Aujourd'hui nous allons discuter :

• Autres modèles de preuve.
• Preuve vide, preuve cas-par-cas, preuve-par-exemple.
• Contre-exemples, et
• Quantificateurs universels
• Traductions de propositions mathématiques en propositions logiques avec beaucoup de $\forall, \exists$.
• Des équivalences logiques et des inférences en présence de $\forall$ et $\exists$.
• Avec preuves.

Modèles de preuve

Nous avons déjà discuté certains modèles de preuves .

- Preuve directe et indirecte (pour les implications $p \to q$).
- Preuve par l'absurde.

Il y en a d'autres qui sont valides (à suivre).

Il y a de fausses "preuves" aussi.

- "Preuve" par raisonnement circulaire.
- "Preuve" par intimidation ou par charme.
- "Preuves" basées sur des contre-vérités.

Une preuve vide.

Supposons on doit montrer $P \to Q$.

Si on sait déjà (ou si on montre) que P est faux ou si Q est vraie : après il ne reste rien à faire !

L'implication $P \to Q$ est vraie.

Une preuve cas-par-cas.

Exemple : Soit $U := \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$ l'univers de discours de la fonction propositionnelle :
$p(u) :=$"u est la somme de trois carrés parfaits".

Montrer la proposition :
$P := \forall u \; p(u)$ (est vraie).

Preuve cas par cas :

$2 = 0 + 1 + 1$, $4 = 0 + 0 + 4$, $6 = 1 + 1 + 4$, $8 = 0 + 4 + 4$, $10 = 0 + 1 + 9$, $12 = 4 + 4 + 4$, $14 = 1 + 4 + 9$, $16 = 0 + 0 + 16$, $18 = 0 + 9 + 9$. $\square$

• On veut montrer $P \leftrightarrow Q$?

Il suffit de montrer cas par cas que $P \rightarrow Q$ et $Q \rightarrow P$.

• On veut montrer $(p \vee q) \rightarrow r$?

Il suffit de montrer cas par cas que $p \rightarrow r$ et $q \rightarrow r$

(C'est correct par l'équivalence logique
$((p \vee q) \rightarrow r) \Leftrightarrow ((p \rightarrow r) \wedge (q \rightarrow r)))$

Un exemple :

Soit n un nombre naturel fixé. À montrer la proposition :

$P :=$ "Si n n'est pas divisible par 3 alors $n^2 - 1$ est divisible par 3".

Preuve ?

Préparation (traduction en logique) : Posons
$p_1 :=$"il existe un nombre naturel m tel que $n = 3m + 1$" ;
$p_2 :=$"il existe un nombre naturel m tel que $n = 3m + 2$" ;
$r :=$"$n^2 - 1$ est divisible par 3".
En math. au cegep (ou avant) on a montré que (on l'accepte) :
"n n'est pas divisible par 3" si et seulement si $p_1 \vee p_2$.
On doit montrer : $(p_1 \vee p_2) \to r$. Il suffit de montrer $p_1 \to r$ et $p_2 \to r$.

(cont.)

p_1 :="il existe un nombre naturel m tel que $n = 3m + 1$" ;
p_2 :="il existe un nombre naturel m tel que $n = 3m + 2$" ;
r :="$n^2 - 1$ est divisible par 3".

Preuve cas-par-cas :

Preuve de $p_1 \to r$: On a que $n^2 - 1 = (3m+1)^2 - 1 = 9m^2 + 6m = 3(3m^2 + 2m)$ est un 3-multiple.

Preuve de $p_2 \to r$: On a que $n^2 - 1 = (3m+2)^2 - 1 = 9m^2 + 12m + 3 = 3(3m^2 + 4m + 1)$ est un 3-multiple.

Fin de la preuve. $\square$

Preuve-par-exemple

Soit $p(u)$ une fonction propositionnelle avec l'univers de discours U.
Pour montrer

$$\exists u \; p(u),$$

il *suffit* de trouver un exemple : c.-à-d. trouver explicitement un $a \in U$ pour lequel on montre que $p(a)$ est vraie.

Par exemple :
On a que
$$\exists n \in \mathbb{Z}\ [\neg "n > 0" \rightarrow "n^2 > 0"]$$
est vraie.
Preuve : Il suffit de donner un exemple : prenons $n = 1$ alors $n \in \mathbb{Z}$, "$n > 0$" est vraie, $\neg$"$n > 0$" est fausse donc l'implication $[\neg "n > 0" \rightarrow "n^2 > 0"]$ est vraie.

Considérons la proposition logique :
"Le nombre naturel 41 est la somme de deux carrés parfait"
Comment traduire en logique ?

$\exists m \ \exists n \ (41 = n^2 + m^2)$, où l'univers de discours de n et m est $\mathbb{N}$
On a besoin d'une quantificateur existentielle !
Une possibilité de preuve est par donner un exemple :
Preuve : Vraie, car $41 = 25 + 16 = 5^2 + 4^2$.

Il y a parfois d'autres méthodes.

Soit $f : \mathbb{R} \to \mathbb{R}$ la fonction $f(x) = x^5 + 12x^3 - 21x^2 + \pi x - \sqrt{2}$.
Montrer :

$$\exists x \in \mathbb{R} \; f(x) = 0.$$

Preuve : utiliser la "continité" des polynômes, voir MAT1400.

Dans un tel preuve on ne donne pas d'exemple explicit !

Variation : Preuve-par-contre-exemple

Soit $p(u)$ une fonction propositionnelle avec l'univers de discours U.
Pour montrer

$$\exists u \ \neg p(u),$$

il *suffit* de trouver un contre-exemple : c.-à-d. trouver explicitement un $a \in U$ pour lequel on montre que $p(a)$ est fausse..

Chercher contre-exemples

Est-ce que

$$P := [(p \wedge \neg q) \wedge [p \to (q \to r)]] \to \neg r$$

est une tautologie ?

Sinon, il existe un contre-exemple. Cherchons un contre-exemple.

Si P est fausse
alors $[(p \wedge \neg q) \wedge [p \to (q \to r)]]$ vraie, mais $\neg r$ fausse ;
alors p, $\neg q$, $p \to (q \to r)$ et r sont vraies ;
alors p, $\neg q$, $(q \to r)$ et r sont vraies ;
alors p, r sont vraies et q est fausse.

Vraie : Si P est fausse, alors nécessairement p, r sont vraies et q est fausse.

$$P := [(p \wedge \neg q) \wedge [p \rightarrow (q \rightarrow r)]] \rightarrow \neg r$$

Si P est fausse, alors nécessairement p, r sont vraies et q est fausse.

Mais aussi dans le sens inverse ?

• Est-ce que tous les "alors" dans l'argument sont des "si et seulement si"'s ?

• Ou simplement vérifier si choisir p, r vraies et q est fausse donne un contre-exemple :

$$[(V \wedge \neg F) \wedge [V \rightarrow (F \rightarrow V)]] \rightarrow \neg V$$

donc P serait F dans cette situation.

Effectivement c'est un contre-exemple et P n'est pas une tautologie.

Montrer que

$$P := [(p \wedge \neg q) \wedge r] \rightarrow [(p \wedge r) \vee q]$$

est une tautologie.

Preuve : Cherchons un contre-exemple.

Si P est fausse
alors $[(p \wedge \neg q) \wedge r]$ est vraie mais $[(p \wedge r) \vee q]$ est fausse ;
alors p, $\neg q$ et r sont vraies, mais $(p \wedge r)$ et q sont fausses ;
alors p, et r sont vraies mais $(p \wedge r)$ est fausse, ce qui est absurde !

Il est impossible de trouver un contre-exemple.

Conclusion : P est une tautologie.

Encore contre-exemples..

Soit $p(u)$ une fonction propositionnelle, avec univers de discours U. Pour montrer que $\forall u \; p(u)$ est faux, il suffit de trouver un contre-exemple.

C.-à-d., trouver un instance $a \in U$ tel que $p(a)$ est faux.

Une possibilité pour montrer que $\forall u \; p(u)$ est vraie est de montrer que des contre-exemples n'existent pas !

Comment traduire en logique ?

P :="Soit n un nombre naturel fixé. Alors $n^2 - 1$ est divisible par 3 si n n'est pas divisible par 3".
ou
"Pour chaque nombre naturel n on a que si n n'est pas divisible par 3 alors $n^2 - 1$ est divisible par 3".

Une traduction en logique.
Introduire des fonctions propositionnelles avec univers de discours $\mathbb{N}$:
$p(n) :=$ "n est divisible par 3",
$r(n)$:="$n^2 - 1$ est divisible par 3.

$$P = \forall n \; [(\neg p(n)) \to r(n)]$$

Nous avons déjà donné une preuve.
Modèle :
Fixons un $n \in N$ (arbitrairement, donc non-explicitement). Puis montrer $[(\neg p(n)) \rightarrow r(n)]$ sachant seulement que $n \in \mathbb{N}$. Etcetera.

Règles logiques pour les fonctions propositionnelles

Souvent on doit traiter des propositions logiques avec $\forall$ et $\exists$.

Il faut des règles pour manipuler, comme

- $\neg(\forall u\ p(u)) \Leftrightarrow \exists u\ \neg p(u)$

$((\forall u\ p(u))$ est faux si et seulement "il existe un contre-exemple")
et

- $\neg(\exists u\ p(u)] \Leftrightarrow \forall u\ \neg p(u)$.

Traduction : "$\exists u\ p(u)$" est fausse si et seulement si pour chaque u on a que $p(u)$ est fausse.
Rappelons une preuve pourquoi.

Soit $p(u)$ une fonction propositionnelle avec univers de discours U.

$$U_V := \{u \in U |\ p(u) \text{ est vraie}\}$$

$$U_F := \{u \in U |\ p(u) \text{ est fausse}\}$$

On a $U = U_V \cup U_F$ et $U_V \cap U_F = \emptyset$.

Donc $U_V = U$ si et seulement si $U_F = \emptyset$.

Par définition :
$\forall u\ p(u)$ si et seulement si $U_V = U$ si et seulement si $U_F = \emptyset$;
$\forall u\ \neg p(u)$ si et seulement si $U_V = \emptyset$ si et seulement si $U_F = U$.

et
$\exists u\ p(u)$ si et seulement si $U_V \neq \emptyset$ si et seulement si $U_F \neq U$;
$\exists u\ \neg p(u)$ si et seulement si $U_V \neq U$ si et seulement si $U_F \neq \emptyset$.

On a aussi
$\neg(\forall u\ p(u))$ si et seulement si $U_V \neq U$ si et seulement si $U_F \neq \emptyset$.
$\neg(\exists u\ p(u))$ si et seulement si $U_V = \emptyset$ si et seulement si $U_F \neq U$.
Conclusion :

$$\neg(\forall u\ p(u)) \Leftrightarrow \exists u\ \neg p(u) \quad \text{et} \quad \neg(\exists u\ p(u)] \Leftrightarrow \forall u\ \neg p(u)$$

Exemple :

$\forall n \in \mathbb{Z}\ [\neg "n > 0" \rightarrow "n^2 > 0"]$ est fausse.

Preuve : parce que $n = 0$ donne un contre-exemple !
Car $\neg "0 > 0"$ est vraie, mais $"0^2 > 0"$ est fausse.

Autres règles

Soit $p(u)$ une fonction propositionnelle avec univers de discours U non-vide alors

$$(\forall u \ p(u)) \rightarrow (\exists u \ p(u))$$

est une tautologie.

Mais si $U = \emptyset$ alors $(\forall u \ p(u))$ est vraie et $(\exists u \ p(u))$ est fausse !

Modification :

$$[(\forall u \ p(u)) \wedge U \neq \emptyset] \Rightarrow (\exists u \ p(u))$$

Soit $a \in U$ un certain élément.

$$[\forall u \ p(u)] \rightarrow p(a)$$

est une tautologie.

$$[[\forall u \ p(u)] \wedge (a \in U)] \Rightarrow p(a)$$

Autres équivalences utiles ?

Pour mieux comprendre nos règles et trouver d'autres :
Supposons que l'univers du discours U est fini :
$U = \{u_1, u_2, \ldots, u_n\}$.

Dans ce cas $\forall u \ p(u)$ veut dire
$p(u_1) \wedge p(u_2) \wedge \ldots \wedge p(u_n)$

Et $\exists u \ p(u)$ veut dire
$p(u_1) \vee p(u_2) \vee \ldots \vee p(u_n)$.

En utilisant les définitions de $\forall$, $\exists$ et la règle de De Morgan plusieurs fois, on obtient

$$\begin{aligned}
\neg[\forall u \; p(u)] &\Leftrightarrow \neg[p(u_1) \wedge p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \\
&\Leftrightarrow \neg p(u_1) \vee \neg[p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \\
&\Leftrightarrow \neg p(u_1) \vee \neg p(u_2) \vee \neg[p(u_3) \wedge \ldots \wedge p(u_n)] \\
&\Leftrightarrow \ldots \\
&\Leftrightarrow \neg p(u_1) \vee \neg p(u_2) \vee \ldots \vee \neg p(u_n) \\
&\Leftrightarrow \exists u \; \neg p(u).
\end{aligned}$$

Donc notre formule $\neg[\forall u \; p(u)] \Leftrightarrow [\exists u \; \neg p(u)]$ est une règle de De Morgan généralisée !

Et si on utilise les règles de la distributivité ? Soit q une proposition logique. En utilisant la distributivité plusieurs fois, on obtient

$$\begin{aligned}
[\forall u \ p(u)] \vee q &\Leftrightarrow [p(u_1) \wedge p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \vee q \\
&\Leftrightarrow [p(u_1) \vee q] \wedge [[p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \vee q] \\
&\Leftrightarrow [p(u_1) \vee q] \wedge [p(u_2) \vee q] \wedge [[p(u_3) \wedge \ldots \wedge p(u_n)] \vee q] \\
&\Leftrightarrow \ldots \\
&\Leftrightarrow [p(u_1) \vee q] \wedge [p(u_2) \vee q] \wedge \ldots \wedge [p(u_n) \vee q] \\
&\Leftrightarrow \forall u \ [p(u) \vee q]
\end{aligned}$$

Nous avons obtenue une règle logique si U est fini. Nous allons voir que cette règle reste vraie si U n'est pas fini.

Proposition

Soit $p(u)$ une fonction propositionnelle d'univers du discours U (fini ou infini), et q une proposition logique.
$([\forall u \ p(u)] \vee q) \Leftrightarrow (\forall u \ [p(u) \vee q])$

Démonstration.

(i) Pour montrer "$((\forall u \ p(u)) \vee q) \rightarrow (\forall u \ [p(u) \vee q])$", supposons $(\forall u \ p(u)) \vee q$ est vraie, c-.à-d. q est vraie ou $(\forall u \ p(u))$ est vraie. Si q est vraie, alors $[p(u) \vee q]$ est vraie pour chaque u ; c.-à-d. $\forall u \ [p(u) \vee q]$ est vraie. Si $p(u)$ est vraie pour chaque u, alors aussi $p(u) \vee q$ est vraie pour chaque u, c.-à-d. $\forall u \ [p(u) \vee q]$ est vraie. Donc nous avons montré que si $(\forall u \ p(u)) \vee q$ est vraie, alors $\forall u \ [p(u) \vee q]$ est vraie aussi. $\square$

(Suite).

(ii) Pour montrer "$(\forall u\ [p(u) \vee q]) \rightarrow [(\forall u\ p(u)) \vee q]$", supposons $(\forall u\ [p(u) \vee q])$ est vraie, c-.à-d., $[p(u) \vee q]$ est vraie pour chaque u. Alors si q est fausse, on a nécessairement $p(u)$ est vraie pour chaque u, i.e, $\forall u\ p(u)$ est vraie et donc aussi $[\forall u\ p(u)] \vee q$ est vraie. Et si q est vraie, alors $[\forall u\ p(u)] \vee q$ est vraie aussi. Donc nous avons montré que si $\forall u\ [p(u) \vee q]$ est vraie alors $(\forall u\ p(u)) \vee q$ est vraie aussi.
Ainsi la formule est montrée. $\square$

En utilisant la commutativité et l'associativité de $\wedge$ et

$$q \Leftrightarrow [q \wedge q] \Leftrightarrow [q \wedge q \wedge q] \Leftrightarrow [q \wedge q \wedge q \wedge q] \Leftrightarrow \ldots$$

on obtient

$$\begin{aligned}
[\forall u \ p(u)] \wedge q &\Leftrightarrow [p(u_1) \wedge p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \wedge q \\
&\Leftrightarrow [p(u_1) \wedge p(u_2) \wedge p(u_3) \wedge \ldots \wedge p(u_n)] \wedge [q \wedge q \ldots \wedge q] \\
&\Leftrightarrow [p(u_1) \wedge q] \wedge [p(u_2) \wedge q] \wedge \ldots \wedge [p(u_n) \wedge q] \\
&\Leftrightarrow \forall u \ [p(u) \wedge q]
\end{aligned}$$

Nous avons obtenue une règle logique si U est fini. Cette règle reste aussi vraie si U n'est pas fini.
Similairement pour $\exists$.

Sommaire :

Proposition

Soit $p(u)$ une fonction propositionnelle avec univers de discours un ensemble U, et q une proposition logique. Alors on a

$$(\forall u\ p(u)) \vee q \quad \Leftrightarrow \quad \forall u\ [p(u) \vee q] \text{ (distr. généralisée)}$$
$$(\forall u\ p(u)) \wedge q \quad \Leftrightarrow \quad \forall u\ [p(u) \wedge q] \text{ (assoc. et comm. de } \wedge \text{ généralisée)}$$
$$(\exists u\ p(u)) \vee q \quad \Leftrightarrow \quad \exists u\ [p(u) \vee q] \text{ (assoc. et comm. de } \vee \text{ généralisée)}$$
$$(\exists u\ p(u)) \wedge q \quad \Leftrightarrow \quad \exists u\ [p(u) \wedge q] \text{ (distr. généralisée)}$$

Les (autres) preuves sont laissées à vous.

Corollaire

Soit $p(u)$ une fonction propositionnelle avec univers du discours un ensemble U, et $q(v)$ une proposition logique avec univers du discours l'ensemble V.
Quelques équivalences (mais on en a d'autres similaires) :

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

Ces règles sont donc naturelles.