TD9 - Preuves formelles

François Le Maître - *f.lemaitre@math.univ-paris-diderot.fr*

Exercice 1 (Des preuves de qualité)**.**
Soit $\mathcal{L}$ un langage et $\varphi(x), \psi(x)$ deux formules à une variable libre.

1. Dans la théorie formée de l'unique énoncé $\forall x(\varphi(x) \to \psi(x))$, donner une preuve formelle de l'énoncé $(\forall x\varphi(x)) \to (\forall x\psi(x))$.
2. Montrer que les deux énoncés $\forall x(\varphi(x) \wedge \psi(x))$ et $(\forall x\varphi(x))$ sont équivalents en donnant une preuve formelle de chacun d'eux dans la théorie formée uniquement de l'autre.

Exercice 2 (Règle de généralisation)**.**
Dans cet exercice, on considère afin de simplifier les définitions par induction que $\exists x\psi$ est simplement une abréviation de $\neg\forall x\neg\psi$. Cela revient à "oublier" l'axiome logique qui définissait le lien entre $\exists$ et $\forall$.
Soit $\mathcal{L}$ un langage. Une $\mathcal{L}$-formule φ est *universelle* si elle est sans quantificateurs ou de la forme $\forall x_1 ... \forall x_n \psi$ où ψ est sans quantificateurs. On définit par induction sur la une application F de l'ensemble des $\mathcal{L}$-formules dans $\{0, 1\}$ par :

— si φ est une formule atomique, alors $F(\varphi) = 1$,
— si φ est de la forme $\forall x\psi$ avec ψ universelle alors $F(\varphi) = F(\psi)$,
— si φ est de la forme $\forall x\psi$ avec ψ non universelle alors $F(\varphi) = 0$,
— F respecte les connecteurs logiques, par exemple $F(\neg\varphi) = 1 - F(\varphi)$.

1. Montrer que si la $\mathcal{L}$-formule φ peut être prouvée formellement sans utiliser la règle de généralisation, alors $F(\varphi) = 1$.
2. En déduire l'existence d'une $\mathcal{L}$-formule tautologique dont toute preuve formelle utilise la règle de généralisation.

Exercice 3 (Axiomes de Péano)**.**
On se place dans le langage $(0, S, +, \times)$ où S est unaire (fonction Successeur). On considère les axiomes suivants :

(A1) $\forall x(\neg Sx = 0)$
(A2) $\forall x(x = 0 \vee \exists y, x = Sy)$
(A3) $\forall x\forall y(Sx = Sy \to x = y)$
(A4) $\forall x(x + 0 = x)$
(A5) $\forall x\forall y(x + Sy = S(x + y))$
(A6) $\forall x(x \times 0 = 0)$
(A7) $\forall x\forall y(x \times Sy = x \times y + x)$

Pour chaque formule $F(x, \bar{y})$, on ajout l'axiome

$(\mathrm{A}_{F,x})$ $\forall\bar{y}\left[(F(0, \bar{y}) \wedge \forall z(F(z, \bar{y}) \to F(Sz, \bar{y})) \to \forall xF(x, \bar{y})\right].$

On obtient alors la théorie PA de l'*arithmétique de Péano.*

1. Donner une démonstration formelle du fait que l'addition soit commutative.
2. Montrer que dans PA on peut faire des récurrences fortes en introduisant (et en prouvant formellement) un analogue de $(\mathrm{A}_{F,x})$.
3. Montrer qu'il existe des modèles de PA où tout entier est de la forme $S^n(0)$ pour un $n \in \mathbb{N}$, et d'autres où ce n'est pas le cas.

Exercice 4 (Fonctions définissables dans PA.)**.**
Une fonction $f : \mathbb{N}^k \to \mathbb{N}$ est définissable dans PA s'il existe une formule $F(\bar{x}, y)$ à $k+1$ variables libres telle que pour tout $(\bar{n}, m) \in \mathbb{N}^k \times \mathbb{N}$ on ait $\mathbb{N} \vdash F(\bar{n}, m)$ si et seulement si $f(\bar{n}) = m$.

On va montrer que la fonction exponentielle est définissable. Il faut d'abord coder les suites finies d'entiers. On définit la fonction β (dite de Gödel) par : $\beta(i, a, b)$ est le reste de la division euclidienne de b par $a \times (i + 1) + 1$.

1. Montrer que la fonction β est définissable dans PA.
2. Soit $(n_1, ..., n_k)$ une suite finie d'entiers. Soit $m \geqslant k$ un entier tel que $a := m!$ soit supérieur à tous les n_i.
   — Monter que les nombres $a \times (i + 1) + 1$ pour $i = 1, ..., k$ sont premiers entre eux deux à deux.
   — En déduire qu'il existe un entier b tel que pour $i = 1, ..., k$, on a $\beta(i, a, b) = n_i$.
3. Conclure que la fonction exponentielle $(n, m) \mapsto n^m$ est définissable dans PA.

On peut ainsi exprimer le dernier théorème de Fermat dans PA. Ce dernier a été démontré par Andrew Wiles dans ZF, et on ne sait pas du tout s'il est prouvable dans PA.