axiomes sont ceux de PréA, plus le schéma d'induction et plus deux axiomes pour $+$.

Exercice 11 (Presburger)**.** *Pourquoi n'ai-je pas simplement écrit « Les axiomes sont ceux de PréA' plus deux axiomes pour + » ?*

Nous ajoutons deux axiomes pour $+$:
$A_4 : \forall x\,(x + 0 = x)$
$A_5 : \forall x \forall y\,((x + s(y) = s(x + y))$

Remarque : la consistance de l'arithmétique de Presburger a été démontrée par Hilbert et Bernays (1934)

Nous venons d'ajouter un symbole à notre langage et comme nous allons en ajouter d'autres, je voudrais, tout de suite, faire une distinction importante :
1) On peut ajouter un nouveau symbole définissable à partir du langage de base, dans ce cas la théorie est la même (possède les mêmes modèles), mais quelques résultats syntaxiques peuvent être différents, l'élimination des quantificateurs par exemple (ce n'est pas étonnant puisque les formules atomiques sont différentes).
2) On peut ajouter un nouveau symbole qui n'est pas définissable à partir du langage de base, mais doit (sinon le nouveau symbole ne sert pas à grand-chose) vérifier quelques axiomes. Dans ce cas la théorie est différente de l'ancienne.

Par la suite nous parlerons de symbole de type 1 ou de type 2. Exemple 1 : Au langage $\mathcal{L} = (0, s)$, on ajoute

le symbole k pour créer un nouveau langage $\mathcal{L}' = (0, s, k), k$ est défini par $k(x) = \exists y(s(s(s(y))) = x)$, une formule sur le langage $\mathcal{L}'$ peut se transformer facilement en une formule sur le langage $\mathcal{L}$ en remplaçant toutes les occurrences de k(x) par sa définition. Par contre une formule sans quantificateur sur $\mathcal{L}'$ peut contenir des quantificateurs sur $\mathcal{L}$.

Exemple 2 : cf. la théorie $T(0, s, <)$ ou encore le $+$ ajouté ci-dessus

Nous allons donc ajouter deux nouveaux symboles de type 1 (donc sans changer la théorie) à notre théorie (notée Presburger) : $\leq$ et $<$ définis de la façon suivante :
$x \leq y \Longleftrightarrow \exists z(x + z = y)$
$x < y \Longleftrightarrow (x \leq y \wedge \neg(x = y))$

Théorème 11 (Presburger)**.** *Les formules suivantes sont démontrables dans l'arithmétique de Presburger.*
T_1 : $Presburger \vdash \forall x(0 + x = x)$
T_2 : $Presburger \vdash \forall x \forall y(s(x) + y = s(x + y))$
T_3 : $Presburger \vdash \forall x \forall y(x + y = y + x)$
T_4 : $Presburger \vdash \forall x \forall y(x \leq y \vee y \leq x)$
T_5 : $Presburger \vdash \forall x \forall y(x + y = 0 \Longleftrightarrow ((x = 0) \wedge (y = 0))$
T_6 : $Presburger \vdash \forall x \forall y \forall z((x + y) + z = x + (y + z))$
T_7 : $Presburger \vdash \forall x \forall y \forall z((x + y = x + z) \Longleftrightarrow (y = z))$
T_8 : $Presburger \vdash \forall x \forall y((x \leq y \wedge y \leq x) \Longleftrightarrow (x = y))$
T_9 : $Presburger \vdash \forall x \forall y((x < y \vee y < x) \Longleftrightarrow \neg(x = y))$
T_{10} : $Presburger \vdash \forall x \forall y \forall z(x \leq y \Longleftrightarrow ((x + z) \leq (y + z)))$
T_{11} : $Presburger \vdash \forall x \forall y(\neg(x < y) \Longleftrightarrow (y \leq x))$
T_{12} : $Presburger \vdash \forall x(0 \leq x)$
T_{13} : $Presburger \vdash \forall x(x < s(x))$
T_{14} : $Presburger \vdash \forall x(s^n(0) + x = s^n(x))$ *(pour tout n)*
T_{15} : $Presburger \vdash \forall x \forall y((x \leq y \wedge y \leq s(x)) \Longrightarrow (y = x \vee y = s(x)))$

Exercice 12 (Presburger)**.** *Démontrer les théorèmes précédents (c'est sans doute un peu fastidieux de les démontrer tous, mais c'est assez formateur de se contraindre à en démontrer quelques-uns).*

Remarques : 1) A_4 et T_1 expriment que 0 est un élément neutre pour +, T_6 exprime que + est associative, T_3 exprime que + est commutative et T_7 exprime que + est régulière. Les modèles de l'arithmétique de Presburger sont donc des monoïdes commutatifs et réguliers.
2) T_8, T_4 et T_{16} expriment que les modèles de l'arithmétique de Presburger sont des ordres totaux et T_{15} exprime que ces ordres sont discrets.
3) T_{10} exprime que dans les modèles de l'arithmétique de Presburger, l'addition est croissante (dans un certain sens).

Nous allons enfin ajouter $\aleph_0$ nouveaux symboles (de type 1, donc toujours sans changer la théorie, et sans besoin qu'il soit nécessaire d'ajouter des axiomes) qui vont être fondamentaux pour la suite.

Nous travaillerons avec le langage $\mathcal{L} = (0, s, +, \equiv_n)$ où $\equiv_n$ est définit par : $a \equiv_n b \iff \exists x(nx + a = b)$
où nx est une abréviation pour x + x + ... + x (n fois).
Attention $\equiv_n$ n'est pas la relation de congruence habituelle (nous l'appellerons congruence néanmoins).

Exercice 13 (Presburger)**.** *Il est clair que la notation nx utilisée ci-dessus permet de définir la multiplication par n, pour tout n, mais pourquoi n'est-ce pas la définition de la multiplication ?.*

Exercice 14 (Presburger)**.** *Montrer que $\equiv_n$ permet de définir $\leq$.*

Théorème 12 (Presburger)**.** *L'arithmétique de Presburger admet l'élimination des quantificateurs sur le langage $\mathcal{L} = (0, s, +, \equiv_n)$*

Avant de donner la preuve du théorème précédent (plutôt qu'une démonstration complète, nous donnerons un aperçu de la démonstration de Presburger, en utilisant les mêmes noms de variables, mais sans utiliser ses notations pour les connecteurs et les quantificateurs qui sont illisibles aujourd'hui), nous allons donner quelques définitions utiles :

L'ensemble des *termes* d'un langage $\mathcal{L}$ est défini inductivement de la façon suivante :
Les variables de $\mathcal{L}$ sont des *termes*.
Les constantes de $\mathcal{L}$ sont des *termes*.
Si $t_1, t_2, ...t_n$ sont des *termes*, et, si $\mathcal{F}$ est une fonction n-aire (d'arité n, c'est à dire avec n variables), alors $\mathcal{F}(t_1, t_2, ...t_n)$ est un *terme*.

L'ensemble des *formules atomiques* d'un langage $\mathcal{L}$ est défini inductivement de la façon suivante :
Si t_1 et t_2 sont des termes, alors $t_1 = t_2$ est une *formule atomique* (puisque que nous ne considérons que des langage égalitaires).
Si $t_1, t_2, ...t_n$ sont des termes, et, si $\mathcal{R}$ est une relation n-aire (d'arité n), alors $\mathcal{R}(t_1, t_2, ...t_n)$ est une *formule atomique*.

Définition : Une théorie $\mathcal{T}$ admet l'élimination des quantificateurs si toute formule est équivalente à une formule sans quantificateur.

Théorème 13 (Logique classique)**.** *Une théorie T admet l'élimination des quantificateurs si pour toutes les formules de la forme $\exists x \phi_1 \wedge \phi_2 \wedge ... \wedge \phi_n$ où les ϕ_i sont des formules atomiques ou des négations de formules atomiques, il existe une formule équivalente : $\phi'_1 \wedge \phi'_2 \wedge ... \wedge \phi'_n$ où les ϕ'_i sont des formules atomiques ou des négations de formules atomiques sans nouvelle variable libre.*

Théorème 14 (Logique classique)**.** *Une théorie T qui admet l'élimination des quantificateurs associé à un procédé constructif de la formule sans quantificateur (comme ici) est décidable.*

Théorème 15 (Logique classique)**.** *Une théorie T décidable et consistante est complète.*

La démonstration se fait par récurrence sur la complexité de la formule.

Enfin voyons un petit lemme qui sera utile dans les calculs par la suite :
Lemme : pour $\beta \neq 0$: $a \equiv_\alpha b \iff \beta a \equiv_{\beta\alpha} \beta b$

Démonstration du théorème 12 :

Il nous faut construire les formules atomiques de $\mathcal{L}$; avec seulement deux symboles de relation (deux au sens du méta-langage, car dans le nouveau langage étendu il y en a autant que d'entiers naïfs), la tâche n'est pas trop compliquée :

$u = v$

$u \equiv_n v$

$\neg(u = v)$

$\neg(u \equiv_n v)$

où u et v sont des termes.

Une première remarque va simplifier le travail :

$\neg(a \equiv_n b) \iff (a + 1 \equiv_n b) \vee (a + 2 \equiv_n b) \vee ... \vee (a + n - 1 \equiv_n b) \vee ((b \equiv_1 a) \wedge a \neq b)$

Il ne reste donc plus que trois types de formules atomiques à étudier.

Il nous faut aussi construire les termes : en remplaçant $s^n(0)$ par n, et $s^n(x)$ par $x + n$, x + x + x + ... x + x (n fois) par nx, et en appliquant diverses propriétés de +, on peut toujours se ramener à :

$\alpha x + a = b$ pour les équations, et donc

$\neg(\alpha x + a = b)$ pour les négations d'équations

$\alpha x + a \equiv_\beta b$ pour les congruences

Il existe donc six formes de conjonctions de deux formules atomiques (l'étude de 2 conjonctions est suffisante).

Voyons en détail un cas intéressant : « Une équation et une congruence » (ci-dessous les lettres grecques représentent des entiers « naïfs »). : $\exists x((\alpha x + a = b) \wedge (\beta x + c \equiv_\gamma d))$

Nous devons montrer que la formule $\exists x((\alpha x + a = b) \wedge (\beta x + c \equiv_\gamma d))$ est équivalente à une formule sans quantificateur.

Posons $\delta = PPCM(\alpha, \beta)$, $a' = a * \delta/\alpha$, $b' = b * \delta/\alpha$, $\gamma' = \gamma * \delta/\beta$, $c' = c * \delta/\beta$, $d' = d * \delta/\beta$

$$\begin{aligned}
&\exists x((\alpha x + a = b) \wedge (\beta x + c \equiv_\gamma d)) \\
&\qquad\iff \\
&\exists x((\delta x + a' = b') \wedge (\delta x + c' \equiv_{\gamma'} d')) \\
&\qquad\iff \\
&\exists x((\delta x + a' = b') \wedge (\delta x + c' + a' \equiv_{\gamma'} d' + a')) \\
&\qquad\iff \\
&\exists x((\delta x + a' = b') \wedge (b' + c' \equiv_{\gamma'} d' + a')) \\
&\qquad\iff \\
&(a' \equiv_\delta b') \wedge (b' + c' \equiv_{\gamma'} d' + a'))
\end{aligned}$$

Cette dernière formule ne contient pas de quantificateur.

Remarque : Cette démonstration utilise lourdement le théorème 11.

Pour les six cas de conjonctions de deux formules atomiques le principe de la démonstration est à peu près le même, on en déduit le théorème suivant.

Théorème 16 (Presburger)**.** *L'arithmétique de Presburger est complète.*

2) Arithmétique de Robinson

Cette arithmétique est aussi appelé « système Q » dans la littérature. Le langage est celui déjà vu plus la multiplication (qui sera notée $\cdot$ pour éviter les confusions avec la ponctuation) : $\mathcal{L} = (0, S, +, \cdot)$, et les axiomes sont

A_1, A_2, A_3 pour s
A_4, A_5 pour $+$
$A_6 : \forall x(x \cdot 0 = 0)$
$A_7 : \forall x \forall y(x \cdot s(y)) = x \cdot y + x$ pour $\cdot$

On remarquera que la seule différence avec l'arithmétique de Peano (cf. infra) est l'absence du schéma d'induction.

Ce qui est important concernant l'arithmétique de Robinson est que cette théorie (finiment axiomatisable) est non seulement non complète, mais qu'elle est incomplétable au sens de Gödel (on dit aussi essentiellement incomplète, cf. infra pour la démonstration dans le cas de l'arithmétique de Peano), ce qui veut dire que le schéma d'induction n'est pas le responsable du théorème d'incomplétude.

Remarque : aucune sous-théorie de l'arithmétique de Robinson (en supprimant un axiome par exemple) n'est incomplétable au sens de Gödel.

De façon plus anecdotique, l'arithmétique de Robinson est assez « pauvre », par exemple on peut y démontrer que $1 + 2 = 2 + 1$ (ou que $123254654 + 987546542 = 987546542 + 123254654$, mais la démonstration est un peu plus longue), mais on ne peut pas y démontrer que $\forall x \forall y(x + y = y + x)$, comme nous allons le voir.

Construction d'un modèle de l'arithmétique de Robinson :

Soit la structure $\mathbb{M} = (\{0\} \times \mathbb{N}) \bigcup (\mathbb{Q}^{*+} \times \mathbb{Z})$, on définit sur $\mathbb{M}$ une $\mathcal{L}$-structure (c'est-à-dire qu'il faut interpréter 0, s, + et $\cdot$ dans cette structure) :

$0_{\mathcal{L}}$ est interprété par $(0, 0)$
$s_{\mathcal{L}}$ est interprété par $s_{\mathbb{M}}(\alpha, n) = (\alpha, n + 1)$
$+_{\mathcal{L}}$ est interprété par $(\alpha, n) +_{\mathbb{M}} (\beta, m) = (\alpha, n + m)$
$\cdot_{\mathcal{L}}$ est interprété par $(\alpha, n) \cdot_{\mathbb{M}} (\beta, m) = (\alpha + \beta, n.m)$ si $(\beta, m) \neq (0, 0)$ et
$(\alpha, n) \cdot_{\mathbb{M}} (0, 0) = (0, 0)$

A partir d'ici, je ferais l'économie des indice $\mathbb{M}$ puisqu'il y a peu de risque de confusion (et pour être parfaitement rigoureux, voire maniaque, j'aurais dû mettre cet indice au signe $=$, et même le définir).

Exercice 15 (Robinson)**.** *Montrer que $\mathfrak{M} = (\mathbb{M}, 0, s, +, \cdot)$ est un modèle de l'arithmétique de Robinson*

Exercice 16 (Robinson)**.** *Montrer que la commutativité de l'addition est indécidable dans l'arithmétique de Robinson*

Remarque : un exemple plus simple : $(\mathbb{N} \bigcup \{\omega\}, +, \cdot)$ en définissant les opérations faisant intervenir ω, comme si celui-ci était l'∞.

Dans le tableau suivant n représente un entier.

x	n	ω
s(x)	n + 1	ω

Dans le tableau suivant n et m représentent des entiers.

+	n	ω
m	n + m	ω
ω	ω	ω

Dans le tableau suivant n et m représentent des entiers non nuls.

$\cdot$	0	n	ω
0	0	0	0
m	0	n $\cdot$ m	ω
ω	0	ω	ω

Théorème 17 (Robinson)**.** *Robinson est Σ_1-complète (c'est-à-dire : permet de démontrer les Σ_1 formules vraies dans tous les modèles)*

Δ_0 est l'ensemble des formules ne contenant que des quantificateurs bornés.

$\overline{x}$ est une abréviation pratique pour représenter un nombre fini quelconque de variables.

Σ_1 est l'ensemble des formules $\Delta_0 \bigcup \{\psi \mid \psi(\overline{y}) = \exists \overline{x} \phi(\overline{x}, \overline{y}) \wedge \phi \in \Delta_0\}$, c'est-à-dire les formules contenant au plus une série de quantificateurs existentiels non bornés.

Π_1 est l'ensemble des formules $\Delta_0 \bigcup \{\psi \mid \psi(\overline{y}) = \forall \overline{x} \phi(\overline{x}, \overline{y}) \wedge \phi \in \Delta_0\}$, c'est-à-dire les formules contenant au plus une série de quantificateurs universels non bornés.

Remarque : Σ_n et Π_n se définissent par récurrence de façon naturelle en alternant les séries de quantificateurs, le premier (à gauche) étant $\exists$ pour Σ_n, et $\forall$ pour Π_n.

Justification informelle :

Si une formule de la forme $\exists x \phi(x)$ (où ϕ est une formule sans quantificateurs) est vraie dans $\mathbb{N}$, alors elle doit être vraie pour un certain $n \in \mathbb{N}$, donc Robinson doit démontrer $\phi(n)$ qui est une formule sans quantificateur (c'est ce point qui nécessiterait une démonstration détaillée) et donc, a fortiori, Robinson doit démontrer $\exists x \phi(x)$.

Note : dans la pseudo-démonstration ci-dessus on peut remplacer x par $\overline{x}$.

On peut aussi rappeler que $\mathbb{N}$ est un segment initial de tous les modèles de l'arithmétique de Robinson (et de Peano, entre autres).

Corollaire 1 (Robinson)**.** *Si T est une théorie consistante qui contient l'arithmétique de Robinson, et soit $\phi \in \Pi_1$:*

i) si $T \vdash \phi$ alors $\mathbb{N} \models \phi$

ii) si ϕ est indécidable dans T alors $\mathbb{N} \models \phi$.

Le point i) est trivial, le point ii) n'est pas beaucoup plus compliqué (raisonnement par l'absurde, la négation d'une formule Π_1 étant une formule Σ_1).

Le point ii) du théorème précédent est souvent énoncé d'une façon que je trouve totalement insupportable (même s'il ne s'agit que d'une question de vocabulaire), sur le mode « journaliste en quête de sensationnel » :

Si la formule ϕ est indécidable alors elle est vraie, par exemple : si la conjecture de Goldbach (qui est bien Σ_1) est indécidable, alors elle est vraie.

Raison de mon ire : dans la phrase précédente, on attribue à la formule ϕ une caractéristique qui n'a de sens que pour une théorie (être indécidable) et une caractéristique qui n'a de sens que dans un modèle bien particulier (être vraie).

Et pourquoi pas l'exponentiation ?

Après avoir étudié successivement des arithmétiques sur les langages : $\mathcal{L} = (0, s), \mathcal{L} = (0, s, +)$ et $\mathcal{L} = (0, s, +, \cdot)$

On est en droit de se demander s'il ne serait pas possible d'aller plus loin en ajoutant une opération qui soit à la multiplication ce que la multiplication est à l'addition, autrement dit l'exponentiation.

Mais, en fait, ceci est inutile ; en effet, l'exponentiation se définit à partir de l'addition et de la multiplication, grâce à la fonction β de Gödel : $\beta(x, y, z) = x \mod (1 + (z + 1) \cdot y)$

Exercice 17. *Démontrer que la fonction de Gödel est définissable au premier ordre (avec $+$ et $\cdot$)*

Théorème 18 (Robinson)**.** *L'exponentiation est définissable dans l'arithmétique de Robinson.*

Démonstration :
Soit $\exp(x, y, z)$ le prédicat dont la sémantique est $z = x^y$ et défini par :

$\exp(x, y, z) \iff \exists u \exists v(\beta(u, v, 0) = 1 \wedge \forall w(w < y \implies \beta(u, v, w + 1) = x \cdot \beta(u, v, w)) \wedge z = \beta(u, v, y))$

L'idée de cette définition est de faire coder la suite finie $(1, x, x^2, ...x^y)$, par la fonction β (cf. infra la justification de cette idée, qui se trouve ainsi démontrée).

3) Arithmétique de Peano

Le langage de l'arithmétique de Peano est celui de l'arithmétique de Robinson, ses axiomes sont aussi ceux de l'arithmétique de Robinson plus le schéma d'induction pour toutes les formules du langage $\mathcal{L} = (0, s, +, \cdot)$ avec une variable libre

Pour rappel :
$A_1 : \forall x \neg(s(x) = 0)$
$A_2 : \forall x \exists y(x = 0 \vee x = s(y))$
$A_3 : \forall x \forall y(s(x) = s(y) \iff x = y)$
$A_4 : \forall x\, (x + 0 = x)$
$A_5 : \forall x \forall y\, ((x + s(y) = s(x + y))$
$A_6 : \forall x(x \cdot 0 = 0)$
$A_7 : \forall x \forall y(x \cdot s(y)) = x \cdot y + x$ pour $\cdot$
$A_\Phi : (\Phi(0) \wedge \forall x(\Phi(x) \implies \Phi(s(x))) \implies \forall x \Phi(x)$.

Nous commencerons par quelques petits théorèmes importants :

Théorème 19 (Peano)**.** *Si, dans un modèle non-standard, une formule est vraie pour une infinité d'entiers standard, alors elle est vraie pour au moins un non-standard.*

Démonstration :
Soit $\phi(x)$ une formule à une variable libre et valide pour une infinité d'entiers du modèle $\mathfrak{M}$ (non-standard), et supposons que $\phi(x)$ soit faux pour tous les x non-standard de ce modèle.

Soit $\psi(x) = \exists y(x \leq y \wedge \phi(y)$, il est clair que $\mathfrak{M} \models \psi(0)$ (puisqu'une infinité d'entiers de $\mathfrak{M}$ vérifient ϕ (c'est bête, mais moi j'aime bien)).

Rappel : La relation d'ordre $\leq y$ est définie de la même façon que pour l'arithmétique de Presburger : $x \leq y \iff \exists z(x + z = y)$
Si x est un entier standard tel que $\mathfrak{M} \models \psi(x)$, alors s(x) est aussi un entier standard, et comme il existe une infinité de nombres entiers de $\mathfrak{M}$ vérifiant ϕ (je ne vais pas le faire à chaque fois), il en existe qui sont plus grands que s(x).
On en déduit que pour x standard $\mathfrak{M} \models \psi(x) \implies \psi(s(x))$.

Si x est non-standard $\mathfrak{M} \models \neg\psi(x)$ (par définition de ϕ), donc si x est non-standard $\mathfrak{M} \models \psi(x) \implies \psi(s(x))$.

On en déduit : $\mathfrak{M} \models \psi(0) \wedge \forall x(\psi(x) \implies \psi(s(x)))$, le schéma d'induction permet d'affirmer que $\mathfrak{M} \models \forall x \psi(x)$, ce qui est contradictoire avec la définition de ϕ.

Exercice 18 (Peano)**.** *Pourquoi un argument de compacité ne fonctionne-t-il pas ici ?*

Corollaire 2 (Peano)**.** *L'ensemble des entiers standard n'est pas définissable.*

Exercice 19 (Peano)**.** *Démontrer le corollaire précédent.*

Théorème 20 (Peano). *Il existe $2^{\aleph_0}$ modèles dénombrables non isomorphes de l'arithmétique de Peano.*

Démonstration :
On définit un nouveau symbole de prédicat $x \mid y \iff \exists t(t \cdot x = y)$ (x divise y). Par la suite $\mathbb{P}$ représentera les nombres premiers de $\mathbb{N}$.
Soit $P \subset \mathbb{P}$, et soit Φ_P^n l'ensemble de formules pour $n \in \mathbb{P}$:
$\Phi_P^n = \{\bigwedge_{\substack{i \in P \\ i \leq n}} (i \mid x) \wedge \bigwedge_{\substack{i \notin P \\ i \leq n}} \neg(i \mid x)\}$
Soit $\mathcal{T}_P$ la théorie $Peano \bigcup_{n \in \mathbb{N}} \Phi_P^n$, par compacité la théorie $\mathcal{T}_P$ est consistante et donc possède au moins un modèle.

Exercice 20 (Peano). *Démontrer l'affirmation précédente.*

Or il existe $2^{\aleph_0}$ ensembles de nombres premiers, et chaque modèle ne peut réaliser que $\aleph_0$ ensembles de formules de type Φ_P, il faut donc qu'il existe $2^{\aleph_0}$ modèles dénombrables non isomorphes.

Exercice 21 (Peano). *Montrer qu'il ne peut en exister plus.*

Remarque : Un ensemble de formules à une variable libre comme Φ_P s'appelle un type.

Formes des modèles : Les modèles de l'arithmétique de Peano sont, évidemment, des modèles de PréA', donc sont de la forme $\mathbb{M} = \mathbb{N} \biguplus \alpha.\mathbb{Z}$ (pour interpréter la fonction successeur), nous allons tenter de préciser ces modèles, pour la relation $\leq$.

Théorème 21 (Peano). *La relation $\leq$ (déjà définie) est une relation d'ordre totale*

Théorème 22 (Peano). $\forall x \forall y(x \leq y \iff (x = y \vee s(x) \leq y))$

Théorème 23 (Peano). $\forall x \exists y(x = y + y \vee s(x) = y + y)$

Théorème 24 (Peano). *Tous les entiers standard sont plus petits que les entiers non-standard*

Exercice 22 (Peano). *Démontrer les théorèmes précédents*

On peut donc écrire (Théorème 24) $\mathbb{M} = \mathbb{N} \oplus \alpha \times \mathbb{Z}$ où $\oplus$ signifie $\ll$ suivi, au sens de $\leq$, de $\gg$.
Essayons d'en savoir plus sur le α de l'équation précédente.
Soit $\sim$ la relation définie par $x \sim y$ si et seulement si il existe $k \in \mathbb{Z}$ tel que x = y + k (c'est-à-dire que x et y appartiennent à la même fibre, c'est-à-dire à la même composante connexe).

Exercice 23 (Peano). *Démontrer que $\sim$ est une relation d'équivalence sur $\alpha \times \mathbb{Z}$*

Chacune des classes d'équivalence étant isomorphe à $\mathbb{Z}$, on peut donc identifier $(\alpha \times \mathbb{Z}/\sim)$ et α.

Soit π la projection canonique $\alpha \times \mathbb{Z} \longrightarrow \alpha$, nous allons montrer que cette surjection induit un ordre sur α, pour cela nous devons montrer :
$((x \leq y) \wedge \neg(x \sim y) \wedge (x \sim x') \wedge (y \sim y')) \Longrightarrow (x' \leq y')$

Traduisons $x \leq y \wedge \neg(x \sim y) : \exists t(x + t = y)$ où t n'est pas standard.
Traduisons $x \sim x' : \exists n(x = x' + n)$ où $n \in \mathbb{Z}$.
Traduisons $y \sim y' : \exists m(y = y' + m)$ où $m \in \mathbb{Z}$.

Donc $x' + n + t = y' + m$ qui peut encore s'écrire $x' + (t + (n - m)) = y'$ c'est-à-dire $x' \leq y' \wedge \neg(x' \sim y')$.
Ce résultat permet de munir α d'une relation d'ordre que nous noterons $\prec$:
$i \prec j \iff \exists x \exists y(\pi(x) = i \wedge \pi(y) = j \wedge x \leq y \wedge \neg(x \sim y)$

Exercice 24 (Peano). *Démontrer que $\prec$ est une relation d'ordre total sur α.*

Etudions plus en détail les caractéristique de $\prec$:

Soit $i \in \alpha$, il existe donc x un élément non-standard de $\mathfrak{M}$ tel que $\pi(x) = i$; soit $j = \pi(x + x)$
$x < x + x$ (par définition de $<$) et $\neg(x \sim x + x)$ (par régularité de $+$) donc $i \prec j$, c'est-à-dire que $(\alpha, \prec)$ n'a pas de plus grand élément.

Comme $\pi(x) = \pi(s(x))$, on choisit u (qui est forcément non-standard) tel que, suivant les cas, $x = u + u$ ou $s(x) = u + u$ (on peut donc toujours se ramener au cas $x = u + u$, en changeant si nécessaire la valeur de x, puisque n'importe quel élément de la même fibre convient), et soit $k = \pi(u)$
$u < u + u$ et $\neg(u \sim u + u)$ donc $k \prec i$, c'est-à-dire que $(\alpha, \prec)$ n'a pas de plus petit élément.

Soit $i \in \alpha$ et $j \in \alpha$ tels que $i \prec j$, donc il existe x et y des éléments non-standard de $\mathfrak{M}$ tel que $\pi(x) = i$ et $\pi(y) = j$, et, comme précédemment, u et v tels que $u + u = x$ et $v + v = y$ (en effectuant, éventuellement, le changement de variable comme dans le cas précédent).
Soit $k = \pi(u + v)$, alors $i \prec k$ et $k \prec j$, c'est-à-dire que $(\alpha, \prec)$ est dense.

Exercice 25 (Peano)**.** *Démontrer l'affirmation précédente.*

Donc $(\alpha, \prec)$ est un ordre strict, total, dense, sans extremums et dénombrable, or cette théorie est $\aleph_0$-catégorique, elle n'a donc qu'un seul (à isomorphisme près) modèle dénombrable : $(\mathbb{Q}, <)$.

Théorème 25 (Peano)**.** *Les modèles non-standard de l'arithmétique de Peano sont de la forme* $\mathbb{M} = \mathbb{N} \oplus \mathbb{Q} \times \mathbb{Z}$*, pour la relation d'ordre, où* $\mathbb{Q} \times \mathbb{Z}$ *est muni de l'ordre lexicographique.*

Ce résultat semble, mensongèrement, indiquer que l'arithmétique de Peano ne possède qu'un seul modèle dénombrable, c'est évidemment faux, puisque la seule chose que nous avons montrée c'est que l'ordre naturel dans les modèles de l'arithmétique de Peano est toujours du même type, mais nous n'avons rien dit de l'addition ni de la multiplication.
Venons en au théorème principal : le théorème d'incomplétude de Gödel

Théorème 26 (d'incomplétude de Gödel)**.** *Toute théorie récursivement axiomatisable, consistante et capable de formaliser l'arithmétique de Peano (en fait de Robinson), est incomplète (il existe une formule indécidable).*

Nous n'allons pas démontrer ce théorème dans toute sa rigueur (trop long et trop technique et se trouve facilement sur le net) mais en donner un aperçu en insistant sur les points fondamentaux.
Etape 1 : on numérote les différents signes du langage (y compris les signes logiques (connecteurs, quantificateurs, les variables) les parenthèses, etc.).
Il existe de nombreuses façons de coder les signes d'un langage, je présente ci-dessous une méthode que j'aime bien car très générale :
Soit $\mathcal{L}$ un langage dénombrable (éventuellement sans l'égalité), $\mathcal{L} = (c_k, x_k, f_k^n, R_k^n)$, où n et k sont des entiers strictement positifs, les x_k sont des variables, les c_k des constantes, les f_k^n des fonctions n-aires, R_k^n des prédicats n-aires.
Comme signes logique nous prendrons en compte des signes de ponctuation : '(', ')' et ',', des connecteurs $\neg$ et $\Longrightarrow$, et un quantificateur $\forall$.
Les autres connecteurs ($\vee$ et $\wedge$ par exemple) et l'autre quantificateur ($\exists$) peuvent s'exprimer avec ceux choisis, le choix de ce jeu de connecteurs et de quantificateurs (n'importe quel choix pouvant générer tous les connecteurs et quantificateurs serait valide) est dû à leur utilisation dans les règles d'inférence (modus ponens et généralisation).

(	$\longrightarrow$	3	
)	$\longrightarrow$	5	
,	$\longrightarrow$	7	
$\neg$	$\longrightarrow$	9	
$\Longrightarrow$	$\longrightarrow$	11	
$\forall$	$\longrightarrow$	13	
c_k	$\longrightarrow$	$7 + 8.k$	$(k \geq 1)$
x_k	$\longrightarrow$	$13 + 8.k$	$(k \geq 1)$
f_k^n	$\longrightarrow$	$1 + 8.(2^n 3^k)$	$(n \geq 1 \wedge k \geq 1)$
R_k^n	$\longrightarrow$	$3 + 8.(2^n 3^k)$	$(n \geq 1 \wedge k \geq 1)$

Exercice 26 (Logique classique)**.** *Démontrer que la fonction qui associe un nombre entier à un signe du langage est injective.*

Pour l'arithmétique de Peano dont le langage est $\mathcal{L} = (0, s, +, \cdot, =)$ (j'ai ajouté l'égalité puisqu'il faut bien coder ce prédicat) ; nous poserons donc :

Nom	Signe	Code
c_1	0	15
x_1	x	21
f_1^1	s	49
f_1^2	+	97
f_2^2	$\cdot$	289
R_1^2	=	99

Etape 2 : à chaque formule (en nombre dénombrable) du langage on associe son nombre de Gödel.

Cette étape peut se résumer à associer de façon injective un entier naturel à toute suite finie d'entiers (c'est-à-dire à coder une telle suite par un entier), nous savons que c'est possible puisque l'ensemble des suites finies d'entiers est de cardinal $\aleph_0$, comme $\mathbb{N}$ (encore faut-il trouver une méthode qui soit définissable dans la théorie envisagée) ; plusieurs méthodes peuvent être envisagées, mais une de ces méthodes est particulièrement intéressante, la fonction vue un peu plus haut : la fonction β de Gödel, définie par :

$$\beta(x, y, z) = x \mod (1 + (z + 1) \cdot y).$$

D'abord un rappel :

Théorème 27 (des restes chinois)**.** *Prenons $m_0, m_1..., m_n$ des entiers supérieurs à 2, deux à deux premiers entre eux, et $a_1, a_2..., a_n$ des entiers. Le système d'équations :*
$x = a_0 \mod m_0$
$x = a_1 \mod m_1$
...
$x = a_n \mod m_n$
admet une unique solution modulo $M = m_0 \times m_1... \times m_n$.

Théorème 28. *La fonction β de Gödel permet de coder toute suite finie d'entiers, à l'aide de trois entiers (les deux premiers paramètres de la fonction β de Gödel, plus la longueur de la suite), donc à l'aide d'un seul.*

Démonstration :
Soit $a_0, a_1, ...a_n$ une suite d'entiers.
Soit m > n et tel que pour tous les éléments de notre suite m ! > a_i.
On pose $b_i = m!(i + 1) + 1$, les b_i sont premiers entre eux deux à deux.

Exercice 27. *Démontrer l'affirmation précédente.*

Indication : la démonstration est très simple, il suffit de considérer les diviseurs de $b_i - b_j$ pour i >j et de vérifier qu'ils ne peuvent être des diviseurs de b_i et b_j.

On applique le théorème des restes chinois au système :
$x = a_0 \mod m!(0 + 1) + 1$
$x = a_1 \mod m!(1 + 1) + 1$
...
$x = a_n \mod m!(n + 1) + 1$
Il existe donc une seule solution inférieure à $\prod_{i=0}^{n}(m!(i+1)+1))$, notons k cette solution, alors $a_i = \beta(k, m!, i)$.

Exercice 28. *Exhiber une bijection de $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$*

Nous avons vu que l'exponentiation est définissable dans l'arithmétique de Robinson, donc a fortiori dans l'arithmétique de Peano, avec la fonction β de Gödel (mais pas dans tous les fragments de l'arithmétique de Peano, et c'est l'intérêt de la fonction β de Gödel), nous allons donc donner un court exemple de codification des formules avec une méthode plus simple à mettre en oeuvre : en utilisant la décomposition (unique) d'un nombre en facteurs premiers (≪ être premier ≫ est aussi définissable, bien sûr) :

Exemple : le nombre de Gödel de l'axiome $A_1 : \forall x \neg(s(x) = 0)$ est

$2^{13}.3^{21}.5^{9}.7^{3}.11^{49}.13^{3}.17^{21}.19^{5}.23^{99}.29^{15}.31^{5}$ (soit un nombre de 273 chiffres)

Exercice 29. *Exhiber d'autres méthode de codage qui pourraient convenir (j'en vois une pas loin d'ici)*

Une question importante : est-ce que l'ensemble des nombres de Gödel des formules bien formées est récursif ? Autrement dit, pouvons nous envisager un programme qui soit capable de répondre à la question : soit n un nombre entier, est-il le nombre de Gödel d'une formule ? Autrement dit peut-on trouver ϕ tel que NombredeGödel$(\phi) = n$. Ces programmes s'appellent des parsers, ils existent bien, la réponse est donc oui.

Cette question n'est qu'un cas particulier du problème général de la reconnaissance des formules bien formées (well formed formulas en anglais, souvent abrévié en wff) dans le cadre des grammaires formelles.

Etape 3 : Une preuve d'une formule est en fait une formule qui commence par des axiomes et se termine par la formule en question, il est donc possible d'affecter un nombre de Gödel à une preuve d'une formule, mais la question est ≪ cette affectation est-elle récursive ? ≫.

C'est la partie délicate de la démonstration et nous n'allons pas entrer dans les détails (plus techniques et fastidieux que compliqués), mais simplement nous en convaincre (j'espère).

Commençons par poser le problème de façon formelle, et d'abord une notation, soit ϕ une formule, nous noterons $\ulcorner\phi\urcorner$ son nombre de Gödel.

Est-ce que l'ensemble des nombres de Gödel des axiomes est récursif, ou encore, est-ce que nous pouvons envisager un programme qui soit capable de répondre à la question : soit n un nombre entier, est-il le nombre de Gödel d'un axiome ? Là encore la réponse est oui, et c'est d'ailleurs là qu'intervient l'hypothèse ≪ théorie récursivement axiomatisable ≫.

Est-ce que l'ensemble des nombres de Gödel des formules qui sont des démonstrations de la formule de nombre de Gödel n est récursif ? Notre parser devient un peu plus compliqué (et la vraie complexité de la démonstration ainsi que la nécessité d'une théorie ≪ assez forte ≫ se cache ici), mais la réponse est toujours oui (en plus de besoins de l'étape 2, notre programme doit reconnaître les axiomes au début et la formule à démontrer à la fin).

C'est-à-dire que nous sommes capable de dire si le nombre m est le nombre de Gödel d'une démonstration de la formule de nombre de Gödel n, c'est dire de fabriquer une formule (récursive) Preuve(m, n), qui dit très exactement qu'il existe Ψ et ϕ, tels que Ψ est une preuve de ϕ (dans notre théorie bien sûr) et tels que $m = \ulcorner\Psi\urcorner$ et $n = \ulcorner\phi\urcorner$.

Etape 4 : Construisons une première formule bizarre : on pose $\Delta(n) = \ulcorner\phi(\ulcorner\phi\urcorner)\urcorner$, où ϕ est une formule à une variable libre et $n = \ulcorner\phi\urcorner$

Ensuite on pose $\Gamma(n) \iff \forall x(\neg\text{Preuve}(x, \Delta(n)))$ (on sent poindre un argument du genre diagonale de Cantor)

Etape 5 : Bon alors, elle vient cette diagonale ? :

Il nous reste à nous poser **la question importante** : la formule $\Gamma(\ulcorner\Gamma\urcorner)$ est-elle vraie, ou fausse ou indécidable ?

Commençons par ≪ déplier ≫ notre formule $\Gamma(\ulcorner\Gamma\urcorner) \iff \forall x(\neg\text{Preuve}(x, \ulcorner\Gamma(\ulcorner\Gamma\urcorner)\urcorner))$, c'est-à-dire que Γ est vraie si et seulement si elle n'est pas démontrable.

L'existence d'une telle formule termine la démonstration du premier théorème d'incomplétude de Gödel.

Après ce gros morceau, voici un autre résultat, le **théorème de Tennenbaum** qui devrait permettre de gagner du temps de sommeil en ne cherchant pas un Graal dont on sait qu'il n'existe pas ...

Définition : un modèle $\mathfrak{M} = (\mathbb{M}, 0, s, +, \cdot)$ de l'arithmétique est dit récursif si il existe une bijection $\phi : \mathbb{N} \longrightarrow \mathbb{M}$ telle que

L'application $Plus : \mathbb{N} \times \mathbb{N} \Longrightarrow \mathbb{N}$ définit par $Plus(x, y) = \phi^{-1}(\phi(x) +_{\mathbb{M}} \phi(y))$ est récursive.

L'application $Mult : \mathbb{N} \times \mathbb{N} \Longrightarrow \mathbb{N}$ définit par $Mult(x, y) = \phi^{-1}(\phi(x) \cdot_{\mathbb{M}} \phi(y))$ est récursive.

(en prenant ϕ = identité, il est clair que $\mathbb{N}$ est récursif).

Théorème 29 (Peano - Tennenbaum)**.** *Il n'existe pas de modèle non-standard de l'arithmétique qui soit récursif.*

Remarque : La démonstration est un peu trop technique pour trouver sa place ici, mais on peut la trouver sur le net.

Conséquence : inutile de chercher à définir une addition et une multiplication dans les modèles déjà vus.

Peut-on déduire que le théorème d'incomplétude signe l'échec des mathématiques (sous leur forme axiomatique) ? De mon point de vue : absolument pas, c'est juste un résultat (presque) comme les autres, et qui ne concerne que la logique du premier ordre, comme nous allons le voir ci-dessous, et, toujours selon moi, moins important que le théorème de complétude de Gödel.

On pourrait même dire que le théorème d'incomplétude permet de prévoir un avenir radieux aux mathématiques (et, en tout état de cause, aux mathématiciens), puisque nous pourrons toujours ajouter autant d'axiomes que l'on veut et toujours avoir de nouveaux théorèmes à démontrer.

Petit florilège incomplet(forcément) de ce qu'il n'aurait jamais fallu écrire à propos du théorème d'incomplétude de Gödel

Exercice 30. *Critiquer la phrase précédente.*

Voir les sites suivants qui recueillent certains excès :
http ://www.yann-ollivier.org/goedel/goedel.html
http ://www.sm.luth.se/ torkel/eget/godel.html
Quelques exemples supplémentaires, il est facile d'en trouver d'autres sur le net (je ne change pas le texte, juste l'orthographe) :

> *Souvenez-vous du théorème d'incomplétude de Gödel qui dit que les axiomes d'une théorie (croyances) ne peuvent être prouvés par cette théorie.*

> *Mais l'on démontrera ici, en utilisant la logique mathématique moderne, qu'il est impossible que le Coran soit à la fois parfait (au sens de : permettant de démontrer toute proposition vraie) et non contradictoire. Or comme il affirme être l'un et l'autre, le Coran ment.*

On trouve la même chose à propos de la Bible.

> *Il existe donc une incomplétude dans les systèmes d'axiomes, quelque chose comme un trou dans un champ de savoir, dont l'obturation demanderait une suite de procédures infinie, de toute façon vouée à l'échec.*

> *Je me borne à donner l'énoncé du Théorème de l'incomplétude, l'internaute fera lui-même la conclusion que l'évolutionnisme est une forfaiture, au moins comme théorie valide et admise universellement comme vraie, alors qu'elle est PAR CE THEOREME improuvable, et donc, non-science. A L'INVERSE, le Paradigme du Créationnisme rationnel, n'étant pas une théorie, mais un paradigme, alors on en déduit que le Créationnisme Rationnel est immensément plus scientifique que la Théorie de l'Evolution...*

4) Arithmétique du second ordre

La logique du second ordre diffère de la logique du premier ordre en ce qu'elle autorise la quantification des sous-ensembles et non seulement des éléments (par convention les éléments sont généralement représentés par des lettres minuscules, et les sous-ensembles par des lettres majuscules).

Le langage de l'arithmétique du second ordre est $\mathcal{L} = (0, s, +, \cdot)$.

Remarque : $\in$ et $=$ sont des symboles logiques et non spécifiques de la théorie.

Axiomes de l'arithmétique du second ordre

A_1 à A_7 (c'est-à-dire les axiomes de l'arithmétique de Robinson (qui elle est du premier ordre) auquel s'ajoute l'axiome d'induction du second ordre (car il nécessite une quantification sur les sous ensembles) :

$A_8 : \forall X((0 \in X \wedge \forall x(x \in X \Longrightarrow s(x) \in X) \Longrightarrow \forall x(x \in X))$.

En logique du second ordre, un modèle de l'arithmétique (mais c'est généralisable) est légèrement différent d'un modèle du premier ordre :

$\mathfrak{M} = (\mathbb{M}, 0, s, +, \cdot, D)$,

$\mathbb{M}, 0, s, +$ et $\cdot$ ont la même signification que pour un modèle du premier ordre, et D est un sous ensemble de $\mathfrak{P}(\mathbb{M})$ (l'ensemble des parties de $\mathbb{M}$) qui précise le domaine des quantification sur des sous-ensembles, quand $D = \mathfrak{P}(\mathbb{M})$, on parle de modèle total.

Théorème 30 (Second ordre)**.** *Il n'existe qu'un seul modèle total de l'arithmétique du second ordre (appelé aussi modèle standard de l'arithmétique)*

Exercice 31 (Second ordre)**.** *Démontrer le théorème précédent (avec le schéma d'induction du second ordre, bien sûr)*

Remarques :

L'arithmétique du second ordre est parfois considérée comme une théorie faible des ensembles.

La logique du second ordre possède la « mauvaise » propriété suivante :

Il n'existe pas de système de règles d'inférence pour la logique du second ordre qui soit à la fois robuste (sound en anglais) et complet.

Robuste : $Z \vdash X \Longrightarrow Z \models X$

Complet : $Z \models X \Longrightarrow Z \vdash X$

C'est-à-dire de système où tout ce qui est prouvable est vrai dans tous les modèles et réciproquement.

On peut aussi noter que la logique du second ordre ne permet pas de démontrer le théorème de compacité, ni le théorème de Löwenheim-Skolem.

5) Aller plus loin ...

Avec l'arithmétique de Peano comme point de départ, il est possible de créer de nouvelles théories plus faibles de plusieurs façons (il existe des centaines, sans doute des milliers d'études portant sur les arithmétiques faibles) :

1) Supprimer un élément du langage (Presburger)
2) Supprimer le schéma d'induction (Robinson)
3) Remplacer un élément du langage (Cégielki)
4) Contraindre le schéma d'induction (Parikh)
5) Contraindre les formules du langage (Baby arithmetic)
6) Changer de logique (Heyting)

par exemple :

Arithmétique de Skolem-Mostowski (avec la multiplication, sans l'addition, ni le successeur) Cette théorie est décidable.

Arithmétique de Kalmar (Uniquement la multiplication et le schéma d'induction est restreint aux formules élémentairement récursives)

Arithmétique de Heyting (aritmétique intuitionniste) Les axiomes sont les mêmes que l'arithmétique de Peano, mais la logique utilisée est la logique intuitionniste (sans tiers exclu).

On peut, bien sûr, définir des arithmétiques faibles en logique intuitionniste.

Arithmétique de Woods avec 0, s, $\perp$ (la relation de coprimalité (attention ce symbole est souvent utilisé en logique pour désigner le « Faux »)). Cette théorie est indécidable.

Arithmétique avec exponentiation. Cette théorie permet de définir + et $\cdot$, elle est donc indécidable.

$x \cdot y \Longleftrightarrow \forall t(t^z = (t^x)^y)$
$x + y \Longleftrightarrow \forall t \forall u(t^{(u^z)} = (t^{u^x})^{u^y}$

Arithmétique de Cegielski avec $\mid$ et s ,(où $x \mid y$ signifie x divise y ; sans 0 ni égalité, pour une fois)
Cette théorie est indécidable

Exercice 32. *Démontrer que* $0, 1, =, \perp$*, ppcm(x, y), Prime(x), la fonction prédécesseur (noté p par la suite, et telle que p(0) = 0) sont définissable avec* $\mid$ *et s.*

Certains des résultats de l'exercice précédent sont utiles pour la définition de + et $\cdot$.

La démonstration que $\cdot$ est définissable avec $\mid$ et s n'est pas très simple, elle fait appel à trois théorèmes :

Théorème 31 (de Dirichlet)**.** *Soit n et m deux nombres premiers entre eux, alors il existe une infinité de nombres premiers de la forme n + k.m, où k est un nombre entier.*

Théorème 32 (de Fermat (le petit))**.** *Soit p un nombre premier et a un nombre non divisible par p (donc* $a \perp p$*), alors* $a^{p-1} \equiv 1[p]$

Théorème 33 (Arithmétique)**.** *Les deux propositions suivantes sont équivalentes :*

1) $z = xy$

2) Pour tout nombre premier p tel que $\neg(p \mid x)$ *et* $\neg(p \mid y)$*, il existe* x' *et* y' *premiers entre eux et avec x, y et z tels que* $\begin{cases} xx' & \equiv & -1\,[p] \\ yy' & \equiv & -1\,[p] \\ zx'y' & \equiv & 1\,[p] \end{cases}$

Exercice 33. *Démontrer le sens 2)* $\Longrightarrow$ *1)*

Démonstration du sens 1) $\Longrightarrow$ 2)

En fait la seule chose à développer est l'existence de x', le reste en découle trivialement :

$p \perp x \Longrightarrow p \perp x^{p-2}$ (p est premier donc >1)

Donc il existe un infinité de n tels que $x_n = np - x^{p-2}$ est un nombre premier (théorème de Dirichlet), comme il existe une infinité de tels n, on peut en choisir un tel que $x_n > x$.

$xx_n = nxp - x.x^{p-2}$ donc :

$xx_n \equiv -x^{p-1}\,[p]$ c'est-à-dire :

$xx_n \equiv -1\,[p]$ (petit théorème de Fermat).

x_n étant premier et plus grand que x, il est bien premier avec x, nous avons trouvé un x' qui vérifie notre condition.

Exercice 34. *A l'aide des résultats précédents, démontrer que* $\cdot$ *et + sont définissables dans le langage* $\mid$ *et s*

Ce qui montre bien que cette théorie est indécidable.

Indication : commencer par $\cdot$ et pour +, on pourra remarquer que
$(x(x + y) + 1)(y(x + y) + 1) = ((x + y)^2(xy + 1)) + 1$ (attention au petit piège).

Arithmétique avec $<$ et $\mid$ (toujours sans 0 ni égalité, pour deux fois)

Théorème 34. *s est définissable avec* $<$ *et* $\mid$

Exercice 35. *Démontrer le théorème précédent.*

Ce théorème nous ramène au cas précédent, elle est donc aussi indécidable.

Arithmétique avec la fonction β de Gödel

Rappel : La fonction de Gödel est définit par $\beta(x, y, z) = x \mod (1 + (z + 1) \cdot y)$

Exercice 36. *Démontrer que $<$ et $|$ sont définissables avec la fonction de Gödel.*

Cet exercice nous ramène au cas précédent, elle est donc aussi indécidable.

Arithmétique de Parikh (ou $I\Delta_0$)

Le langage est $\mathcal{L} = (0, s, +, \cdot)$
Les axiomes sont ceux de l'arithmétique de Robinson plus quelques axiomes qui assurent quelques résultats bien connus, mais indécidables dans Robinson :
Commutativité de $+$ et $\cdot$.
Associativité $+$ et $\cdot$.
Distributivité de $\cdot$ sur $+$.
Plus le schéma d'induction, mais réduit aux formules de Δ_0 (c'est-à-dire les formules ne contenant que des quantificateurs bornés)

Par exemple, soit G(x) la propriété de Goldbach (le prédicat P(x) indique que x est premier (facilement définissable)) :
$G(x) \iff \exists y \exists z(x \leq s(0) \vee (P(y) \wedge P(z) \wedge x + x = y + z))$

Exercice 37. *Démontrer que $G(x) \in \Delta_0$*

Arithmétique de Buss
L'arithmétique de Buss est $I\Delta_0$ plus trois prédicats :
$|x| = \lceil (lg_2(x + 1)) \rceil$
$x\#y = 2^{|x| \cdot |y|}$
$x/2 = \lfloor (x/2) \rfloor$
Avec des axiomes qui permettent de définir ces prédicats.

Baby arithmetic (ou de Goodstein) :
Le langage est le même que pour l'arithmétique de Robinson, mais la logique utilisée ne permet pas les quantificateurs, et les axiomes sont presque ceux de Robinson, sauf que ceux-ci utilisent des quantificateurs, il faut donc les remplacer par des schémas d'axiomes, par exemple :
L'axiome $A_1 = \forall x \neg(s(x) = 0)$ est remplacé par le schéma $A_1^n = \neg(s(n) = 0)$.
Cette théorie est complète.

Arithmétique de Büchi $(+, V_k)$: pour k un nombre premier, on note V_k la fonction qui à chaque entier fait correspondre la plus grande puissance de k qui le divise. Cette théorie est décidable.

Arithmétique avec 2^x : C'est la théorie de $(\mathbb{N}, +, 2^x)$. Cette théorie est décidable.

Arithmétique de Putnam : C'est la théorie de $(\mathbb{N}, +, C)$ où C est un prédicat unaire qui identifie les carrés. Cette théorie est incomplétable.
Sans nous y attarder trop, cette théorie permet de mettre en évidence un résultat que je trouve surprenant :

Théorème 35 (Putnam)**.** *On peut définir la multiplication, simplement à l'aide d'un prédicat identifiant les carrés et $+$.*

Exercice 38 (Putnam)**.** *Démontrer le théorème précédent*

Indication 1 : il faut définir un premier prédicat P dont la sémantique est $P(x, y)$ si et seulement si $y = x^2$, puis un deuxième prédicat dont la sémantique est : $m(x, y, z)$ si et seulement si $z = x \times y$. Pour se simplifier l'écriture, le premier prédicat pourra s'écrire $y = x^2$ et le deuxième $z = x \times y$.

Indication 2 : l'indication 1 est incomplète (mais complètable).

Le théorème précédent démontre que l'arithmétique de Robinson est définissable dans l'arithmétique de Putnam, ce qui établit bien que cette dernière est incomplétable.

Arithmétique Σ_n ou Π_n (avec un nombre borné de d'alternances de quantificateurs dans les formules).

Arithmétique avec $\cdot$ et $<_P$ (où $<_P$ est la relation d'ordre restreinte aux nombres premiers). Cette théorie est décidable

Arithmétique avec $\cdot$ et $<$. Cette théorie est indécidable

Arithmétique avec $\cdot$ et $\sim$ (où $\sim$ est la relation d'équivalence « même nombre de composantes premières »). Cette théorie est décidable

Arithmétique avec + et P (où P est un prédicat pour identifier les nombres premiers). La question de savoir si $\cdot$ est définissable dans cette arithmétique est ouverte.

Arithmétiques Modales (en particulier arithmétique épistémique).

Etc. etc.

Conjecture de Woods-Erdös. Question posée initialement par Julia Robinson (pour les très courageux, puisque cette conjecture est toujours ouverte).

Peut-on définir l'addition et la multiplication à l'aide de l'égalité, de la relation de coprimalité et de la fonction successeur ?

Une autre façon de le dire : $Th(\mathbb{N}, 0, +, \cdot) = Th(\mathbb{N}, 0, s, \perp)$, où $\perp$ est le prédicat de coprimalité (arithmétique de Woods).

6) Le mot de la fin

- Merci, Papa, je n'ai pas tout compris, mais c'est déjà un peu plus clair, j'ai au moins compris qu'un problème qui paraît très simple et parfaitement « naturel » n'est pas forcément aussi simple que cela dès que l'on se penche vraiment dessus. Enfin, là je parle de l'arithmétique, parce que pour les bébés, tu n'as toujours rien expliqué ...

- Oh, pour les bébés, c'est facile, c'est comme l'arithmétique, sauf que $1 + 1 = 3$.