TP 3 - Premières démonstrations

1 Objectif

Le but de cette séance de TP est de voir comment on peut utiliser LEAN *pour démontrer des énoncés du type suivant :*

(a) Pour toute fonction $f : \mathbb{Z} \to \mathbb{Z}$, si f est surjective, alors $f \circ f$ est surjective.

(b) Pour toutes fonctions $f, g : \mathbb{Z} \to \mathbb{Z}$, si $f \circ g$ est surjective, alors f est surjective ;

(c) Pour toutes fonctions $f, g : \mathbb{Z} \to \mathbb{Z}$ si f est surjective, et si g est surjective, alors $f \circ g$ est surjective.

(d) ...

Dans un premier temps, on va présenter une preuve complètement détaillée de la première assertion, écrite en LEAN *d'un côté, et en langage ordinaire de l'autre. On donnera aussi une version plus condensée, acceptable dans une rédaction écrite par un être humain.*

Vous devrez lire et comprendre cette rédaction pas-à-pas. Ensuite, ce sera à vous de faire votre propre rédaction pour d'autres énoncés.

2 Un exemple détaillé

Objectif. Montrer que pour toute fonction $f : \mathbb{Z} \to \mathbb{Z}$, si f est surjective, alors $f \circ f$ est surjective.

2.1 Questions introductives

1. Ecrire une formule du premier ordre représentant l'assertion à démontrer.

Voici la réponse à la question 1 : il s'agit de montrer la formule suivante :

$$\forall f : \mathbb{Z} \to \mathbb{Z}, \underbrace{(\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, f(x) = y)}_{f \text{ est surjective}} \Rightarrow \underbrace{(\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, f(f(x)) = y)}_{f \circ f \text{ est surjective}}$$

2. Ecrire le début de l'énoncé d'un théorème en LEAN démontrant la formule précédente. N'écrivez pas encore les arguments de la preuve.

Voici la réponse à la question 2 :

```
def composee_surjective :
  ∀  f : Int → Int,
  ( ∀ y : Int, ∃ x : Int, f x = y)  →  ( ∀ y : Int, ∃ x : Int, f (f x) = y) := by
{
    --Arguments de la preuve
}
```

Rappelez-vous : les retours à la ligne et les espaces n'ont pas d'importance, mais vous pouvez vous en servir pour structurer votre code.

2.2 Présentation de la preuve

On va maintenant présenter la preuve de l'énoncé ci-dessus. Vous trouverez le code LEAN complet ci-dessous, suivi de la rédaction en langage naturel.

Avant d'étudier la preuve.

0. Réfléchissez un instant à la façon dont vous feriez pour prouver cet énoncé.

*1. Munissez-vous de l'**aide-mémoire** disponible sur Arche.*

2. La démonstration est faite en plusieurs étapes. Tapez le code LEAN *étape par étape, et regardez l'objectif et le contexte s'actualiser au fur et à mesure.*

3. A chaque étape, posez vous les questions suivantes : de quel forme est l'objectif actuel ? (par ex. du type « $P \Rightarrow Q$ », du type « $\forall x \in E, P(x)$ », ou du type « $\exists x \in E, P(x)$ » ?)
Puis-je utiliser des hypothèses du contexte pour modifier le contexte ou ou bien modifier l'objectif ?

4. A chaque étape, **lisez en entier l'encadré concerné de l'aide-mémoire**, *et constatez que le code et la preuve suivent bien la rédaction indiquée.*

Voici maintenant la preuve de l'énoncé en question.

```
theorem composee_surjective :
  ∀  f : Int → Int,
  ( ∀ y : Int, ∃ x : Int, f x = y)  →  ( ∀ y : Int, ∃ x : Int, f (f x) = y) := by
{
    -- Etape 1
    intro f

    -- Etape 2
    intro H1

    -- Etape 3
    intro y

    -- Etape 4
    have H2 := H1 y

    -- Etape 5
    rcases  H2  with  ⟨x1, H3⟩
```

```
    -- Etape 6
    have  H4 := H1 x1

    -- Etape 7
    rcases  H4  with  ⟨x0, H5⟩

    -- Etape 8
    use x0

    -- Etape 9
    rw  [H5]

    -- Etape 10
    assumption
}
```

Ecriture de la démonstration. Voici à présent la démonstration écrite pas-à-pas.

1. Soit $f : \mathbb{Z} \to \mathbb{Z}$. Montrons que si f est surjective, alors $f \circ f$ est surjective.
2. Supposons que f est surjective, et notons `H1` cette hypothèse :

   $$\texttt{H1} : \quad \forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, f(x) = y.$$

   Montrons que $f \circ f$ est surjective.
3. Soit $y \in \mathbb{Z}$. Montrons qu'il existe $x \in \mathbb{Z}$ tel que $f(f(x)) = y$.
4. On applique l'hypothèse `H1` à y. On en déduit l'hypothèse `H2` :

   $$\texttt{H2} : \quad \exists x \in \mathbb{Z}, f(x) = y.$$

5. D'après l'hypothèse `H2`, il existe $x_1 \in \mathbb{Z}$ tel que $f(x_1) = y$. Notons `H3` cette hypothèse :

   $$\texttt{H3} \ : \quad f(x_1) = y.$$

6. On applique l'hypothèse `H1` à x_1. On en déduit l'hypothèse `H4` :

   $$\texttt{H4} : \quad \exists x \in \mathbb{Z}, f(x) = x_1.$$

7. D'après l'hypothèse `H4`, il existe $x_0 \in \mathbb{Z}$ tel que $f(x_0) = x_1$. Notons `H5` cette hypothèse :

   $$\texttt{H5} \ : \quad f(x_0) = x_1.$$

8. On doit montrer qu'il existe $x \in \mathbb{Z}$ tel que $f(f(x)) = y$. Montrons que $x = x_0$ convient, c'est-à-dire $f(f(x_0)) = y$.
9. D'après `H5`, on doit en fait montrer que $f(x_1) = y$.
10. Le résultat à montrer est donné par l'hypothèse `H3`. La preuve est terminée.

Version plus condensée. Dans une preuve écrite par un être humain, on s'autoriserait à fusionner certaines étapes pour aller un peu plus vite. On ne donnerait pas forcément non plus de nom à toutes les hypothèses. Par exemple :

Preuve. *Soit $f : \mathbb{Z} \to \mathbb{Z}$. Supposons que f est surjective, et montrons que $f \circ f$ est surjective.*

Soit $y \in \mathbb{Z}$. On va montrer qu'il existe $x \in \mathbb{Z}$ tel que $f(f(x)) = y$. Puisque f est surjective, il existe $x_1 \in \mathbb{Z}$ tel que $f(x_1) = y$. A nouveau, puisque $f : \mathbb{Z} \to \mathbb{Z}$ est surjective, il existe $x_0 \in \mathbb{Z}$ tel que $f(x_0) = x_1$. Posons $x = x_0$. On a alors

$$f(f(x)) = f(f(x_0)) = f(x_1) = y.$$

Ceci montre le résultat.

3. Arrivez-vous à identifier où sont passées chacune des étapes 1 à 10 dans la preuve ci-dessus ?

3 Résultats à démontrer par soi-même

Pour chacun des énoncés ci-dessous, suivez la démarche suivante :

0. Réfléchissez un moment à la façon dont vous feriez pour démontrer l'assertion en question.

1. Écrivez une formule du premier ordre représentant l'assertion à démontrer. *(Attention aux parenthèses !)*

2. Écrire le début de l'énoncé d'un théorème LEAN démontrant la formule précédente. N'écrivez pas encore les arguments de la preuve.

3. En vous servant de l'aide mémoire, écrivez pas-à-pas une preuve en LEAN de l'assertion. En parallèle, écrivez sur une feuille la preuve détaillée en langage naturel.

Énoncé 1. Pour toute fonction $f : \mathbb{N} \to \mathbb{Z}$ et pour toute fonction $g : \mathbb{Z} \to \mathbb{N}$, si f est surjective et si g est surjective, alors $f \circ g$ est surjective.

Énoncé 2. Pour toute fonction $f : \mathbb{N} \to \mathbb{Z}$ et pour toute fonction $g : \mathbb{Z} \to \mathbb{N}$, si f est injective et si g est injective, alors $f \circ g$ est injective.

Énoncé 3. Pour toute fonction $f : \mathbb{N} \to \mathbb{Z}$ et pour toute fonction $g : \mathbb{Z} \to \mathbb{N}$, si $f \circ g$ est surjective, alors f est surjective.

Énoncé 4. Pour toute fonction $f : \mathbb{N} \to \mathbb{Z}$ et pour toute fonction $g : \mathbb{Z} \to \mathbb{N}$, si $f \circ g$ est injective, et si g est surjective, alors f est injective.