Licence STS, semestre 4 — 2010–2011
Mathématiques pour l'Informatique (Info 229) — 4 mai 2011
`http://www.lri.fr/~paulin/MathInfo`

TP 5 - Récapitulatif noté

Comme d'habitude on travaillera en remplissant le squelette fourni sur la page du cours. Le fichier sera rendu à la fin de la séance, par mail à l'encadrant de TP : `christine.paulin@lri.fr` ou `david.baelde@lri.fr`.

1 Logique propositionnelle

Exercice 1 *Parmi les énoncés suivants, deux ne sont pas valides. Prouvez les quatre autres :*

- $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow P \Rightarrow R$
- $((P \wedge Q) \Rightarrow R) \Rightarrow (P \Rightarrow Q \Rightarrow R)$
- $(P \vee Q) \Rightarrow (P \wedge Q)$
- $(P \vee Q) \Rightarrow (\neg P) \Rightarrow Q$
- $(P \Rightarrow Q) \Rightarrow R \Rightarrow (P \Rightarrow Q)$
- $(P \Rightarrow Q) \Rightarrow \neg(Q \Rightarrow P)$

2 Fonctions

Exercice 2 *On se donne un ensemble A :*

```
Variable A : Set.
```

Nous allons raisonner sur les fonctions de A dans lui-même. On introduit la notion de semi-inverse *: on dit que f est semi-inverse de f' si $f(f'(x)) = x$ pour tout $x \in A$.*

```
Definition semi_inverse (f : A->A) (f' : A->A) := forall x, f (f' x) = x.
```

Si f est semi-inverse de f' et f' est semi-inverse de f alors f et f' sont inverses l'une de l'autre au sens classique. Mais il se peut que f soit semi-inverse de f' sans pour autant être son inverse. Par exemple, avec $A = \mathbb{N}$:

$$f(x) = \begin{cases} 0 \text{ si } x = 0 \\ x - 1 \text{ sinon} \end{cases} \qquad f'(x) = x + 1$$

Nous allons étudier les propriétés entre semi-inverses, injectivité et surjectivité.

1. *Formaliser la définition de fonction injective, surjective :*

   ```
   Definition injective (f : A->A) := (* A vous de jouer *).
   Definition surjective (f : A->A) := (* A vous de jouer *).
   ```

2. *Montrer que si f est semi-inverse de f' alors elle est nécessairement surjective :*

   ```
   Theorem semi_inverse_surjective :
     forall f f', semi_inverse f f' -> surjective f.
   ```

3. *Montrer que si f est semi-inverse de f', et que f est injective alors f' est semi-inverse de f :*

```
Theorem semi_inverse_injective :
  forall f f', semi_inverse f f' -> injective f -> semi_inverse f' f.
```

bonus *On définit la composition de fonctions :*

```
Definition comp (f : A->A) (g : A->A) := fun x => f (g x).
```

Etant données f semi-inverse de f' et g semi-inverse de g', montrer que $f \circ g$ a aussi un semi-inverse :

```
Theorem semi_inverse_comp :
  forall f f' g g', semi_inverse f f' -> semi_inverse g g' ->
    exists h', semi_inverse (comp f g) h'.
```

3 Division euclidienne

Exercice 3 *L'algorithme de division euclidienne définit une fonction qui prend en entrée deux entiers n et p avec $p > 0$, et renvoie q et r tels que $n = p \times q + r$ et $r < p$. Nous allons montrer cela, en partant de la définition par clôture :*

$$\frac{n < p}{div(n, p, 0, n)} \qquad \frac{div(n, p, q, r)}{div(n + p, p, q + 1, r)}$$

1. *Formaliser les règles ci-dessus en une définition inductive :*

   ```
   Inductive div : nat -> nat -> nat -> nat -> Prop := ...
   ```

   Attention *: on prendra garde à écrire* `S q` *plutôt que* `q+1`.

2. *Prouver que le reste est plus petit que le diviseur :*

   ```
   Theorem r_correct : forall n q p r, div n p q r -> r < p.
   ```

   Indice *: c'est une preuve très simple quand on fait la bonne induction.*

3. *Prouver que la division est correcte :*

   ```
   Theorem q_correct : forall n p q r, div n p q r -> n = q * p + r.
   ```

   Aide *: Pour prouver les sous-buts arithmétiques simples, on pourra utiliser* `omega`*, éventuellement précédée d'une simplification calculatoire* `simpl`*. Finalement, l'utilisation de* `admit` *(tactique d'"abandon") sera tolérée pour les propriétés arithmétiques évidentes, si l'idée de la preuve est la bonne.*