Aujourd'hui nous allons discuter :

- Exemple de preuve par algèbre
- Modèles de preuve.
- Directe, indirecte, par contradiction.
- 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.

Autre exemple de l'utilisation de l'algèbre de Boole.

Considérons

$$[(p \vee q) \to r] \Leftrightarrow ((p \to r) \wedge (q \to r)).$$

Preuve algébrique :

$$\begin{aligned}
[(p \vee q) \to r] &\Leftrightarrow \neg(p \vee q) \vee r \text{ (Car } p \to q \Leftrightarrow \neg p \vee q) \\
&\Leftrightarrow (\neg p \wedge \neg q) \vee r \text{ (Par De Morgan)} \\
&\Leftrightarrow (\neg p \vee r) \wedge (\neg q \vee r) \text{ (Par distr.)} \\
&\Leftrightarrow (p \to r) \wedge (q \to r) \text{ (Car } p \to q \Leftrightarrow \neg p \vee q)
\end{aligned}$$

Et voilà. $\square$

Rappel : on peut substituer !

Exemple : Dans l'équivalence logique

$$[(p \to r) \wedge (q \to r)] \Leftrightarrow [(p \vee q) \to r]$$

remplace "p" partout par $q \vee (r \to s)$ et "q" partout par $p \to s$ et r par p.
On obtient une autre équivalence (mais pas intéressante) :

$$[([q \vee (r \to s)] \to r) \wedge ([p \to s] \to p)] \Leftrightarrow [([q \vee (r \to s)] \vee [p \to s]) \to p]$$

Utilisation des équivalences logiques en mathématiques

Surtout les équivalences logiques simples sont utilisées dans les arguments et les preuves mathématiques.

Il faut être conscient quand on le fait.

Les équivalences déjà mentionnées sont souvent utilisées :

$$(P \leftrightarrow Q) \Leftrightarrow ((P \rightarrow Q) \wedge (Q \rightarrow P))\,;$$

$$(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P) \Leftrightarrow (\neg P \vee Q) \Leftrightarrow \neg(P \wedge \neg Q).$$

Soient P et Q deux proposition logiques en mathématiques.
Supposons on veut montrer :

Théorème
$P \to Q$.

- À montrer que cette proposition logique $P \to Q$ est vraie.
- Il suffit de montrer que l'implication $(\neg Q \to \neg P)$ est vraie.
- Il suffit de montrer que la proposition $(\neg P \vee Q)$ est vraie.
- Il suffit de montrer que la proposition $(P \wedge \neg Q)$ n'est pas vraie.

Donc il y a logiquement plusieurs façons de montrer le théorème.

Exemple.
Soit donné un nombre $n \in \mathbb{Z}$.
À montrer :

S'il existe un nombre $m \in \mathbb{Z}$ tel que $n = m^2$ alors $n \geq 0$.

À montrer : $p \to q$ avec

p :='Il existe un nombre $m \in \mathbb{Z}$ tel que $n = m^2$"
q := "$n \geq 0$".

Il y a plusieurs façons logiquement équivalentes !

$p \to q$: "S'il existe un $m \in \mathbb{Z}$ tel que $n = m^2$ alors $n \geq 0$."

$\neg q \to \neg p$: "Si $n < 0$ alors il n'existe pas de $m \in \mathbb{Z}$ tel que $n = m^2$"

ou

$(\neg p \vee q)$: "Il n'existe pas de $m \in \mathbb{Z}$ tel que $n = m^2$ ou $n \geq 0$".

$\neg(p \wedge \neg q)$:" Ce n'est pas vraie que simultanément $n < 0$ et il existe un $m \in \mathbb{Z}$ tel que $n = m^2$.

Donc il y a logiquement plusieurs façons de montrer un théorème du type

$P \to Q$.

Preuve directe typique :

Si P est fausse, l'implication $P \to Q$ est automatiquement vraie et il n'y aura rien à faire (cette phrase est souvent omise).

Supposons P est vraie. Puis (avec cette hypothèse et avec de l'aide des théorèmes déjà montrés), on montre que Q serait en conséquence aussi vraie.

Ainsi on aura montré que $P \to Q$ est vraie. $\square$

En math : si on écrit "On veut montrer P" ça veut dire "On veut montrer que la proposition logique P est vraie."

Preuve indirecte typique :
Il suffit de montrer la contraposé $(\neg Q) \to (\neg P)$.

Si $\neg Q$ est fausse (c.-à-d., Q est vraie), l'implication est automatiquement vraie. (Cette phrase est souvent omise).

Supposons $\neg Q$ est vraie, c.-à-d, que Q est fausse. Puis (avec cette hypothèse et avec de l'aide des théorèmes déjà montrés), on montre que P serait aussi fausse.

On aura montré que $(\neg Q) \to (\neg P)$ est vraie et donc automatiquement aussi que $P \to Q$ est vraie. $\square$

Différence : avec une preuve directe on travaille avec l'hypothèse que P soit vraie pour montrer qu'alors Q serait aussi vraie.

Avec une preuve indirecte on travaille avec l'hypothèse que Q soit fausse pour montrer qu'alors P serait fausse aussi.

Troisième type de preuve : Il suffit de montrer que c'est fausse que $(P \wedge \neg Q)$.

Supposant par contre que c'est vraie, c-à-d. on suppose P soit vraie ET Q soit fausse.
Puis, en utilisant ça comme hypothèse et des théorèmes déjà montrés, on déduit une absurdité à votre choix, par exemple qu'un certain nombre entier serait au même temps pair et impair, ou que $0 = 1$, ou $V = F$. Ce qui est absurde !
Alors c'est fausse que $(P \wedge \neg Q)$!

On conclut la preuve du théorème. $\square$

Différence : avec une telle preuve on commence par l'hypothèse généreuse que P est vraie ET Q est fausse. Avec cette hypothèse on travaille pour obtenir une absurdité.

Ce troisième type est un exemple de preuve par contradiction, "reduire à l'absurdité", voir plus tard....

Mais faites attention :

on ne doit pas mixer les hypothèses et les conclusions des trois types de preuves !

Il faut clairement écrire vos hypothèses pour éviter la confusion.

Preuve par l'absurde ou Reductio ad absurdum

Si, en supposant qu'une proposition P soit fausse, on peut argumenter qu'une autre proposition serait simultanément vraie et fausse (une contradiction, ce qui est absurde).

Dans ce cas P est nécessairement vraie ! !

C'est une preuve par l'absurde, ou une preuve par contradiction.

Une telle preuve peut être basée sur la règle d'inférence :

$$[(\neg p \to (q \wedge \neg q)] \Rightarrow p$$

ou sur la règle

$$[(\neg p \to q) \wedge \neg q] \Rightarrow p$$

On répète :

Supposons on veut montrer qu'une proposition p est vraie.

En supposant p est fausse, on montre une proposition auxiliaire disons q. Alors que $\neg p \to q$ est vraie.
Puis on montre (ou on sait déjà) que son opposé $\neg q$ est vraie.
Donc l'hypothèse de la règle d'inférence est vraie :

$$[(\neg p \to q) \wedge \neg q] \Rightarrow p.$$

C'est une règle d'inférence, donc aussi la conclusion p est vraie.

Une modèle de preuve :

Soit P une proposition en mathématiques.

Théorème

P

Preuve par l'absurde typique.

Supposons P est fausse. Puis (avec cette hypothèse et avec de l'aide de théorèmes déjà montrés) on montre une proposition auxiliaire, disons q. Puis on montre directement (sans utiliser l'hypothèse que P est fausse) que q est fausse. Ce qui serait absurde.
On conclut : P est vraie. $\square$

Un cas spécial. Soient P et Q deux propositions en mathématiques.

Théorème

$P \rightarrow Q$

Preuve par l'absurde typique=troisième type.

Supposons $P \rightarrow Q$ est fausse, c.-à-d., supposons P vraie et Q fausse. Puis (avec ces deux hypothèses et avec de l'aide de théorèmes déjà montrés) on montre une proposition auxiliaire, disons r. Puis on montre directement (sans utiliser l'hypothèse que $P \rightarrow Q$ est fausse) que r est fausse. Ce qui serait absurde.
On conclut : $P \rightarrow Q$ est vraie. $\square$

Exemple :

Théorème

Soient A et B deux ensembles et $F : A \to B$ et $G : B \to A$ deux fonctions telles que $G \circ F = 1_A$.
Alors F est injective.

Supposons $F : A \to B$ et $G : B \to A$ sont deux fonctions telles que $G \circ F = 1_A$.
Posons P :="F est injective."
Montrons que P est vraie.

Preuve par l'absurde : Supposons P est faux, c.-à-d., F n'est pas injective.

Par définition d'injectivité, ils existent alors deux éléments a_1, a_2 de A telles que $F(a_1) = F(a_2)$, mais $a_1 \neq a_2$.
Parce que $G \circ F = 1_A$ on a

$$a_1 = 1_A(a_1) = G(F(a_1)) = G(F(a_2)) = 1_A(a_2) = a_2.$$

Donc sous l'hypothèse que P est fausse, on aurait montré que la proposition $a_1 = a_2$ est vraie et fausse. Ce qui est absurde.
On conclut P est vraie. $\square$

Autres 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.

(Parce que $(P \to Q) \Leftrightarrow (\neg P \vee Q)$.)

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
$((p \vee q) \rightarrow r) \Leftrightarrow ((p \rightarrow r) \wedge (q \rightarrow r))$
et donc
$((p \rightarrow r) \wedge (q \rightarrow r)) \Rightarrow (p \vee q) \rightarrow r))$

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 :
La proposition

$$\exists n \in \mathbb{Z}\ [\neg "n > 0" \rightarrow "n^2 > 0"]$$

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 pour $n = 1$. $\square$

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 $41 = 25 + 16 = 5^2 + 4^2$ donne un exemple. $\square$

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 "continuité" 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

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

est une tautologie ?

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

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

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

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 :

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

donc P serait F dans cette situation.
Effectivement c'est un contre-exemple et P n'est pas une tautologie.

Montrer que

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

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.