TP 4 - Les opérateurs logiques « et » et « ou »

Mise à jour de l'aide-mémoire. *Comme vous pourrez le voir sur Arche, l'aide-mémoire a été mis-à-jour pour expliquer comment démontrer des énoncés de la forme suivante :*

$$P \text{ et } Q, \quad P \text{ ou } Q, \quad P \Leftrightarrow Q.$$

L'aide-mémoire explique aussi comment utiliser des hypothèses ayant cette forme. L'objectif de cette séance est d'apprendre à utiliser les différentes syntaxes LEAN que cela met en jeu, et à écrire des preuves correctes associées.

Remarque. *Dans tout ce TP, même si ce n'est pas toujours écrit, il sera attendu que vous écriviez les preuves* ***au papier*** *en même temps que vous effectuerez les démonstrations sur machine.*

1 L'opérateur logique « et »

On va commencer par démontrer l'affirmation suivante :

$$\forall x \in \mathbb{Z}, \quad x = 4 \Rightarrow (x^2 = 16 \text{ et } x + 10 = 14).$$

1. Ecrire l'énoncé d'un théorème `exemple_et` en LEAN décrivant l'affirmation précédente. *(On utilisera le symbole « ∧ » pour désigner le connecteur logique « et ». Tapez « \and » pour écrire ce symbole).*

Voici la réponse à la question 1 :

```
theorem exemple_et :
  ∀  x : Int, x = 4 → (x^2 = 16  ∧  x + 10 = 14) := by
{
    --Arguments de la preuve
}
```

2. A présent, écrivez les arguments de la preuve en vous servant de l'aide-mémoire, et écrivez la preuve au papier en parallèle. *(N'oubliez pas de vous demander à chaque étape de la preuve de quelle forme est l'objectif, et quel est l'encadré pertinent de l'aide-mémoire).*

3. Ecrire l'énoncé d'un théorème `exemple_et_2` affirmant la chose suivante :

$$\forall x, y \in \mathbb{Z}, (x = 4 \text{ et } y = 5) \Rightarrow x + y = 9.$$

Démontrer ensuite cet énoncé en écrivant la preuve au papier en parallèle.

4. Ecrire l'énoncé d'un théorème `exemple_et_3` affirmant la chose suivante :

$$\forall x, y \in \mathbb{Z}, (x = 3 \text{ et } \ y = 7) \Rightarrow (xy = 21 \text{ et } x^2 + y = 16)$$

Démontrer ensuite ce résultat.

2 L'opérateur logique « ou »

5. Ecrire, puis démontrer des théorèmes `exemple_ou_1` et `exemple_ou_2` pour démontrer les formules du premier ordre suivantes :

$$\forall x \in \mathbb{Z},\ x = 3 \Rightarrow (x + 1 = 10 \text{ ou } x - 1 = 2)$$

et

$$\forall x \in \mathbb{Z},\ x = 9 \Rightarrow (x + 1 = 10 \text{ ou } x - 1 = 2).$$

On utilisera le symbole « $\vee$ » pour désigner l'opérateur logique « ou ». Tapez « \or » pour écrire ce symbole.

La question précédente donnait un exemple de démonstration d'expression de la forme « P ou Q ». On va voir maintenant comment utiliser une « hypothèse » de la forme « P ou Q » : cela correspond à faire une disjonction de cas.

6. Ecrire, puis démontrer un théorème `exemple_ou_3` correspondant à la formule du premier ordre suivante :

$$\forall x \in \mathbb{Z}, (x = 2 \text{ ou } x = -2) \Rightarrow x^2 = 4.$$

7. Ecrire et démonstrer un théorème `exemple_ou_4` correspondant à la formule du premier ordre suivante :

$$\forall x \in \mathbb{Z}, (x = 3 \text{ ou } x = 5) \Rightarrow (x + 1 = 4 \text{ ou } x + 1 = 6).$$

Voyons à présent deux exemples utilisant à la fois des opérateurs « et » et « ou ».

8. Ecrire et démontrer des théorèmes `exemple_mixte_1` et `exemple_mixte_2` correspondant aux formules du premier ordre suivantes :

$$\forall x, y \in \mathbb{Z}, (x = 4 \text{ ou } x = 5) \text{ et } (y = 5) \Rightarrow (xy = 20 \text{ ou } x^2y = 125)$$

puis

$$\forall x, y \in \mathbb{Z}, (x = 4 \text{ et } y = 4) \text{ ou } (x = 5 \text{ et } y = 6) \Rightarrow y \geq x$$

(*Tapez « \geq » pour écrire le symbole* $\geq$*).*

3 Le connecteur logique « si et seulement si »

Commençons par donner un exemple ou l'on doit démontrer une affirmation de la forme « $P \Leftrightarrow Q$ ».

9. Ecrire et démontrer un théorème `exemple_ssi_1` correspondant à l'assertion suivante :

$$\forall x, y \in \mathbb{Z},\quad x = -y + 4 \ \Leftrightarrow\ x + y = 4.$$

En LEAN, le symbole $\Leftrightarrow$ sera retranscrit par le symbole « $\leftrightarrow$ », que vous pourrez tapez en écrivant « \iff » (« iff » signifie « if and only if », c'est-à-dire « si et seulement si »).

La question suivante donne une situation où l'on doit utiliser une hypothèse de la forme $P \Rightarrow Q$.

10. Ecrire et démontrer un théorème `exemple_ssi_2` correspondant à l'assertion suivante :

$$\forall x, y \in \mathbb{Z}, ((x = 3 \Leftrightarrow y = 4) \text{ et } x = 3) \Rightarrow y + 1 = 5$$

11. Ecrire et démontrer un théorème correspondant à l'assertion suivante :

$$\forall x, y \in \mathbb{Z}, (x = 3 \text{ et } x = y) \iff (y = 3 \text{ et } x = 3).$$

4 Retour sur les propriétés d'injectivité et de surjectivité des fonctions.

Rappelons que l'on peut formuler un prédicat affirmant qu'une fonction $f : \mathbb{Z} \to \mathbb{Z}$ est injective, de la façon suivante :

```
def est_injective (f : Int→Int) : Prop :=
    ∀ x y : Int, f x = f y →  x = y
```

Si `f` est une fonction de type `Int→Int`, alors l'expression « `est_injective f` » désigne en LEAN l'affirmation suivant laquelle f est injective.

12. *(Rappel).* Ecrire un prédicat `est_surjective` portant sur une fonction $f : \mathbb{Z} \to \mathbb{Z}$, affirmant que f est surjective.

On peut maintenant utiliser les mots `est_injective` *et* `est_surjective` *dans nos preuves. En guise d'entraînement, montrons que la fonction $g : x \in \mathbb{Z} \to x + 3 \in \mathbb{Z}$ est surjective.*

13. Définissez une fonction `g : Int → Int` qui prend $x \in \mathbb{Z}$, et qui renvoie $x + 3$. Une fois cela fait, écrivez le début de la preuve de la surjectivité de `g`, de la façon suivante :

```
theorem surjectivite_de_g :
    est_surjective g := by
{
    --Arguments de la preuve
}
```

Ecrivez à présent les arguments de la preuve. Vous aurez besoin de commencer par réécrire explicitement la définition de `est_surjective`, en écrivant :

```
rw[est_surjective]
```

Une fois cela fait, vous devriez pouvoir vous en sortir en appliquant les techniques que vous connaissez déjà.

14. *(Rappel)* Définissez une fonction prenant en entrée deux fonctions `f : Int→Int` et `g : Int→Int` et renvoyant en sortie la fonction composée $f \circ g$. *(Relisez le deuxième complément de cours si vous ne vous souvenez plus comment faire.)*

Ainsi, si `f : Int→Int` et `g : Int→Int` sont deux fonctions, l'expression « `composee f g` » désigne la composée $f \circ g$. De la même manière, l'expression « `est_surjective (composee f g)` » est l'affirmation suivant laquelle la composee $f \circ g$ est surjective.

On peut se servir de cela pour réénoncer l'un des théorèmes vus au TD précédent :

> **Théorème.** Soient $f, g : \mathbb{Z} \to \mathbb{Z}$ deux fonctions. Si f est surjective et si g est surjective alors $f \circ g$ est surjective.

La syntaxe pour cela est la suivante :

```
theorem composee_surjective :
    ∀ f g : Int→Int,
    (est_surjective f) ∧ (est_surjective g) → est_surjective (composee f g) := by
{
    --Arguments de la preuve
}
```

15. De la même manière, écrivez un enoncé correspondant à l'affirmation : « la composée de deux fonctions injectives est injective ».

16. Démontrez chacun de ces deux énoncés. Vous aurez besoin de réécrire explicitement les définitions de `est_injective`, `est_surjective` et `composee` en utilisant la commande `rw`, ou sa variante

```
rw[est_injective] at H
```

qui permet de réécrire la définition de `est_injective` dans une hypothèse `H` appartenant au contexte (bien sûr, il faut remplacer le nom « `H` » par celui qui apparaît dans votre cas).

17. Démontrez les deux énoncés suivants, en utilisant tout ce que vous avez vu jusqu'à présent :

Enoncé 1. Pour toute fonction $f : \mathbb{Z} \to \mathbb{Z}$, f est surjective si et seulement si $f \circ f$ est surjective.

Enoncé 2. Pour toute fonction $f : \mathbb{Z} \to \mathbb{Z}$, f est injective si et seulement si $f \circ f$ est injective.