Master 1 Informatique, Semestre 2 **Ingénierie de la preuve**
Université de Strasbourg 2009/2010

TP 3 - Définitions Inductives en Coq

1 Echauffement

On va implanter un type inductif permettant de représenter les jours de la semaine.
1- Proposer une structure de données pour ce type.
2- Programmer en `Coq` des fonctions `jour_suivant` et `jour_precedent`.
3- Prouver les propriétés suivantes :
- $\forall j$: `jour`, `jour_suivant` (`jour_precedent` j) $=$ j,
- $\forall j$: `jour`, `jour_precedent` (`jour_suivant` j) $=$ j.

2 Entiers de Gauss

On dispose dans `Coq` d'une théorie sur les entiers relatifs $\mathbb{Z}$. Concrètement cela veut dire que l'on dispose d'un type de données `Z` de sorte `Set`, de constantes 0 et 1 et des opérations habituelles : l'addition `Zplus : Z -> Z -> Z`, l'opposé `Zopp : Z -> Z`, la soustraction `Zminus : Z -> Z -> Z` et la multiplication `Zmult : Z -> Z -> Z`. On dispose d'une tactique `ring` permettant de démontrer automatiquement les égalités sur les expressions à valeurs entières. Par exemple la formule suivante

$$\forall a\ b\ c : Z, a * (b + c - d) = a * b - d * a + a * c$$

peut se démontrer grâce à la tactique `ring`.

Par ailleurs, on rappelle que les entiers de Gauss sont les nombres complexes de la forme $a + ib$ avec a et b des entiers relatifs.

1- Proposer une structure de données inductive `gauss` pour décrire les entiers de Gauss. Comment construire les valeurs 0 (noté $g0$), $g1$ et gi ?

2- Proposer des opérations d'addition, soustraction et multiplication sur les entiers de Gauss.

3- Comment procèder pour démontrer formellement en `Coq` que $\forall a$: `gauss`, $0 + a = a$?

4- Prouver en Coq l'associativité et la commutativité de l'addition pour les entiers de Gauss. On rappelle que les théorèmes établissant ces propriétés pour les entiers relatifs sont déjà disponibles dans `Coq` :

```
Zplus_comm : forall a b : Z, a+b = b+a.
Zplus_assoc : forall a b c : Z (a+b)+c = a+(b+c).
Zmult_comm : forall a b : Z, a*b = b*a.
```

5- Etudier comment démontrer toutes les propriétés d'anneau de l'ensemble des entiers de Gauss muni des opérations définies à la question 2.

3 Pour aller plus loin. . .

Reprendre les définitions faites dans la partie 1 et répondre aux questions suivantes :
1- Ecrire une fonction d'itération `iter` sur les entiers naturels `nat` et prouver la propriété suivante : $\forall j$: `jour`, `iter` 7 `jour_suivant` j $=$ j.
2- Prouver un théorème similaire avec `jour_precedent`.