Aujourd'hui nous allons discuter :

- Modèle de preuve : Comment montrer $\forall u \ p(u)$?
- Notation $\sum_{n=4}^{23} f(n)$, $\prod_{n=4}^{23} f(n)$, $\vee_{n=4}^{23} p(n)$, etc.
- Modèle de preuve $\forall n \in \mathbb{N} \ p(n)$ par Modus Ponens Répété
- Principe d'induction simple

Rappel d'hier

Proposition

Supposons $p(u)$ et $q(u)$ sur le même univers de discours U.

$$\begin{aligned} (\forall u\ p(u)) \vee (\forall u\ q(u)) &\Rightarrow (\forall u\ (p(u) \vee q(u))) \\ (\exists u\ (p(u) \wedge q(u))) &\Rightarrow (\exists u\ p(u)) \wedge (\exists u\ q(u)) \end{aligned}$$

mais mème

$$\begin{aligned} (\forall u\ p(u)) \wedge (\forall u\ q(u)) &\Leftrightarrow (\forall u\ (p(u) \wedge q(u))) \\ (\exists u\ (p(u) \vee q(u))) &\Leftrightarrow (\exists u\ p(u)) \vee (\exists u\ q(u)) \end{aligned}$$

Preuve de $(\forall u\ p(u)) \vee (\forall u\ q(u))) \Rightarrow (\forall u\ (p(u) \vee q(u)))$ par une preuve directe.

• Si l'hypothèse est fausse, il n'y a rien à faire : l'implication est vraie.

• Supposons l'hypothèse est vraie. C.-à-d.
(i) $p(u)$ est vraie pour chaque $u \in U$ ou
(ii) $q(u)$ est vraie pour chaque $u \in U$.
Si (i) est vraie alors $p(u)$ est vraie pour chaque $u \in U$, et donc aussi $p(u) \vee q(u)$ est vraie pour chaque $u \in U$.
Si (ii) est vraie alors $q(u)$ est vraie pour chaque $u \in U$, et donc aussi $p(u) \vee q(u)$ est vraie pour chaque $u \in U$.
Si (i) ou (ii) est vraie, alors aussi $(\forall u\ (p(u) \vee q(u)))$.

• Ainsi on a montré l'implication. $\square$

Preuve de $(\exists u\ (p(u) \vee q(u))) \Leftrightarrow (\exists u\ p(u)) \vee (\exists u\ q(u))$.

• Supposons que $(\exists u\ (p(u) \vee q(u)))$ est vraie, c.-à-d, il existe un élément de U, disons $u_0 \in U$, tel que $(p(u_0) \vee q(u_0)))$ est vraie, alors $p(u_0)$ ou $q(u_0))$ est vraie. Donc $(\exists u\ p(u))$ ou $(\exists u\ q(u))$ est vraie. Donc on a montré

$(\exists u\ (p(u) \vee q(u))) \Rightarrow (\exists u\ p(u)) \vee (\exists u\ q(u))$.

• Inversement, supposons que $(\exists u\ p(u)) \vee (\exists u\ q(u))$ est vraie.

Si $(\exists u\ p(u))$ est vraie, il y a un $u_0 \in U$ tel que $p(u_0)$ est vraie, donc $(p(u_0) \vee q(u_0)))$ est vraie et $(\exists u\ (p(u) \vee q(u)))$ aussi.

Si $(\exists u\ q(u))$ est vraie, il y a un $u_0 \in U$ tel que $q(u_0)$ est vraie, donc $(p(u_0) \vee q(u_0)))$ est vraie et $(\exists u\ (p(u) \vee q(u)))$ aussi.

On a montré $(\exists u\ (p(u) \vee q(u))) \Rightarrow (\exists u\ (p(u) \vee q(u)))$

• Ça complète la preuve. $\square$

(Nous laissons les deux autres propositions comme exercices.)

On avait une autre situation qui demandait un peu d'attention.

Proposition

Soit $p(u,v)$ une fonction propositionnelle avec univers du discours $U \times V$ non-vide.
(i) On a seulement :

$$(\exists v\ \forall u\ p(u,v)) \Rightarrow (\forall u\ \exists v\ p(u,v))$$

(ii) Mais

$$\begin{aligned}(\forall u\ \forall v\ p(u,v)) &\Leftrightarrow (\forall v\ \forall u\ p(u,v))\\ (\exists u\ \exists v\ p(u,v)) &\Leftrightarrow (\exists v\ \exists u\ p(u,v))\end{aligned}$$

(i)

$$(\exists v \ \forall u \ p(u,v)) \Rightarrow (\forall u \ \exists v \ p(u,v))$$

Démonstration.

Par une preuve directe.

• Si l'hypothèse est fausse, il n'y a rien à faire : l'implication serait vraie.

• Supposons $(\exists v \ \forall u \ p(u,v))$ est vraie, c.-à-d., il existe un élément de V, disons $v_0 \in V$, tel que $p(u, v_0)$ est vraie pour chaque $u \in U$.
Est-ce que $(\forall u \ \exists v \ p(u,v))$ serait vraie aussi ?
Soit $u \in U$, est-ce qu'il existe un $v \in V$ (qui dépend possiblement de u) tel que $p(u,v)$ est vraie ? Oui, prend v_0 !
Alors $(\forall u \ \exists v \ p(u,v))$ serait vraie aussi.

• On a ainsi montré l'implication. □

$$
\begin{aligned}
(\forall u\ \forall v\ \ p(u,v)) &\iff (\forall v\ \forall u\ \ p(u,v))\\
(\exists u\ \exists v\ \ p(u,v)) &\iff (\exists v\ \exists u\ \ p(u,v))
\end{aligned}
$$

Démonstration.

(ii) $(\forall u\ \forall v\ \ p(u,v))$ veut dire pour chaque u et pour chaque v on a $p(u,v)$. Mais parce que $u \wedge v \Leftrightarrow v \wedge u$, c'est la même chose comme dire pour chaque v et pour chaque u on a $p(u,v)$, c.-à-d., $(\forall v\ \forall u\ \ p(u,v))$

(iii) Similairement pour l'autre équivalence : exercice. $\square$

Modèles de preuve de $\forall u \ p(u)$?

Soit $p(u)$ une fonction propositionnelle avec univers de discours U. Est-ce qu'il y a une modèle de preuve pour montrer

$$P := "\forall u \ p(u)" \ ?$$

Beaucoup d'énoncés en mathématiques sont de cette form.

Il n'y a pas une seule stratégie qui marche toujours.

• Une stratégie déjà employée est de montrer qu'un contre-exemple n'existe pas (une preuve par contradiction).

• Une preuve directe typique serait :

" Soit $u \in U$ arbitraire. Avec l'information que u est dans l'ensemble U et des théorèmes déjà montrés on montre directement que $p(u)$ est vraie."

Donc la seule hypothèse est que $u \in U$, mais quand même c'est une information importante (la seule....).

Un exemple suit.

Proposition

Pour chaque nombre naturel $n \geq 0$ *on a*

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Préparation. Posons $P(n) :=$ "$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$" ;
c'est une fonction propositionnelle avec univers de discours $\mathbb{N}$.
Il faut montrer que $\forall n \; P(n)$ est vraie.

Preuve directe : Soit n un nombre naturel arbitraire.
Posons $s(n) = 0 + 1 + 2 + 3 + \ldots + n$, pour $n \in \mathbb{N}$. Alors

$$\begin{aligned}
2s(n) &= (1 + 2 + 3 + \ldots + n) + (1 + 2 + 3 + \ldots + n) \\
&= (1 + 2 + 3 + \ldots + n) + (n + (n-1) + (n-2) + \ldots + 2 + 1) \\
&= (1 + n) + (2 + (n-1)) + (3 + (n-2)) + \ldots + (n+1) \\
&= n(n+1)
\end{aligned}$$

Et $2s(n) = n(n+1)$ implique que $s(n) = \frac{n(n+1)}{2}$.
Donc pour chaque $n \in \mathbb{N}$ la formule est vraie. $\square$

Notation

Nous introduisons de la notation utile :

Soit $f : \mathbb{N} \to \mathbb{R}$ une fonction.
On définit :
$\sum_{i=0}^{n} f(i) = f(0) + f(1) + f(2) + \ldots + f(n)$.
Exemple : $\sum_{i=0}^{n} i = 0 + 1 + 2 + \ldots + n$.
Et
$\prod_{i=0}^{n} f(i) = f(0) \cdot f(1) \cdot f(2) \cdots f(n)$.

Variations :
$\sum_{i=3}^{8} f(i) = f(3) + f(4) + f(5) + f(6) + f(7) + f(8)$.
$\prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdots n = n!$

Soit A un ensemble, avec ensemble des parties $P(A)$.
Soit $S : \mathbb{N} \to P(A)$ une fonction ; en particulier, $S(i) \subseteq A$ pour chaque i

$$\cup_{i=0}^{n} S(i) = S(0) \cup S(1) \cup S(2) \cup \ldots \cup S(n)$$

$$\cap_{i=3}^{8} S(i) = S(3) \cap S(4) \cap S(5) \cap S(6) \cap S(7) \cap S(8).$$

Si $p(n)$ est une fonction propositionnelle avec univers de discours $\mathbb{N}$:

$$\vee_{i=3}^{8} p(i) = ...?$$

$$\wedge_{i=0}^{7} p(i) = ...?$$

Mais nous n'utiliseront pas dans ce cours les versions avec ∞

$$\vee_{i=0}^{\infty} p(i) = ...$$

(Mais ça fait du sense quand-même !)

• Les preuves-cas-par-cas suggère une autre méthode (pour montrer $P =$ "$\forall u \; p(u)$") :

Idée : Briser U en des plus petits morceaux convenables.

Supposons $U = U_1 \cup U_2 \cup \ldots \cup U_n$, où $n \geq 1$. Alors

$$[\forall u \in U \; p(u)] \Leftrightarrow [\forall u \in U_1 \; p(u)] \wedge [\forall u \in U_2 \; p(u)] \wedge \ldots \wedge [\forall u \in U_n \; p(u)]$$

Si $u \in U_i$ et pas seulement que $u \in U$, ça donne plus d'informations sur u, qu'on pourrait utiliser pour une preuve cas-par-cas ! !

Revisitons l'exemple :

$$P := \forall\ n \in \mathbb{Z}\ \left[\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right].$$

Preuve : Posons
$U_1 := \{n \in \mathbb{Z} |\ \exists m \in \mathbb{Z}\ n = 3m\}$,
$U_2 := \{n \in \mathbb{Z} |\ \exists m \in \mathbb{Z}\ n = 3m + 1\}$,
$U_3 := \{n \in \mathbb{Z} |\ \exists m \in \mathbb{Z}\ n = 3m + 2\}$.
On a $\mathbb{Z} = U_1 \cup U_2 \cup U_3$.
Preuve morceau-par-morceau :

• $\forall n \in U_1 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$.

Preuve : Soit $n \in U_1$. Par définition il existe un entier m tel que $n = 3m$. Substitution : $\frac{n(n+1)(n+5)}{3} = \frac{3m(3m+1)(3m+5)}{3} = m(3m+1)(3m+5) \in \mathbb{Z}$. En effet. $\square$

- $\forall n \in U_2 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$.

Preuve : Soit $n \in U_2$. Par définition il existe un entier m tel que $n = 3m + 1$. Substitution :
$\frac{n(n+1)(n+5)}{3} = \frac{(3m+1)(3m+2)(3m+6)}{3} = (3m+1)(3m+2)(m+2) \in \mathbb{Z}$.
En effet. $\square$

- $\forall n \in U_3 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$.

Preuve : Soit $n \in U_1$. Par définition il existe un entier m tel que $n = 3m + 2$. Substitution :
$\frac{n(n+1)(n+5)}{3} = \frac{3m+2(3m+3)(3m+7)}{3} = (3m+2)(m+1)(3m+7) \in \mathbb{Z}$.
En effet. $\square$

Parce que

$$\forall\ n \in \mathbb{Z}\ \left[\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}.\right]$$

si et seulement si

$\forall n \in U_1 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$ et
$\forall n \in U_2 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$ et
$\forall n \in U_3 : \left(\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}\right)$
il suit que $P = \forall\ n \in \mathbb{Z}\ \left[\frac{n(n+1)(n+5)}{3} \in \mathbb{Z}.\right]$ est vrai aussi.

$\square$

Modus ponens répété un nombre fini de fois.

• Si on veut montrer $\forall n\ p(n)$ si l'univers de discours est $\mathbb{N}$ il y a une méthode spéciale !

Celle d'induction mathématiques, ou "Modus Ponens Généralisé".

Soit $p(n)$ une fonction propositionnelle avec univers de discours $U = \{0, 1, 2, \dots, 7\}$.

- Supposons $p(0)$ est vraie et
- $p(n) \to p(n+1)$ vraie pour chaque $0 \leq n < 7$.

Alors $\forall n\ p(n)$ est vraie.

Preuve : Hypothèses : $p(0)$ est vraie et aussi sont $p(0) \to p(1)$,

$p(1) \to p(2)$, $p(2) \to p(3)$, $p(3) \to p(4)$, $p(4) \to p(5)$,
$p(5) \to p(6)$, $p(6) \to p(7)$.

$p(0)$ et aussi $p(0) \to p(1)$ vraies, donc $p(1)$ (par modus ponens).
$p(1)$ et aussi $p(1) \to p(2)$ vraies, donc $p(2)$ (par modus ponens).
Mais aussi $p(2) \to p(3)$ donc $p(3)$ (modus ponens).
Mais aussi $p(3) \to p(4)$ donc $p(4)$ (modus ponens).
Mais aussi $p(4) \to p(5)$ donc $p(5)$ (modus ponens).
Mais aussi $p(5) \to p(6)$ donc $p(6)$ (modus ponens).
Mais aussi $p(6) \to p(7)$ donc $p(7)$ (modus ponens).

Conclusion : $p(0), p(1), \ldots, p(7)$ sont tous vraies. $\square$

Montrer par Modus-Ponens-Répété que pour chaque $n \leq 10000^{1000}$ on a l'identité :

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

- Préparation : Posons la proposition logique

$$p(n) := "0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}".$$

avec univers de discours

$$U := \{n \in \mathbb{N} |\ 0 \leq n \leq 10000^{1000}\}$$

Il faut montrer $\forall n\ p(n)$.

- Début : Alors $p(0) =$ "$0 = \frac{0(0+1)}{2}$", ce qui est vraie.
- Montrons pour chaque $0 \leq m < 10000^{1000}$ que $[p(m) \to p(m+1)]$ par une preuve directe.

Preuve : Fixons un nombre entier m tel que $0 \leq m < 10000^{1000}$ arbitrairement.

Si l'hypothèse $p(m)$ est fausse, il n'y a rien à faire. L'implication $p(m) \to p(m+1)$ serait vraie.

Supposons l'hypothèse $p(m)$ vraie, c.-à-d.

$$0 + 1 + 2 + 3 + \ldots + m = \frac{m(m+1)}{2}.$$

En ajoutant $m+1$ aux deux côtés, on obtient l'identité

$$0+1+2+3+\ldots+m+(m+1) = \frac{m(m+1)}{2} + (m+1) = \frac{(m+1)(m+2)}{2}.$$

Alors $p(m+1)$ serait vrai aussi.

Nous avons montré que $p(m) \to p(m+1)$ est vrai (sans savoir si $p(m)$ est vraie).

Donc $p(0)$ est vraie, et pour chaque $n \in \mathbb{N}$ tel que $n < 10000^{1000}$ on a montré que $p(n) \to p(n+1)$ est vraie.

• Conclusion : Par Modus Ponens Répéte par un nombre fini (mais beaucoup) de cas, on conclut

$$p(0), p(1), p(2), p(3), \dots p(10000^{1000})$$

sont toutes vraies, ainsi

$$\forall n \in U \;\; p(n)$$

est vrai. $\square$

Dans notre situation, il n'y a pas de raison d'arrêter à 10000^{1000} !
On peut remplacer par n'importe quel nombre entier !

Et modus ponens répété un nombre infini de fois ?

L'hypothèse que $\mathbb{N}$ existe, avec ses propriétés élémentaires, implique la tautologie suivante extrêmement importante.

Principe d'induction

Soit $p(n)$ une fonction propositionnelle avec univers du discours $\mathbb{N}$.

$$[p(0) \wedge [\forall n \ (p(n) \rightarrow p(n+1)]] \Leftrightarrow [\forall n \ p(n)]$$

La partie $\Leftarrow$ est évidente. Mais pas $\Rightarrow$, car ça dépend des propriétés de $\mathbb{N}$, une théorie à développer encore.

Acceptons ce principe, pour le moment. Ça donne une stratégie pour montrer $[\forall n \ p(n)]$, si l'univers du discours est $\mathbb{N}$! !

La différence avec une preuve directe de $[\forall n \; p(n)]$?

Dans une preuve directe on montre $p(n)$ directement, sans autre hypothèse que $n \in \mathbb{N}$.

Dans une preuve par induction on montre le cas spécial $p(0)$ et puis on suppose que $n \geq 0$ et que $p(n)$ vraie pour montrer que $p(n+1)$ serait vrai aussi. L'hypothèse est plus généreuse, donc c'est plus facile de montrer $p(n)$ (sous ses hypothèses).

Le principe d'induction est vraiment très, très souvent utilisé dans les preuves (et définitions !) en mathématiques.

Proposition

Pour chaque nombre naturel $n \geq 0$ on a

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Nous avons déjà une preuve directe. Maintenant une preuve par induction.

Preuve par induction.

• Préparation : Posons $s(n) = \sum_{i=0}^{n} i$. Il faut montrer que $p(n) :=$ "$s(n) = \frac{n(n+1)}{2}$" est vraie pour chaque $n \in \mathbb{N}$.

• Début : Au moins $p(0) =$ "$0 = \frac{0(0+1)}{2}$" est vraie (car les deux côtés sont 0).

• Étape d'induction : Soit $n \in N$ et supposons $p(n)$ vraie, c.-à-d., $0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

En ajoutant $(n+1)$ aux deux côtés on obtient :

$$\begin{aligned} 0 + 1 + 2 + \ldots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2} \\ &= \frac{[n+1]([n+1]+1)}{2} \end{aligned}$$

(suite)

Nous avons montré que si $p(n)$ vraie, alors aussi $p(n+1)$ vraie, alors nous avons montré l'étape d'induction que l'implication $p(n) \rightarrow p(n+1)$ est vraie, et ça pour chaque $n \in \mathbb{N}$.

• Conclusion : Nous avons montré que $p(0)$ vraie et que pour chaque $n \in \mathbb{N}$: $p(n) \rightarrow p(n+1)$ est vraie. Donc, par le principe d'induction, on conclut la preuve de la proposition par induction. $\square$

Lemme

Pour chaque nombre naturel n on a

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Preuve directe : ? ? ?

Preuve par induction est plus facile :

• Préparation : Posons
$p(n) :=$ " $\left(0^2 + 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}\right)$ ". Il faut montrer $\forall n\ p(n)$.

• Début : $p(0) =$ "$0^2 = \frac{0(0+1)(2\cdot 0+1)}{6}$" est vraie (les deux côtés donnent 0).
$p(1) =$ "$0^2 + 1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$" est vraie aussi (les deux côtés donnent 1) (cette étape n'est pas nécessaire, mais donne confiance).

• Étape d'induction : Soit $n \geq 0$ arbitraire. Supposons $p(n)$ est vraie, c.-a-d. $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
Alors en ajoutant $(n+1)^2$ des deux côtés :

$$\begin{aligned}
1^2 + 2^2 + \ldots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= (n+1) \cdot \left(\frac{n(2n+1)}{6} + \frac{6n+6}{6} \right) \\
&= (n+1) \cdot \left(\frac{2n^2 + 7n + 6)}{6} \right) \\
&= \left(\frac{[n+1]([n+1]+1)(2[n+1]+1))}{6} \right)
\end{aligned}$$

Alors $p(n+1)$ serait aussi vraie. Nous venons de montrer $p(n) \rightarrow p(n+1)$ est vraie, et ça pour chaque $n \in \mathbb{N}$.

Donc nous avons montré que

- $p(0)$ vraie
- et pour chaque $n \in \mathbb{N}$: $p(n) \rightarrow p(n+1)$ est vraie.

• Conclusion : Par le principe d'induction, on conclut la preuve du lemme par induction. $\square$

Exemple : Considérons pour chaque $n \in \mathbb{N}$.

$$s(n) = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \ldots + \frac{1}{(n+1) \cdot (n+2)}$$

Trouver une formule pour $s(n)$ et montrer cette formule ensuite.
Brouillon :

$$s(0) = \tfrac{1}{2},\ s(1) = \tfrac{1}{1\cdot 2} + \tfrac{1}{2\cdot 3} = \tfrac{2}{3},\ s(2) = \tfrac{2}{3} + \tfrac{1}{3\cdot 4} = \tfrac{3}{4}.$$

Conjecture : Pour chaque $n \in \mathbb{N}$: $s(n) = \frac{n+1}{n+2}$.

Proposition

Pour chaque $n \in \mathbb{N}$ *on a :* $s(n) = \frac{n+1}{n+2}$.

Démonstration par induction.

Préparation. Posons $P(n) = "s(n) = \frac{n+1}{n+2}"$. Il faut montrer $\forall n \; P(n)$.

Début : Au moins nous avons déjà vérifié que $P(0)$, $P(1)$ et $P(2)$ sont vraies.

Étape d'induction : Soit $n \in \mathbb{N}$ arbitraire. Supposons $P(n)$ vraie, c.-à-d., $s(n) = \frac{n+1}{n+2}$. Donc

$s(n+1) = s(n) + \frac{1}{(n+2)\cdot(n+3)} = \frac{n+1}{n+2} + \frac{1}{(n+2)\cdot(n+3)} =$
$= \frac{(n+1)(n+3)+1}{(n+2)(n+3)} = \frac{(n^2+4n+3)+1}{(n+2)(n+3)} = \frac{(n+2)^2}{(n+2)(n+3)} \frac{n+2}{(n+3)}$. Donc $P(n) \to P(n+1)$ est vraie.

Conclusion : Par le principe d'induction notre formule est vraie pour chaque $n \in \mathbb{N}$. Alors nous avons aussi montré la proposition ! $\square$