LOGIQUE

Un exemple de preuve formelle

On veut prouver, à partir des axiomes de Peano que

$$\forall x \;\; 0 + x = x$$

Voici une preuve *détaillée*, mais pas encore *formelle*, partant des axiomes de Peano.

1−	$Notons : P(x) : 0 + x = x$	(notation)
2−	$0 + 0 = 0$	(axiome A4)
3−	$P(0)$	(traduction de (2) via la notation (1))
4−	$SupposonsP(x) : \;\; 0 + x = x$	(hypothèse)
5−	$0 + S(x) = S(0 + x)$	(axiome A5)
6−	$0 + S(x) = S(x)$	(déduit de (4,5))
7−	$P(S(x))$	(traduction de (6) via la notation (1))
8−	$P(x) \to P(S(x))$	(déduit de (7) par “déchargement de l'hypothèse (4)”)
9−	$\forall x(P(x) \to P(S(x)))$	(déduit de (8) par généralisation)
10−	$\forall x P(x)$	(déduit de (3,9) et du schéma d'axiome de récurrence)
11−	$\forall x \;\; 0 + x = x$	(traduction de (10) via la notation (1))

Une preuve *formelle*.

On écrit maintenant, en suivant les mêmes idées, une preuve *formelle* :
- dans le système logique NK,
- partant des axiomes de Peano.

0−	$\mathrm{PA} \vdash \forall \mathrm{x}\ \ \mathrm{x}+0=\mathrm{x}$	$(\mathtt{A4}, \mathtt{ax})$
1−	$\mathrm{PA} \vdash 0+0=0$	$(0, \forall_{\mathtt{elim}})$
2−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \forall \mathrm{y},\mathrm{z}\ \ (\mathrm{y}+\mathrm{S}(\mathrm{z})=\mathrm{S}(\mathrm{y}+\mathrm{z}))$	$(\mathtt{A5}, \mathtt{ax})$
3−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(0+\mathrm{x})$	$(2, \forall^2_{\mathtt{elim}})$
4−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash 0+\mathrm{x}=\mathrm{x}$	$(\mathtt{ax})$
5−	$\mathrm{EG} \vdash \forall \mathrm{y},\mathrm{z}\ \ \mathrm{y}=\mathrm{z} \to \mathrm{S}(\mathrm{y})=\mathrm{S}(\mathrm{z})$	$(\mathtt{COMPF}, \mathtt{ax})$
6−	$\mathrm{EG} \vdash \ \ 0+\mathrm{x}=\mathrm{x} \to \mathrm{S}(0+\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(5, \forall^2_{\mathtt{elim}})$
7−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ 0+\mathrm{x}=\mathrm{x} \to \mathrm{S}(0+\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(6, \mathtt{aff})$
8−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ \mathrm{S}(0+\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(4, 7, \to_{\mathtt{elim}})$
9−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(0+\mathrm{x}) \ \wedge\ \mathrm{S}(0+\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(3, 8, \wedge_{\mathtt{intro}})$
10−	$\mathrm{EG} \vdash \ \ \forall \mathrm{y},\mathrm{z},\mathrm{t}\ \ (\mathrm{y}=\mathrm{z} \wedge \mathrm{z}=\mathrm{t}) \to \mathrm{y}=\mathrm{t})$	$(\mathtt{TRANS}, \mathtt{ax})$
11−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ \forall \mathrm{y},\mathrm{z},\mathrm{t}\ \ (\mathrm{y}=\mathrm{z} \wedge \mathrm{z}=\mathrm{t}) \to \mathrm{y}=\mathrm{t})$	$(10, \mathtt{aff})$
12−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ (0+\mathrm{S}(\mathrm{x})=\mathrm{S}(0+\mathrm{x}) \ \wedge\ \mathrm{S}(0+\mathrm{x})=\mathrm{S}(\mathrm{x})) \to 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(11, \forall^2_{\mathtt{elim}})$
13−	$\mathrm{PA}, 0+\mathrm{x}=\mathrm{x} \vdash \ \ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(9, 12, \to_{\mathtt{elim}})$
14−	$\mathrm{PA} \vdash \ \ 0+\mathrm{x}=\mathrm{x} \ \to\ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x})$	$(13, \to_{\mathtt{intro}})$
15−	$\mathrm{PA} \vdash \ \ \forall \mathrm{x}\ \ (0+\mathrm{x}=\mathrm{x} \ \to\ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x}))$	$(14, \forall_{\mathtt{intro}})$
16−	$\mathrm{PA} \vdash \ \ 0+0=0 \ \wedge\ \forall \mathrm{x}\ \ (0+\mathrm{x}=\mathrm{x} \ \to\ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x}))$	$(1, 15, \wedge_{\mathtt{intro}})$
17−	$\mathrm{PA} \vdash \ \ [0+0=0 \ \wedge\ \forall \mathrm{x}\ \ (0+\mathrm{x}=\mathrm{x} \ \to\ 0+\mathrm{S}(\mathrm{x})=\mathrm{S}(\mathrm{x}))] \to (\forall \mathrm{x}\ \ 0+\mathrm{x}=\mathrm{x})$	$(\mathrm{REC}_{\Phi}, \mathtt{ax})$
18−	$\mathrm{PA} \vdash \ \ \forall \mathrm{x}\ \ 0+\mathrm{x}=\mathrm{x}$	$(16, 17, \to_{\mathtt{elim}})$

N.B. dans (17) Φ désigne la formule : $0+x=x$.

Commentaire : nous avons ainsi réduit un *raisonnement* sur l'addition des entiers, à une suite de manipulations syntaxiques qui s'apparentent à un *calcul*. Les formules et les preuves sont des mots et si on les représente par des entiers (par exemple leur numéro dans l'ordre hiérarchique) :
- l'ensemble des preuves est un ensemble calculable : on peut écrire un programme, d' ailleurs assez simple, qui teste si un nombre est le code d'une preuve correcte
le programme répond **oui** si et seulement si le nombre code une preuve ; le programme répond **non** si et seulement si le nombre code un mot qui n' est pas une preuve.
- l'ensemble des théorèmes d'une théorie axiomatique T, c'est à dire des formules qui ont une preuve partant des axiomes de T, est semi-calculable : on peut écrire un programme, qui détermine si le nombre est le code d'une formule prouvable ; le programme répond **oui** si et seulement si le nombre code une formule **prouvable** ; le programme répond **non** ou bien **boucle** indéfiniment si et seulement si le nombre code une formule **non-prouvable**.

Pas de preuve *formelle*

On se demande si l'usage de l'axiome de récurrence, dans la preuve précédente, était incontournable. Autrement dit : peut-on prouver,$\forall x\ \ 0 + x = x$:
- dans le système logique NK,
- en partant des axiomes de P0 seulement (l'arithmétique "élémentaire").
On considère la structure suivante :

$$\begin{aligned}
\mathcal{N} &=_{\text{déf.}} (\mathbb{N} \times \{\bullet\}) \cup (\mathbb{N} \times \{\circ\}) \text{ où } \bullet \neq \circ \\
0_{\mathcal{N}} &=_{\text{déf.}} \langle 0, \bullet \rangle \\
\mathrm{S}_{\mathcal{N}}\langle p, \alpha \rangle &=_{\text{déf.}} \langle \mathrm{S}p, \alpha \rangle \text{ où } \alpha \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle +_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p + q, \alpha \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\} \\
\langle p, \alpha \rangle \times_{\mathcal{N}} \langle q, \beta \rangle &=_{\text{déf.}} \langle p \times q, \beta \rangle \text{ où } \alpha, \beta \in \{\bullet, \circ\}
\end{aligned}$$

Le domaine $\mathcal{N}$ est constitué de deux copies de $\mathbb{N}$: les entiers « noirs » $\langle p, \bullet \rangle$ ($p \in \mathbb{N}$) et les entiers « blancs » $\langle p, \circ \rangle$ ($p \in \mathbb{N}$). La constante zéro est interprétée par le zéro noir $\langle 0, \bullet \rangle$; les opérations successeur, addition et multiplication sont interprétées de telle sorte que :
- le successeur conserve la couleur de son argument,
- l'addition prend la couleur de son *premier* argument,
- la multiplication prend la couleur de son *second* argument.

1. Montrer que $\mathcal{N}$ est un modèle de P′0 (= PO sans $A2$) .

2. La formule $\forall x\ \ 0 + x = x$ est-elle *vraie* dans la structure $\mathcal{N}$?
3. Montrer qu' *il n'existe pas* de preuve de $\forall x\ \ 0 + x = x$ à partir des axiomes de P′0.
4. Montrer qu' *il n'existe pas* non-plus de preuve de $\exists x\ \ \neg(0 + x = x)$ à partir des axiomes de P′0.