Master 1 Année 2012/2013

Logique pour l'Informatique Avancée

Feuille de TD n° 5

Exercice 1 — Soit $(\mathcal{G}, +)$ un groupe, c'est à dire que $\mathcal{G}$ est un ensemble muni d'une loi de composition interne $+$ vérifiant les propriétés suivantes :

Ass : $+$ est associative : $\forall a, b, c \in \mathcal{G}, (a + b) + c = a + (b + c)$.

Neu : $+$ admet un élément neutre $\mathbf{e}$ dans $\mathcal{G}$: $\forall a \in \mathcal{G}, a + \mathbf{e} = \mathbf{e} + a = a$.

Sym : chaque élément $a \in \mathcal{G}$ admet un symétrique $s(a)$ tel que : $a + s(a) = s(a) + a = \mathbf{e}$.

Formellement, on a la signature S suivante : $\mathcal{P}_S = \{=\}$, $\mathcal{F}_S = \{+, s\}$ et $\mathcal{C}_S = \{\mathbf{e}\}$. On interprètera l'égalité (et seulement celle-ci) de façon canonique. De plus, on écrira l'opérateur $+$ de façon infixé (c'est à dire que l'on écrira $a + b$ en lieu et place de $+(a, b)$). *Attention* : notez bien que $+$ n'est *pas* supposé commutatif ici !

On pourra utiliser les propriétés *Ass*, *Neu* et *Sym* aussi bien dans les hypothèses que dans les conséquences. Par ailleurs on s'autorisera de faire des étapes de calcul, c'est à dire, pour toute proposition P, la règle suivante :

$$\frac{\Gamma; P(x) = P(y) \vdash F}{\Gamma; x = y \vdash F}\, Calcul$$

Effectuer une preuve en déduction naturelle des propriétés suivantes :

1. Le symétrique à droite d'un élément quelconque de $\mathcal{G}$ est unique.
2. L'élément neutre à droite est unique.
3. Quel est le symétrique de $(x + y)$? En donner la preuve.
   Indication : on pourra utiliser la règle dérivé $\wedge i_g$ démontrée précédemment :

$$\frac{\Gamma; A; B \vdash F}{\Gamma; A \wedge B \vdash F}\, \wedge i_g$$

Exercice 2 — Arithmétique de Peano

Cette théorie est écrite sur le langage $\mathcal{L} = \{0, S, +, \times, =\}$, où S est la fonction unaire *successeur*. Formellement, on a la signature S suivante : $\mathcal{P}_S = \{=\}$, $\mathcal{F}_S = \{S, +, \times\}$ et $\mathcal{C}_S = \{0\}$. On interprètera l'égalité (et seulement celle-ci) de façon canonique. De plus, on écrira les opérateurs $+$ et $\times$ de façon infixé là encore. *Attention* : $+$ et $\times$ ne sont *pas* supposés commutatifs ici !
Soit P_0 l'ensemble des sept formules suivantes :

F1 : $\forall x, S(x) \neq 0$
F2 : $\forall x, x = 0 \vee (\exists y, x = S(y))$
F3 : $\forall x, \forall y, S(x) = S(y) \rightarrow x = y$
F4 : $\forall x, x + 0 = x$
F5 : $\forall x, \forall y, x + S(y) = S(x + y)$
F6 : $\forall x, x \times 0 = 0$
F7 : $\forall x, \forall y, x \times S(y) = x \times y + x$

De plus, à P_0 nous ajoutons la règle suivante, valable pour n'importe quel prédicat F :

$$\frac{\Gamma \vdash F(0) \qquad \Gamma \vdash \forall x, F(x) \rightarrow F(S(x))}{\Gamma \vdash \forall x, F(x)}\, Rec$$

La théorie $PA = P_0 \cup Rec$ est appelée *arithmétique de Peano*.

On pourra utiliser deux règles d'introduction et d'élimination de l'égalité :

$$\frac{}{\Gamma \vdash t = t} = i \qquad\qquad \frac{\Gamma \vdash A(t) \qquad \Gamma \vdash u = t}{\Gamma \vdash A(u)} = e$$

1. Démontrer que F2 est superflue (c'est à dire que $\vdash$ F2 sans utiliser la règle F2).
2. Démontrer que l'addition est associative (c'est à dire que $\vdash \forall x, \forall y, \forall z, (x+y)+z = x+(y+z)$).
3. Démontrer que l'addition est commutative (c'est à dire que $\vdash \forall x, \forall y, x + y = y + x$).
   Indication : commencer par démontrer que l'addition est commutative dans F4 et F5.
4. Démontrer les théorème T et T' et la règle dérivée $\exists i_g$ suivante (la règle $\wedge i_g$ pourra être utilisée) :

   $$T : \forall y, \forall x, ((x + y = x) \to (y = 0)); \qquad T' : \forall y, \forall x, (x + y = 0) \to ((x = 0) \wedge (y = 0));$$

   $$\frac{\Gamma; A; B \vdash F}{\Gamma; A \wedge B \vdash F} \wedge i_g; \qquad \frac{\Gamma; A(x_0) \vdash C \qquad x_0 \textit{ non libre ni dans } \Gamma \textit{ ni dans } C}{\Gamma; \exists x, A(x) \vdash C} \exists i_g.$$

5. Soit $x \leqslant y$ l'abréviation de la formule $\exists z, x + z = y$. Démontrez que :
   (a) $\cdot \leqslant \cdot$ est une relation d'ordre (réflexivité, antisymétrie et transitivité) ;
   (b) 0 est le plus petit élément ;
   (c) $\forall x, x \leqslant S(x)$.

Exercice 3 — *Propriété :* Il existe deux irrationnels x et y tels que x^y soit rationnel.
Preuve : Supposons que le nombre $\sqrt{2}^{\sqrt{2}}$ soit rationnel, alors prenons $x = y = \sqrt{2}$. Sinon, prenons $x = \sqrt{2}^{\sqrt{2}}$ et $y = \sqrt{2}$. *CQFD.*

La logique intuitionniste est une logique constructiviste. Ainsi, on ne veut pas seulement connaître l'existence d'une solution, on veut pouvoir la construire. Par conséquent la preuve de la propriété précédente n'est pas valide en logique intuitionniste. Par rapport aux règles vues en cours, une seule d'entre elle est modifiée afin de raisonner en logique intuitionniste. La règle *Abs* est remplacée par la règle *Abs int* suivante :

$$\frac{\Gamma \vdash_{int} \bot}{\Gamma \vdash_{int} F} \textit{ Abs int}$$

On admet qu'alors la règle *Abs* classique n'est alors *pas* démontrable. Démontrer que l'on ne peut pas prouver en logique intuitionniste : $\vdash_{int} \neg\neg F \to F$.

Exercice 4 — Dans la suite, la variable l sera toujours une *liste*. On considère les programmes fonctionnels suivants, en OCaml :

```
let rec foo x l =
        match l with
                | []    -> 0
                | t::q -> t + x * (bar x q) ;;

let rec bar a l =
        match l with
                | []    -> a
                | t::q -> bar (t::a) q ;;
```

Prouvez, par induction structurelle sur l, que :

1. si l $= [a_0; \ldots; a_n]$, alors foo x l renvoie la valeur de $P(l) = \sum_{k=0}^{n} a_k x^k$.
2. bar [] l renvoie la liste l, mais dans l'ordre inverse.