

# IF107 - Techniques de preuve

Frédéric Herbreteau

`frederic.herbreteau@bordeaux-inp.fr`

8 novembre 2024

# 1. Introduction à la preuve

# Raisonnement et démonstration

*Le **raisonnement** est défini comme une **suite d'arguments**, de propositions liés les uns aux autres, en particulier **selon des principes logiques**, et **organisés** de manière à **aboutir à une conclusion** – (Larousse)*

## Définition

Une **démonstration** est un raisonnement permettant la **vérification** d'une **proposition** à partir d'un ensemble de connaissances : **définitions**, **axiomes**, **conjectures**, **théoremes**

# Proposition

## Définition

Une **proposition** est un énoncé qui est soit vrai, soit faux

## Exemple

- ▶  $2 + 3 = 5$ , proposition vraie
- ▶ “pour tout  $n \in \mathbb{N}$ ,  $n^2 + n + 41$  est un nombre premier”, proposition fausse : pour  $n = 41$ , on obtient  $41^2$
- ▶ “le ciel” n’est pas une proposition
- ▶ **tiers-exclus** : une proposition qui n’est pas fausse est vraie et inversement
- ▶ **non paradoxale** : “cette phrase est fausse” n’est pas une proposition

# Prédicat

## Définition

Un **prédicat** est une proposition dont la véracité dépend d'une ou plusieurs variables

## Exemple

- ▶ “ $n$  est pair” n’est pas une proposition mais un prédicat : vrai pour  $n = 2$ , faux pour  $n = 3$   
(notation usuelle : “ $pair(n)$ ”)
- ▶ “si  $n$  est pair, alors  $n + 1$  est impair” est une proposition vraie pour tout  $n \in \mathbb{N}$   
(ou : “pour tout  $n \in \mathbb{N}$ , si  $pair(n)$  alors non( $pair(n + 1)$ )”)

# Axiomes (Euclide, vers 300 av. J.C.)

## Définition

Un **axiome** est une proposition **supposée vraie**

## Exemple

- ▶ pour tout  $x, y, z \in \mathbb{Z}$  si  $x \leq y$  et  $y \leq z$ , alors  $x \leq z$
- ▶ par toute paire de points passe une droite
- ▶ un entier  $n$  est pair s'il existe un entier  $k$  tel que  $n = 2k$
- ▶ un nombre  $r$  est rationel s'il existe deux entiers  $a$  et  $b \neq 0$  tels que  $r = \frac{a}{b}$  (forme irréductible)

# Théorie

Un ensemble d'axiomes définit une **théorie**, qui fixe un cadre de raisonnement

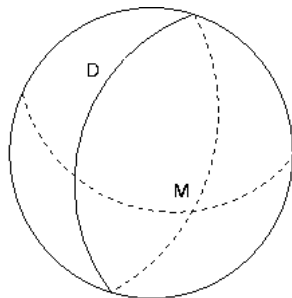
## Exemple (Axiomes de la géométrie Euclidienne)

1. un segment de droite peut être tracé en joignant deux points quelconques distincts ;
2. un segment de droite peut être prolongé indéfiniment en une ligne droite ;
3. étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre ;
4. tous les angles droits sont congruents ;
5. si deux droites sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est strictement inférieure à deux angles droits, alors ces deux droites sont forcément sécantes de ce côté.

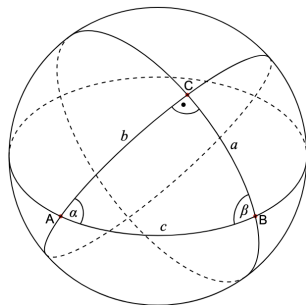
(source Wikipédia)

Certains résultats standards de géométrie (Pythagore, Thalès, etc) et de physique (Newton, etc) peuvent être **démontrés dans cette théorie**.

## Autres axiomes, autre théorie



(Source : Wikipédia)



En géométrie elliptique :

- ▶ étant donné une droite ( $D$ ) et un point ( $M$ ) extérieur à cette droite, il n'existe aucune droite parallèle à cette droite passant par ce point ;
- ▶ la somme des angles d'un triangle fait entre 180 et 540 degrés.

# Quelle théorie ?

Un ensemble d'axiomes est

- ▶ **consistant** si on ne peut pas prouver qu'une proposition est à la fois vraie et fausse
- ▶ **complet** si toute proposition peut être prouvée vraie ou fausse

## Théorème (Gödel, 1931)

*Tout ensemble récursif d'axiomes consistant pour l'arithmétique entière est nécessairement incomplet*

En pratique, on choisit un ensemble d'axiomes **pertinent** pour ce que l'on veut modéliser

### Exemple

Les axiomes d'Euclide sont pertinents pour modéliser le monde physique ambiant (ni macroscopique, ni microscopique)

**Nos axiomes** : les connaissances mathématiques de base

# Énoncés

- ▶ **Définition** : proposition qui définit un objet ou un concept par ses principales caractéristiques

## Exemple

Un nombre entier  $n$  est pair s'il existe  $k \in \mathbb{Z}$  tel que  $n = 2k$

- ▶ **Conjecture** : proposition supposée vraie pour laquelle on ne connaît pas encore de preuve

## Exemple (Goldbach)

tout entier pair  $n > 2$  est la somme de deux nombres premiers

- ▶ **Théorème** : proposition qui peut être démontrée

## Exemple

pour tout  $n \in \mathbb{N}$ , si  $n$  est pair, alors  $n + 1$  est impair

# Démontrer

- Pour démontrer qu'une proposition ou un prédicat est vrai, il faut montrer qu'elle/il est vrai **dans tous les cas** (en général une infinité)

## Exemple

“pour tout  $n \in \mathbb{N}$ , si  $n$  est pair, alors  $n + 1$  est impair”

- soit  $n$  est impair, auquel la proposition est vraie
- soit  $n$  est pair, alors  $n = 2k$  pour un certain  $k \in \mathbb{N}$ , donc  $n + 1 = 2k + 1$  est un nombre impair
- Par contre, pour montrer qu'une proposition ou un prédicat est faux, il suffit de trouver **une situation où elle/il est faux** (contre-exemple).

## Exemple

“ $n^2 + n + 41$  est un nombre premier” est faux pour  $n = 41$

# Déduction logique

## Définition

Une **règle de déduction** combine des axiomes et d'autres propositions vraies, afin d'établir de nouvelles propriétés vraies

## Exemple

- ▶ **Modus Ponens** : 
$$\frac{A \quad A \text{ implique } B}{B}$$
- ▶ **Transitivité de l'implication** : 
$$\frac{A \text{ implique } B \quad B \text{ implique } C}{A \text{ implique } C}$$
- ▶ **Contraposée** : 
$$\frac{A \text{ implique } B}{\text{non}(B) \text{ implique } \text{non}(A)} \quad \text{et} \quad \frac{\text{non}(B) \text{ implique } \text{non}(A)}{A \text{ implique } B}$$

**Cohérence** : lorsque les prémisses sont vraies, alors la conclusion doit également être vraie

## Exemple

Non-cohérente : 
$$\frac{A \text{ implique } B}{B \text{ implique } A}$$

# Preuve axiomatique

*On énoncera explicitement les concepts primitifs au moyen desquels on se propose de définir logiquement les autres. On énoncera explicitement les propositions fondamentales (postulats) grâce auxquelles on se propose de **démontrer logiquement** les autres propositions (théorèmes). Ces propositions fondamentales doivent apparaître comme de **pures relations logiques entre les concepts primitifs**, et cela indépendamment de la signification que l'on donne à ces concepts primitifs – Pasch (et Hilbert)*

*(Source : Wikipédia)*

**Preuve** : succession d'étapes de déduction, partant des axiomes, et aboutissant à la proposition à démontrer

## 2. Schémas de preuve

## 2.1 Implication

# Implication

“Si  $A$ , alors  $B$ ”      ou      “ $A$  implique  $B$ ”

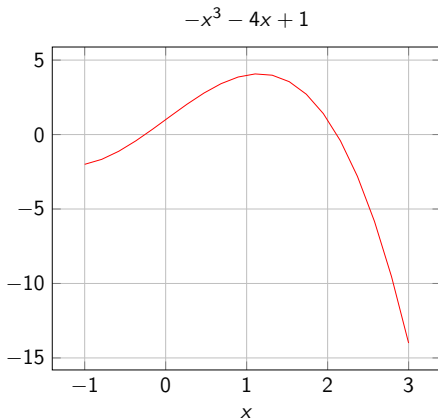
## Exemple

- ▶ Si  $ax^2 + bx + c = 0$  et  $a \neq 0$ , alors  $x = (-b \pm \sqrt{b^2 - 4ac})/2a$
- ▶ Si  $n$  est un entier pair strictement supérieur à 2, alors  $n$  est la somme de deux nombres pairs (conjecture de Goldbach)
- ▶ Si  $0 \leq x \leq 2$ , alors  $-x^3 + 4x + 1 > 0$
- ▶ Si  $x$  est irrationnel, alors  $\sqrt{x}$  est irrationnel

## Intuition, brouillon de preuve

“Si  $0 \leq x \leq 2$ , alors  $-x^3 + 4x + 1 > 0$ ”

| $x$ | $-x^3$ | $4x$ |
|-----|--------|------|
| 0   |        |      |
| 1   |        |      |
| 2   |        |      |



$4x$  **semble** dominer  $-x^3$  sur l'intervalle  $[0; 2]$

## 1ère méthode (directe)

**“Si  $A$ , alors  $B$ ”**

1. Supposer que  $A$  est vrai
2. Puis montrer que  $B$  est une conséquence logique

### Exemple

**“Si  $0 \leq x \leq 2$ , alors  $-x^3 + 4x + 1 > 0$ ”**

**Supposons  $0 \leq x \leq 2$**

**Conclusion :  $-x^3 + 4x + 1 > 0$**

## 2ème méthode (contraposée)

**“Si  $A$ , alors  $B$ ”**

1. équivalent à **“Si  $\text{non}(B)$ , alors  $\text{non}(A)$ ”**
2. utiliser la méthode 1

### Exemple

**Si  $n^2$  est pair, alors  $n$  est pair**

**Contraposée : “Si  $n$  est impair, alors  $n^2$  est impair”**

## 2.2 Équivalence “si et seulement si”

# Preuve d'équivalence

“A si et seulement si B”

## Exemple

- ▶ pour tout entier  $n$ ,  $n$  est pair si et seulement si  $n^2$  est pair
- ▶ égalité d'ensembles :  $\mathbb{Z}$  et  $\{-x \mid x \in \mathbb{Z}\}$  sont égaux

Deux méthodes :

- ▶ Méthode 1 : double implication

$$\frac{A \text{ implique } B \quad B \text{ implique } A}{A \text{ ssi } B}$$

- ▶ Méthode 2 : chaîne d'équivalences

$$\frac{A \text{ ssi } C \quad C \text{ ssi } B}{A \text{ ssi } B}$$

# Méthode 1 : double implication

“ $A$  si et seulement si  $B$ ”

1. montrer “ $A$  implique  $B$ ”
2. montrer “ $B$  implique  $A$ ”

## Exemple

“Pour tout entier  $n$ ,  $n$  est pair si et seulement si  $n^2$  est pair”

- ▶ “ $n$  est pair implique  $n^2$  est pair”
  
- ▶ “ $n^2$  est pair implique  $n$  est pair”

## 2.3 Preuve par disjonction de cas

# Preuve par disjonction de cas

**Méthode :** **découper** une preuve complexe en plusieurs **sous cas plus simples**

## Exemple

“le produit de deux entiers consécutifs est pair”

Soit  $n$  un entier quelconque :

- ▶ **Cas où  $n$  est pair :**
  
- ▶ **Cas où  $n$  est impair :**

## 2.4 Preuve par contradiction

# Preuve par contradiction

**Principe :** pour prouver une propriété  $A$ , on montre que si  $A$  est fausse, alors une propriété réputée fausse serait vraie

$$\frac{\text{non}(A) \text{ implique } \textit{false}}{A}$$

**Méthodologie :**

1. “On prouve  $A$  par contradiction”
2. “Supposons que  $A$  est fausse” (c’est à dire  $\text{non}(A)$  vraie)
3. Dédire une propriété réputée fausse (contradiction logique)
4. “Contradiction, donc  $A$  est nécessairement vraie”

# Un exemple de preuve par contradiction

## Exemple

“ $\sqrt{2}$  est irrationnel”

On montre cette propriété **par contradiction**.

**Supposons** que  $\sqrt{2}$  est rationnel.

**Contradiction :**

## 2.5 Conclusion

## À ne pas faire

- ▶ **Preuve par généralisation** : “Ça marche pour 17, donc ça marche pour tout nombre réel”
- ▶ **Preuve par intimidation** : “Trivial”
- ▶ **Preuve par épuisement** : 2 pages pour une preuve qui peut s'écrire en 5 lignes
- ▶ **Preuve par omission** : “Les 127 autres cas sont analogues”, “Le lecteur règlera facilement les détails”
- ▶ **Preuve par obscurcissement** : une longue suite incohérente d'assertions syntaxiquement proches, toutes vraies et/ou sans signification.
- ▶ **Preuve par fin de l'exposé** : “Vu l'heure, je laisserai la preuve de ce théorème en exercice”
- ▶ **Preuve par consensus** : “tous d'accord ?”
- ▶ **Preuve par démocratie** : “Que ceux qui sont d'accord lèvent la main”. À utiliser seulement si la preuve par consensus est impossible.

## Qu'est-ce qu'une bonne preuve ?

- ▶ **Objectif premier** : établir la véracité d'une proposition **avec certitude absolue**
- ▶ **Objectif second** : pour être compréhensible et utile, une preuve doit également être **claire** et **convaincante**
  - ▶ **Annoncer explicitement** le raisonnement suivi
  - ▶ **Une preuve est un discours, pas un calcul**, faites des phrases, avec quelques équations (pas l'inverse)
  - ▶ **Adopter une démarche linéaire**, les arguments doivent s'enchaîner logiquement
  - ▶ **Symboles et notations** doivent être introduits pour simplifier la lecture, et non pas la compliquer
  - ▶ **Structurer** les preuves longues à l'aide de lemmes intermédiaires
  - ▶ **Méfiez-vous de "trivial"**, ce n'est pas forcément le cas pour votre lecteur, ni toujours vrai
  - ▶ **Concluez** la preuve
  - ▶ **Relisez et simplifiez** jusqu'à obtenir un discours clair et bien structuré