

# Objectifs et preuves

Dédou

Février 2011

# On passe aux preuves

On a vu

les définitions et les énoncés.

Il nous reste à voir

les preuves.

Preuve et démonstration

c'est la même chose.

# Que prouve-t-on ?

## A la base

on veut prouver un énoncé.

## Au final

on doit prouver un énoncé  $E$  dans un contexte  $C$ .

C'est ça qu'on appelle un objectif.

## Définition

Un objectif, c'est un contexte muni d'un énoncé (bien défini dans ce contexte) qu'on appelle le but.

## Et même

on doit prouver une pile d'énoncés chacun dans son contexte.

## Autrement dit

on doit prouver une pile d'objectifs.

# Exemple d'objectif

## Exemple

$x : \mathbb{R}, y : \mathbb{R}, H : x < y \vdash x^3 < y^3$ .

Le symbole  $\vdash$  sépare le contexte du but ; il se lit “thèse”.

# Questions de validité I

Une condition nécessaire de validité :

pour que l'énoncé  $E$  soit bien défini (on dit aussi "valide") dans le contexte  $C$ , il faut au moins que toutes les variables libres dans  $E$  soient déclarées dans  $C$ .

Exemple

L'énoncé  $x = y + 2k\pi$  n'est pas valide dans le contexte  $x : \mathbb{R}, y : \mathbb{R}, Hc : \cos x = \cos y, Hs : \sin x = \sin y$ .

Exo 1

Corrigez l'énoncé ci-dessus pour qu'il devienne bien défini et même vrai dans le contexte donné.

## Questions de validité II

La condition nécessaire de validité qu'on vient de voir  
n'est pas suffisante.

C'est à cause des fonctions partielles.

### Exemple

Dans le contexte  $x : \mathbb{R}, H : x < 0$ , on n'a pas trop envie de dire que l'énoncé  $\ln x = \sqrt{x}$  est valide.

## Questions de validité III

En fait, le contexte spécifie un ensemble (l'ensemble des valeurs possibles pour les variables) sur lequel l'énoncé est une fonction (à valeurs dans Prop) qui doit être partout définie.

### Dans l'exemple

Dans le contexte  $x : \mathbb{R}, H : x < 0 \vdash \ln x = \sqrt{x}$ , le problème est que la fonction

$$x \mapsto \ln x = \sqrt{x}$$

n'est pas partout définie sur l'ensemble spécifié par le contexte, à savoir :

$$\{x : \mathbb{R} \mid x < 0\}.$$

# Prouver, c'est quoi ?

## Prouver une pile d'objectifs, c'est

- gérer cette pile
- en respectant les règles de gestion (dites **règles d'inférence**)
- jusqu'à ce que la pile soit vide.

## Au départ, on veut prouver un énoncé

- on en fait un objectif (avec le contexte vide)
- et on fait de cet objectif une pile à un élément.



# T'a plus qu'à..

## Y'a plus qu'à

comprendre les **règles d'inférence**, qu'on appelle aussi tactiques, autrement dit comprendre ce qu'on a le droit de faire pour améliorer la pile.

On va donner la liste des tactiques (règles de preuves).

En gros, une preuve d'un objectif  $O$ , c'est une liste de tactiques qui, appliquées l'une après l'autre, réduisent l'objectif initial à zéro objectif.

Quand on fait une preuve, on gère une pile d'objectifs.

- Au départ de la preuve d'un énoncé  $E$ , la pile contient un seul objectif, dont le contexte est vide, et le but est  $E$ .
- La preuve consiste à appliquer des tactiques à l'objectif courant, le premier de la pile.
- Chaque tactique modifie l'objectif courant, et éventuellement la pile.
- La preuve est finie quand la pile est vide.

# Que dire sur chaque tactique ?

## Pour chaque tactique, on va dire

- son sens
- à quels objectifs elle s'applique
- ses arguments éventuels
- comment elle transforme la pile d'objectifs
- si elle est "gratuite" ou non
- comment elle se rédige.