TD 8 - Preuves formelles

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 dans la théorie formée de l'unique énoncé $\forall x(\varphi(x) \to \psi(x))$ en donnant une preuve formelle de chacun d'eux dans la théorie formée de l'autre et de $\forall x(\varphi(x) \to \psi(x))$.

Solution de l'exercice 1. On va utiliser de manière répétée le *lemme de déduction* qui dit que si $T \cup \{\psi\} \vdash \varphi$ alors $T \vdash \psi \to \varphi$. Remarquons que la particularisation est valide lorsque l'on effectue pas de substitution (que l'on substitue x à x !).

1. Soit $T = \{\forall x(\varphi(x) \to \psi(x))\}$. D'après le lemme de déduction il suffit de montrer que $T \cup \{(\forall x\varphi(x))\} \vdash \forall x\psi(x)$. Or dans la théorie $T \cup \{(\forall x\varphi(x))\}$ on a :

$$\begin{aligned}
(\text{Hypothèse}) &\vdash \forall x\varphi(x) && (1)\\
(\text{Particularisation}) &\vdash \varphi(x) && (2)\\
(\text{Hypothèse}) &\vdash \forall x(\varphi(x) \to \psi(x) && (3)\\
(\text{Particularisation}) &\vdash \varphi(x) \to \psi(x) && (4)\\
(\text{Modus Ponens de 2 et 4}) &\vdash \psi(x) && (5)\\
(\text{Généralisation}) &\vdash \forall x\psi(x), && (6)
\end{aligned}$$

   ce qui est le résultat voulu.
2. Montrons d'abord que $T \cup \{\forall x(\varphi(x) \wedge \psi(x))\} \vdash \forall x\varphi(x)$. Dans la théorie $T \cup \{\forall x(\varphi(x) \wedge \psi(x))\}$ on a :

$$\begin{aligned}
(\text{Hypothèse}) &\vdash \forall x(\varphi(x) \wedge \psi(x)) && (1)\\
(\text{Particularisation}) &\vdash \varphi(x) \wedge \psi(x) && (2)\\
(\text{Tautologie}) &\vdash (\varphi(x) \wedge \psi(x)) \to \varphi(x) && (3)\\
(\text{Modus Ponens de 2 et 3}) &\vdash \varphi(x) && (4)\\
(\text{Généralisation}) &\vdash \forall x\varphi(x), && (5)
\end{aligned}$$

   et donc on a bien $T \cup \{\forall x(\varphi(x) \wedge \psi(x))\} \vdash \forall x\varphi(x)$ (on n'a pas eu besoin de T). Dans l'autre sens, plaçons nous dans la théorie $T \cup \{\forall x\varphi(x)\}$. On a la démonstration formelle suivante :

$$\begin{aligned}
(\text{Hypothèse}) &\vdash \forall x(\varphi(x)) && (1)\\
(\text{Particularisation}) &\vdash \varphi(x) && (2)\\
(\text{Hypothèse}) &\vdash \forall x(\varphi(x) \to \psi(x))) && (3)\\
(\text{Particularisation}) &\vdash \varphi(x) \to \psi(x) && (4)\\
(\text{Modus Ponens de 2 et 4}) &\vdash \psi(x) && (5)\\
(\text{Tautologie}) &\vdash \varphi(x) \to (\psi(x) \to (\varphi(x) \wedge \psi(x))) && (6)\\
(\text{Modus Ponens de 2 et 6}) &\vdash \psi(x) \to (\varphi(x) \wedge \psi(x)) && (7)\\
(\text{Modus Ponens de 5 et 7}) &\vdash \varphi(x) \wedge \psi(x) && (8)\\
(\text{Généralisation}) &\vdash \forall x\varphi(x) \wedge \psi(x) && (9)
\end{aligned}$$

Ainsi on a bien $T \cup \{\forall x \varphi(x)\} \vdash \forall x \varphi(x) \wedge \psi(x)$

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 complexité 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.

Solution de l'exercice 2.

1. On va montrer par induction sur la longueur d'une démonstration n'utilisant pas la généralisation que toutes ses étapes φ satisfont $F(\varphi) = 1$. Pour cela, il suffit de montrer que les axiomes logiques satisfont $F(\varphi) = 1$ et que le modus ponens préserve cette propriété, c'est-à-dire que si $F(\varphi) = 1$ et $F(\varphi \to \psi) = 1$ alors $F(\psi) = 1$. Commençons par les axiomes logiques.
   - Si φ est un axiome de distribution $\forall v(m \to n) \to (m \to \forall v n)$ où v n'a aucune occurence libre dans m, on distingue plusieurs cas :
     - si φ est une tautologie, $F(\varphi) = 1$ car F respecte les connecteurs logiques.
     - si m ou n contiennent des quantificateurs, $(m \to n)$ n'est pas universelle et donc $F(\forall v(m \to n)) = 0$ et comme F respecte les connecteurs logiques, $F(\varphi) = 1$.
     - si ni m ni n ne contiennent de quantificateurs, alors $m \to n$ est universelle donc $F(\forall v(m \to n)) = F(m \to n)$. De plus comme n est sans quantificateurs, $F(\forall v n) = F(n)$ et ainsi $F(\forall v(m \to n)) = F(m \to \forall v n) = F(m \to n)$ et donc $F(\varphi) = 1$.
   - Si φ est une règle de particularisation $\forall v m \to m_{t|v}$, remarquons d'abord que $F(m_{t|v}) = F(m)$ (induction facile sur les formules ; c'est vrai pour les formules atomiques par définition de F). Si m est universelle on a donc $F(\forall v m) = F(m) = F(m_{t|v})$ donc $F(\varphi) = 1$, et sinon $F(\forall v m) = 0$ donc on a également $F(\varphi) = 1$.
   - Enfin si φ est un axiome de l'égalité, φ est atomique donc $F(\varphi) = 1$

   Montrons enfin que si si $F(\varphi) = 1$ et $F(\varphi \to \psi) = 1$ alors $F(\psi) = 1$, ce qui achèvera la preuve comme expliqué plus haut. C'est une simple conséquence du fait que F respecte les connecteurs : ceci empêche $F(\psi) = 0$ d'après la table de vérité de l'implication.
2. Considérons la formule $\forall x \neg \forall y \neg (x = x)$. Comme $\neg \forall y \neg (x = x)$ n'est pas universelle, on a $F(\varphi) = 0$. Pourtant $\forall x \neg \forall y \neg (x = x)$ est une tautologie : en effet on a

$$\forall y \neg (x = x) \vdash \neg (x = x) \quad (1)$$
$$\vdash x = x \quad (2)$$
$$\vdash \bot, \quad (3)$$

   où (1) est obtenu par particularisation, (2) est un axiome est (3) provient de l'axiome logique $\varphi \to (\neg \varphi \to \bot)$ suivi d'un double modus ponens. Ainsi $\vdash \forall y \neg (x = x) \to \bot$, ce qui

d'après l'axiome logique $(\varphi \to \bot) \to \neg\varphi$ (principe de la preuve par contradiction) suivi d'un modus ponens donne $\vdash \neg\forall y\neg(x = x)$ et donc par généralisation $\forall x\neg\forall y\neg(x = x)$.

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

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

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

1. Donner une démonstration formelle du fait que l'addition soit commutative. On pourra commencer par prouver que $\mathrm{PA} \vdash \forall x(0 + x = x)$.
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.

Solution de l'exercice 3.

1. Comme indiqué, on va commencer par prouver que $\mathrm{PA} \vdash \forall x(0 + x = x)$. Pour ce faire, on va faire une preuve par récurrence, et il faut d'abord s'occuper de l'initialisation. [...]
2. Les axiomes sont

$$(A_{F,x}) \qquad \forall\bar{y}\left[(\forall x((\forall z < x F(z, \bar{y})) \to F(x, \bar{y}))) \to \forall x F(x, \bar{y})\right]$$

   On les prouve par une preuve formelle fastidieuse mais qui reprend les idées de la preuve usuelle dans $\mathbb{N}$.
3. Il suffit de prendre une ultrapuissance de $\mathbb{N}$ et de considérer la classe d'équivalence de la suite $(n)_{n\in\mathbb{N}}$.

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.