# Preuves assistées par ordinateur

## CM 1 - Quelques rappels de logique

5 février 2025

# Formules du premier ordre

Tous les énoncés mathématiques (au moins vus au cours des premières années d'université) peuvent s'écrire au moyen de formules utilisant

1. les quantificateurs $\forall$, $\exists$ ;
2. un nombre fini de symboles (par ex. $+, \times, \pi$, etc.) ;
3. les opérateurs logiques (par ex. $\Rightarrow$, et, ou, non).

Les énoncés ont la plupart du temps une transcription en **langage naturel**.

## Exemples

1. *Si* $n, m \in \mathbb{N}$ *sont tels que* $mn$ *est pair, alors* $m$ *est pair ou* $n$ *est pair.*

$$\forall m, n \in \mathbb{N}, \quad (\exists k \in \mathbb{N}, mn = 2k) \Rightarrow \left[(\exists k \in \mathbb{N}, m = 2k) \text{ ou } (\exists k \in \mathbb{N}, n = 2k)\right]$$

2. *La fonction sinus n'est pas injective.*

$$\text{non } \left(\forall x, x' \in \mathbb{R}, (\sin(x) = \sin(x')) \Rightarrow (x = x').\right)$$

On appelle **formule du premier ordre** une formule transcrivant un énoncé mathématique au moyen des symboles ci-dessus.

# Objectifs

## Objectifs du cours dans son ensemble

**Partie mathématique :**

1. Être capable d'écrire correctement la formule du premier ordre associé à un énoncé en langage naturel.
2. Savoir écrire correctement les étapes de la démonstration d'un énoncé écrit avec une formule du premier ordre.

**Partie informatique :**

1. Savoir transcrire correctement un énoncé en logique du premier ordre dans l'assistant de preuve **LEAN** ;
2. Savoir transcrire correctement les étapes de la démonstration d'un énoncé en utilisant **LEAN** ; à l'inverse, utiliser **LEAN** comme guide pour écrire ces étapes correctement.

## Objectif de la séance

1. Comment construit-on un formule du premier ordre exactement ?
2. Comment rédige-t-on la preuve d'une telle formule ?

# I
# Construction de formules du premier ordre

A retenir : les quantificateurs $\forall, \exists$ et les opérateurs logiques $\Rightarrow, \mathrm{et}, \mathrm{ou}, \mathrm{non}$ permettent de construire des formules plus compliquées à partir de formules plus simples, en suivant des règles précises.

Expliquons ces règles.

# Opérateurs logiques **et**, **ou** et **non** et $\Rightarrow$

1. Si $P$ et $Q$ sont des formules représentant deux assertions mathématiques, alors on peut former trois nouvelles formules :

$$P \text{ ou } Q \quad (\text{aussi notée } P \vee Q)$$

$$P \text{ et } Q \quad (\text{aussi notée } P \wedge Q)$$

$$P \Rightarrow Q$$

2. Si $P$ est une formule représentant une assertion mathématique, alors on peut former la formule

$$\mathrm{non}(P) \quad (\text{aussi notée } \neg P)$$

# Quantificateurs $\forall$ et $\exists$

## Vocabulaire

On appelle **prédicat** sur un ensemble $E$ une formule $P(x)$ dépendant d'un élément variable $x \in E$, et désignant une propriété pouvant être satisfaite par des éléments de ensemble $E$.

## Exemples

1. La propriété « $n$ est pair », où $n \in \mathbb{N}$, qu'on pourra écrira :

$$P(n): \quad \exists m \in \mathbb{N}, n = 2 * m.$$

2. La propriété « $f$ est croissante », où $f$ est une fonction de $\mathbb{N}$ dans $\mathbb{N}$, qu'on pourra écrire :

$$P(f) \quad \forall n, m \in \mathbb{N}, n \leqslant m \Rightarrow f(n) \leqslant f(m).$$

# Quantificateurs $\forall$ et $\exists$ - suite

Soit $E$ un ensemble.

Si $P(x)$ est une formule représenant un prédicat sur un ensemble $E$, alors on peut former deux nouvelles formules :

1. $$\forall x \in E, P(x)$$

   (qui signifie « Pour tout $x \in E$, la propriété $P(x)$ est vraie »)

2. $$\exists x \in E, P(x)$$

   (qui signifie « Il existe $x \in E$ tel que la propriété $P(x)$ soit vraie »)

Attention, on ne doit pas écrire « tel que » dans les formules ci-dessus !

# Précisions

- Dans les formules du premier ordre, on peut utiliser divers **symboles mathématiques** (par ex. $\geqslant, \in, +, \cdot \ldots$), et parfois des mots représentants des **concepts mathématiques** (par ex. les adjectifs injective, surjective, etc.)

- Dans les expressions $\forall x \in E$, et $\exists x \in E$, le symbole $E$ doit représenter un **ensemble**.

  Les ensembles suivants seront utiles pour nous :

  1. ***Ensembles de nombres*** : $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C} \ldots$ ;
  2. ***Ensemble des parties*** : si $E$ est un ensemble, $\mathcal{P}(E)$ désigne l'ensemble des parties de $E$.
  3. ***Ensembles de fonctions*** : si $E, F$ sont des ensembles, $\mathcal{F}(E, F)$ désigne l'ensemble des fonctions de $E$ dans $F$.

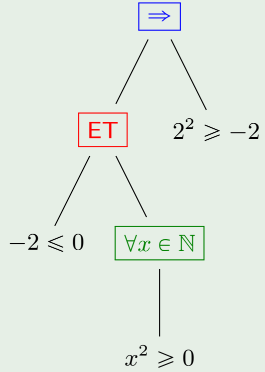
# Arbres représentant une formule

Une formule du premier ordre peut être représentée sous la forme d'un **arbre** qui détaille la manière dont elle est construite : c'est un diagramme ressemblant à celui-ci :

Pour la formule :

$$(-2 \leqslant 0) \text{ et } (\forall x \in \mathbb{N}, x^2 \geqslant 0) \quad \Rightarrow \quad 2^2 \geqslant -2$$

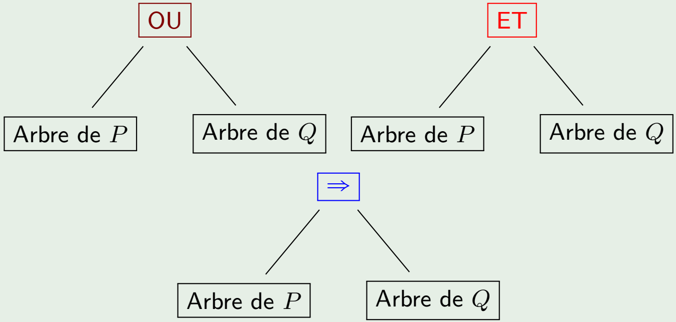
Arbre associé :



## Règles de construction de l'arbre

Construire l'arbre peut-être utile pour bien comprendre la structure de la formule.

- Si la formule est de la forme « $P$ ou $Q$ », « $P$ et $Q$ », « $P \Rightarrow Q$ » où $P$ et $Q$ sont des formules, on utilise les représentations suivantes :




Dans chacun des cas ci-dessus, il faut ensuite écrire explicitement les arbres de $P$ et $Q$, en utilisant les règles de construction.

# Règles de construction (suite)

- Si la formule est de la forme « Non$(P)$ », où $P$ est une formule, on utilise la représentation suivante :

$$\begin{array}{c}\boxed{\text{NON}}\\ | \\ \boxed{\text{Arbre de } P}\end{array}$$

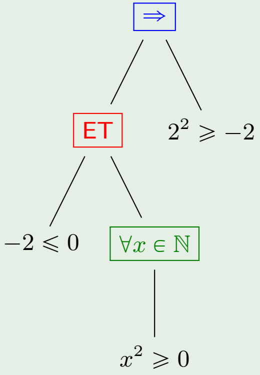
- Si la formule est de la forme « $\forall x \in E, P(x)$ » ou « $\exists x \in E, P(x)$ », où $P(x)$ est un prédicat sur $x$, on utilise les représentations suivantes :

$$\begin{array}{c}\boxed{\forall x \in E}\\ | \\ \boxed{\text{Arbre de } P(x)}\end{array} \qquad \begin{array}{c}\boxed{\exists x \in E}\\ | \\ \boxed{\text{Arbre de } P(x)}\end{array}$$

# Retour sur l'exemple

## Exemples

$$((-2 \leqslant 0) \text{ et } (\forall x \in \mathbb{N}, x^2 \geqslant 0)) \quad \Rightarrow \quad 2^2 \geqslant -2$$




Attention aux parenthèses !

# II
# Ecriture de démonstrations de formules du premier ordre

## Comment écrit-on la preuve d'une assertion donnée par une formule du premier ordre ?

Lorsqu'on essaie de démontrer une formule, on se donne :

- un **objectif** : c'est la formule à démontrer.
- un **contexte** : c'est l'ensemble formé par
  - les **objets déjà introduits** au moment de l'écriture de la preuve
    (par ex. les nombres $\pi, e$, les fonctions trigonométriques, les ensembles de nombres $\mathbb{N}$, $\mathbb{R}$ etc.)
  - les **théorèmes déjà connus** au moment de l'écriture de la preuve
    (par ex. les identités remarquables, le théorème de Thalès, le théorème de Pythagore, le théorème des valeurs intermédiaires, etc.)

Par exemple :

**Contexte**

Objets déjà introduits :

$\exp : \mathbb{R} \to \mathbb{R}_+^*$

$\pi \in \mathbb{R}$

$\ldots$

Théorèmes et assertions connues :

$\forall a, b \in \mathbb{R}, e^{a+b} = e^a e^b$

$e^0 = 1$

$\forall a, b \in \mathbb{R}, a \leqslant b \Rightarrow e^a \leqslant e^b$

$\ldots$

**Objectif**

$\forall x \in \mathbb{R}_+^*, \exists y \in \mathbb{R}, e^y = x$

**Pour démontrer un énoncé écrit sous la forme d'une formule du premier ordre, on modifie l'objectif et le contexte en écrivant la démonstration en parallèle, en suivant une procédure qu'on va détailler.**

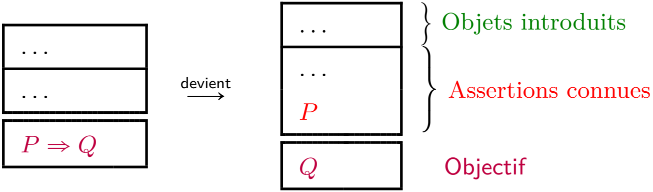
# Si l'objectif est de la forme...

1. $P \Rightarrow Q$ :

   1. On écrit « Supposons $P$. Montrons que $Q$ est vraie. » dans la démonstration.

   2. On ajoute « $P$ » dans les assertions connues.

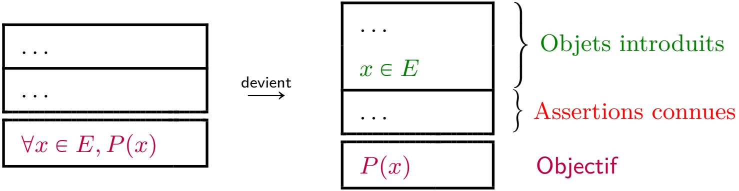
   3. On remplace l'objectif par $Q$.



# Si l'objectif est de la forme...

2. $\forall x \in E, P(x)$ :

1. On écrit « Soit $x \in E$. Montrons que $P(x)$ est vraie. » dans la démonstration.
2. On ajoute « $x \in E$ » dans les objets introduits.
3. On remplace l'objectif par $P(x)$.



# Si l'objectif est de la forme...

3. $\exists x \in E, P(x)$ :

   1. On écrit « Posons $x = < \mathrm{FORMULE} >$. Montrons que $x$ convient. » dans la démonstration. La formule doit être remplacée par une expression adéquate.
   2. On ajoute « $x \in E$ » dans les objets introduits.
   3. On ajoute l'hypothèse « $x = < \mathrm{FORMULE} >$ » dans les assertions connues.
   4. On remplace l'objectif par $P(x)$.

| |
|---|
| ... |
| ... |
| $\exists x \in E, P(x)$ |

$\xrightarrow{\text{devient}}$

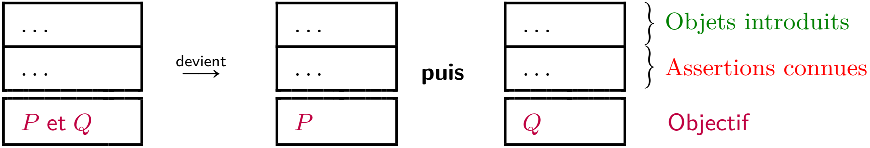
| | |
|---|---|
| ...<br>$x \in E$ | Objets introduits |
| ...<br>$x = $ <FORMULE> | Assertions connues |
| $P(x)$ | Objectif |

# Si l'objectif est de la forme...

4. $P$ et $Q$ :

   1. On écrit « Montrons que $P$ est vraie. », puis on écrit une preuve de $P$. Ensuite, on écrit : « Montrons que $Q$ est vraie. », puis on écrit une preuve de $Q$.

   2. L'objectif devient un objectif double : on remplace d'abord l'objectif par $P$ (puis on termine la preuve de $P$), **et ensuite** on remplace l'objectif par $Q$ (puis on termine la preuve de $Q$).

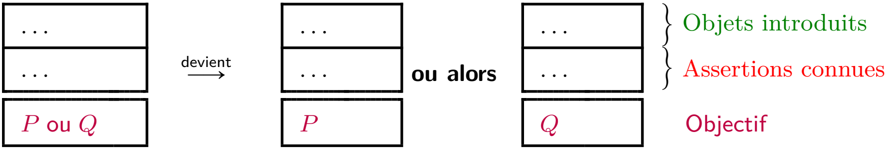


# Si l'objectif est de la forme...

4. $P$ ou $Q$ :

   1. **Suivant la situation** : On écrit « Montrons que $P$ est vraie. », puis on écrit une preuve de $P$. **ou alors**, on écrit : « Montrons que $Q$ est vraie. », puis on écrit une preuve de $Q$.

   2. **Suivant la situation**, on remplace l'objectif par $P$ (puis on termine la preuve de $P$), **ou bien** on remplace l'objectif par $Q$ (puis on termine la preuve de $Q$.




Ici, il y a un **choix à faire**, en fonction du contexte.

On verra plus tard en TP comment traiter le cas où l'objectif est de la forme $\mathrm{non}(P)$.

# Utiliser des hypothèses du contexte - quantificateur $\forall$

A n'importe quelle étape, il est possible de transformer le contexte en utilisant une des hypothèses.

4. Si dans le contexte, on a une hypothèse **H** de la forme $\forall x \in E, P(x)$, et un objet $a \in E$, alors on a le droit :

   1. d'écrire « On applique l'hypothèse **H** à $a$. On en déduit que $P(a)$ est vraie. ».
   2. d'ajouter ensuite « $P(a)$ » aux assertions connues.

| |
|---|
| $a \in E$ |
| ... |
| **H** : $\forall x \in E, P(x)$ |
| ... |
| $Q$ |

$\xrightarrow{\text{devient}}$

| | |
|---|---|
| $a \in E$ | Objets introduits |
| ... | |
| **H** : $\forall x \in E, P(x)$ | Assertions connues |
| ... | |
| $P(a)$ | |
| $Q$ | Objectif |

# Utiliser des hypothèses du contexte - quantificateur $\exists$

5. Si dans le contexte, on a une hypothèse **H** de la forme $\exists x \in E, P(x)$, alors on a le droit :

   1. d'écrire « D'après l'hypothèse **H**, il existe un élément $a \in E$ tel que $P(a)$ soit vrai. » dans la preuve.
   2. d'ajouter ensuite un élément $a \in E$ aux objets déjà introduits ;
   3. d'ajouter enfin l'hypothèse « $P(a)$ » aux assertions connues.

| |
|---|
| ... |
| **H** : $\exists x \in E, P(x)$<br>... |
| $Q$ |

$\xrightarrow{\text{devient}}$

| | |
|---|---|
| $a \in E$<br>... | Objets introduits |
| **H** : $\exists x \in E, P(x)$<br>...<br>$P(a)$ | Assertions connues |
| $Q$ | Objectif |

# Utiliser des hypothèses du contexte - implication $\Rightarrow$

5. Si dans le contexte, on a une hypothèse **H1** de la forme $P$ et une autre hypothèse **H2** de la forme $P \Rightarrow Q$, alors on a le droit :

   1. d'écrire « Puisque $P$ est vraie d'après **H1**, et puisque $P$ implique $Q$ d'après **H2**, alors $Q$ est vraie. » dans la preuve.
   2. d'ajouter l'hypothèse « $Q$ » aux assertions connues.

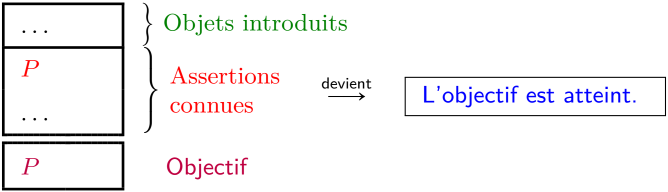
| |
|---|
| ... |
| **H1** : $P$ <br> **H2** : $P \Rightarrow Q$ <br> ... |
| ... |

$\xrightarrow{\text{devient}}$

| | |
|---|---|
| ... | Objets introduits |
| **H1** : $P$ <br> **H2** : $P \Rightarrow Q$ <br> **H** : $Q$ <br> ... | Assertions connues |
| ... | Objectif |

# Fin de la preuve

Si l'objectif $P$ est l'une des hypothèses du contexte, c'est gagné ! On écrit :
« L'assertion à prouver fait partie des hypothèses, donc celle-ci est démontrée. »




Attention, s'il y a plusieurs objectifs (par exemple si on a rencontré le connecteur logique **ET** dans la preuve), il faut démontrer chacun des sous-objectifs.

Il y a d'autres types de raisonnements (disjonction de cas, raisonnement par l'absurde...) que l'on verra au fur et à mesure des TPs.

# III
# Un exemple détaillé

## Exercice

On se donne une fonction $f : \mathbb{N} \to \mathbb{N}$. On suppose que $f$ est surjective. Montrer que si $f$ est surjective, alors $f \circ f$ est surjective.

La première partie de l'exercice consiste à écrire avec des quantificateurs l'assertion à démontrer. Ici, c'est :

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

Ensuite, on identifie le contexte et l'objectif à démontrer. Au départ, on a juste une fonction $f : \mathbb{N} \to \mathbb{N}$, et on ne suppose rien d'autre de connu.

| | |
|---|---|
| $f : \mathbb{N} \to \mathbb{N}$ | Objets |
| | Assertions |
| $(\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y) \Rightarrow (\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(f(x)) = y)$ | Objectif |

On peut maintenant écrire la preuve, étape par étape.

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| |

| |
|---|
| $(\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y)$ $\Rightarrow (\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(f(x)) = y)$ |

(couleurs : Objets introduits, Assertions connues, Objectif)

**Ecriture de la démonstration**

*(Vide pour le moment)*

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(f(x)) = y$ |

## Ecriture de la démonstration

1. Supposons que $f$ est surjective, et notons **H1** cette hypothèse :

   **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \rightarrow \mathbb{N}$ <br> $y_0 \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| $\exists x \in \mathbb{N}, f(f(x)) = y_0$ |

## Ecriture de la démonstration

1. Supposons que $f$ est surjective, et notons **H1** cette hypothèse :

   **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$

2. Soit $y_0 \in \mathbb{N}$. Montrons que : $\exists x \in \mathbb{N}, f(f(x)) = y_0$.

## Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| $\exists x \in \mathbb{N}, f(f(x)) = y_0$ |

### Ecriture de la démonstration

1. Supposons que $f$ est surjective, et notons **H1** cette hypothèse :

   $$\textbf{H1} : \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$$

2. Soit $y_0 \in \mathbb{N}$. Montrons que : $\exists x \in \mathbb{N}, f(x) = y$.
3. On applique l'hypothèse **H1** à $y$. On en déduit que la proposition suivante est vraie :

   $$\mathbf{H2} : \exists x \in \mathbb{N}, f(x) = y_0$$

## Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |

| |
|---|
| $\exists x \in \mathbb{N}, f(f(x)) = y_0$ |

### Ecriture de la démonstration

...

3. On applique l'hypothèse **H1** à $y$. On en déduit que la proposition suivante est vraie :

$$\mathbf{H2} : \exists x \in \mathbb{N}, f(x) = y_0$$

4. D'après **H2**, il existe $y_1 \in \mathbb{N}$ tel que

$$\mathbf{H3} : f(y_1) = y$$

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |

| |
|---|
| $\exists x \in \mathbb{N}, f(f(x)) = y_0$ |

## Ecriture de la démonstration

...

4. D'après **H2**, il existe $y_1 \in \mathbb{N}$ tel que
$$\mathbf{H3} : f(y_1) = y.$$
5. On applique l'hypothèse **H1** à $y_1$. On en déduit que la proposition suivante est vraie :
$$\mathbf{H4} : \exists x \in \mathbb{N}, f(x) = y_1$$

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| $y_2 \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |
| **H5** : $f(y_2) = y_1$ |

| |
|---|
| $\exists x \in \mathbb{N}, f(f(x)) = y_0$ |

## Ecriture de la démonstration

...

4. D'après **H2**, il existe $y_1 \in \mathbb{N}$ tel que

$$\mathbf{H3} : f(y_1) = y.$$

5. On applique l'hypothèse **H1** à $y_1$. On en déduit que la proposition suivante est vraie :

$$\mathbf{H4} : \exists x \in \mathbb{N}, f(x) = y_1$$

6. D'après **H4**, il existe $y_2 \in \mathbb{N}$ tel que

$$\mathbf{H5} : f(y_2) = y_1.$$

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| $y_2 \in \mathbb{N}$ |
| $x \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |
| **H5** : $f(y_2) = y_1$ |
| **H6** : $x = y_2$ |
| $f(f(x)) = y_0$ |

## Ecriture de la démonstration

...

6. D'après **H4**, il existe $y_2 \in \mathbb{N}$ tel que

$$\mathbf{H5} : f(y_2) = y_1.$$

7. Posons $x = y_2$, et montrons que $x$ convient, c-à-d $f(f(x)) = y_0$.

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| $y_2 \in \mathbb{N}$ |
| $x \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |
| **H5** : $f(y_2) = y_1$ |
| **H6** : $x = y_2$ |

| |
|---|
| $f(f(y_2)) = y$ |

## Ecriture de la démonstration

...

7. Posons $x = y_2$, et montrons que $x$ convient, c-à-d $f(f(x)) = y_0$. Notons **H6** l'hypothèse $x = y_2$.
8. D'après **H6**, on peut remplacer $x$ par $y_2$ dans la formule à démontrer.

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| $y_2 \in \mathbb{N}$ |
| $x \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |
| **H5** : $f(y_2) = y_1$ |
| **H6** : $x = y_2$ |

| |
|---|
| $f(y_1) = y$ |

## Ecriture de la démonstration

...

7. Posons $x = y_2$, et montrons que $x$ convient, c-à-d $f(f(x)) = y_0$. Notons **H6** l'hypothèse $x = y_2$.
8. D'après **H6**, on peut remplacer $x$ par $y_2$ dans la formule à démontrer.
9. D'après **H5**, on peut remplacer $f(y_2)$ par $y_1$ dans la formule à démontrer.

# Ecriture de la preuve

| |
|---|
| $f : \mathbb{N} \to \mathbb{N}$ |
| $y_0 \in \mathbb{N}$ |
| $y_1 \in \mathbb{N}$ |
| $y_2 \in \mathbb{N}$ |
| $x \in \mathbb{N}$ |
| **H1** : $\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$ |
| **H2** : $\exists x \in \mathbb{N}, f(x) = y_0$ |
| **H3** : $f(y_1) = y$ |
| **H4** : $\exists x \in \mathbb{N}, f(x) = y_1$ |
| **H5** : $f(y_2) = y_1$ |
| **H6** : $x = y_2$ |
| $f(y_1) = y$ |

## Ecriture de la démonstration

...

7. Posons $x = y_2$, et montrons que $x$ convient, c-à-d $f(f(x)) = y_0$. Notons **H6** l'hypothèse $x = y_2$.
8. D'après **H6**, on peut remplacer $x$ par $y_2$ dans la formule à démontrer.
9. D'après **H5**, on peut remplacer $f(y_2)$ par $y_1$ dans la formule à démontrer.
10. Il faut montrer que $f(y_1) = y_0$, ce qui est exactement l'hypothèse **H3**. La preuve est terminée.

# Preuve complète

1. Supposons que $f$ est surjective, et notons **H1** cette hypothèse :
$$\mathbf{H1}: \ \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, f(x) = y$$
2. Soit $y_0 \in \mathbb{N}$. Montrons que : $\exists x \in \mathbb{N}, f(f(x)) = y_0$.
3. On applique l'hypothèse **H1** à $y$. On en déduit que la proposition suivante est vraie :
$$\mathbf{H2} : \exists x \in \mathbb{N}, f(x) = y_0$$
4. D'après **H2**, il existe $y_1 \in \mathbb{N}$ tel que
$$\mathbf{H3} : f(y_1) = y.$$
5. On applique l'hypothèse **H1** à $y_1$. On en déduit que la proposition suivante est vraie :
$$\mathbf{H4} : \exists x \in \mathbb{N}, f(x) = y_1$$
6. D'après **H4**, il existe $y_2 \in \mathbb{N}$ tel que
$$\mathbf{H5} : f(y_2) = y_1.$$
7. Posons $x = y_2$, et montrons que $x$ convient, c-à-d $f(f(x)) = y_0$.
8. D'après **H6**, on peut remplacer $x$ par $y_2$ dans la formule à démontrer. Notons **H6** l'hypothèse $x = y_2$.
9. D'après **H5**, on peut remplacer $f(y_2)$ par $y_1$ dans la formule à démontrer.
10. Il faut montrer que $f(y_1) = y_0$, ce qui est exactement l'hypothèse **H3**. La preuve est terminée.

# Utilisation de LEAN

LEAN est un outil informatique qui permet de réaliser pas-à-pas le travail précédent :

1. on annonce à la machine quelle étape élementaire de raisonnement on souhaite faire en tapant une certaine commande ;
2. on voit le **contexte** et l'**objectif** s'actualiser au fur et à mesure.

LEAN

```
variable (f : Nat → Nat)

theorem composee_surjective :
  (∀ y : Nat, ∃ x : Nat, f x = y) → (forall y : Nat, ∃ x : Nat, f (f x) = y) :=
  by
  {
    intro H1
    intro y

  }

```

```
▾ mathlib-demo.lean:9:4
▾ Tactic state
1 goal
f : Nat → Nat
H1 : ∀ (y : Nat), ∃ x, f x = y
y : Nat
⊢ ∃ x, f (f x) = y
▸ All Messages (1)
```

Exemple d'affichage en LEAN - Début de la preuve

```
variable (f : Nat → Nat)

theorem composee_surjective :
  (∀ y : Nat, ∃ x : Nat, f x = y) → (forall y : Nat, ∃ x : Nat, f (f x) = y) :=
  by
  {
    intro H1
    intro y
    have H2 := H1 y
    rcases H2 with ⟨ y1, H3 ⟩
    have H4 := H1 y1
    rcases H4 with ⟨ y2, H5 ⟩
    let x := y2
    have H6 : (x = y2) := by rfl
    exists x
    rw [H6]
    rw [H5]
    exact H3
  }
```

▾ mathlib-demo.lean:20:0
▾ Tactic state
No goals
▾ All Messages (0)
No messages.

Exemple de démonstration en LEAN - Preuve complète