Un peu de logique

Métamathématiques

- la logique est présente *"depuis toujours"*

  syllogismes, ...
- début du 20è siècle: **programme de Hilbert**
  - formaliser les fondements des mathématiques
  - exprimer toutes les théories existantes à l'aide d'un ensemble *fini*, *complet* d'axiomes

    complet: tout énoncé mathématique vrai peut être prouvé dans le système
  - + prouver que les axiomes sont *consistants*

    le faux ne peut être dérivé
  - + *décidabilité*: donner un "algorithme" permettant d'accepter ou de refuser tout énoncé mathématique
  - + on rase gratis

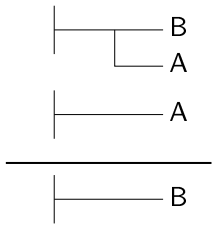
Formaliser le raisonnement mathématique

- on cherche à "systématiserprogrammer le raisonnement mathématique"

  trouver les lois élémentairesl'assembleur du raisonnement mathématique
- Boole: moitié du 19è siècle

  Analyse mathématique de la logique, *Les lois de la pensée*
- Frege

  Begriffsschrift, 1879



Gentzen, années 30: déduction naturelle

on écrit des séquents $\underbrace{A, B \to C, A \to D, (A \to B) \to C}_{\text{ensemble } \Gamma \text{ d'hypothèses}} \vdash B \to B$

$$\frac{}{\Gamma, AA \vdash A}\ \text{Ax}$$

$$\frac{\Gamma, AA \vdash B}{\Gamma \vdash A \to B}\ \to\text{-I} \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \to\text{-E}$$

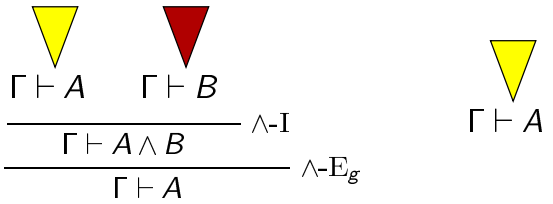
$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge\text{-I} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge\text{-E}_g \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge\text{-E}_d$$

La déduction

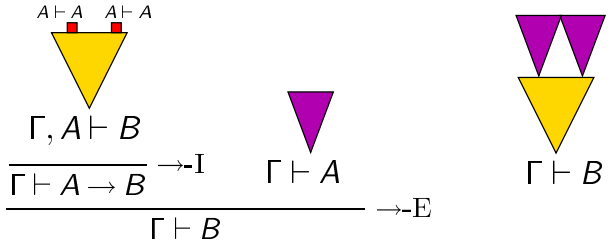
- le système de Gentzen est en fait né sous forme de *calcul des séquents* $\Gamma \vdash \Delta$
- d'ailleurs Hilbert avait proposé ça:
  - des axiomes
    - $\vdash A \to B \to A$
    - $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
  - une (seule) règle $\dfrac{\vdash A \to B \qquad \vdash A}{\vdash B}$ c'est pédestre...
- quoi qu'il en soit, on a un *objet syntaxique*, que peut-on dire dessus?
  - **complétude et correction** (vis-à-vis d'un modèle)
    ce qui est *vrai*, ce qui est *prouvable*
  - propriétés plus syntaxiques: on étudie les dérivations que l'on peut construire

La vie des preuves

- que peut-on dire de cette preuve de A?



- que peut-on dire de cette preuve de B?



- à chaque fois, introduction puis élimination: **coupure**

Hauptsatz

- rappel: complétude et correction
- les coupures, c'est les maths: lemme intermédiaire
  introduire une coupure, c'est inventer une étape de preuve
  (cf. transparent précédent)
- **élimination des coupures** (*Hauptsatz* de Gentzen)
  - si on peut déduire $\Gamma \vdash A$, alors il existe une preuve de $\Gamma \vdash A$ sans coupure *("simple"...)*
    même résultat, manières différentes d'y arriver
- corollaire: propriété de la sous-formule
  - si on peut déduire $\Gamma \vdash A$, alors il existe une preuve de ceci où l'on n'utilise que des sous-formules de Γ et A
    ça "restreint l'espace de recherche de preuves"

Consistance

- **non contradiction**
  on ne peut construire une preuve du séquent $\vdash A \wedge \neg A$
- oui mais c'est quoi $\neg A$?
  - on introduit $\bot$ (le faux), avec uniquement
    $$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$
    et on dit que $\neg A$, c'est une notation pour $A \to \bot$
  - ou alors on travaille avec des séquents à une ou zéro conclusions
    $$\frac{\Gamma \vdash A}{\Gamma, \neg A \vdash} \qquad \frac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$$
- preuve: corollaire de la Hauptsatz
  s'il y a une dérivation de $\vdash A \wedge \neg A$, alors il y a une dérivation de $\vdash \bot$ (ou de $\vdash$), donc il y en a une dérivation sans coupure, impossible car aucune règle ne s'applique

Elimination des coupures

- rappel:

$$\dfrac{\dfrac{\dfrac{D}{\Gamma, \phi \vdash \psi}}{\Gamma \vdash \phi \to \psi} \quad \dfrac{D'}{\Gamma \vdash \phi}}{\Gamma \vdash \psi} \qquad \text{devient} \qquad \dfrac{D''}{\Gamma \vdash \psi}$$

où D'' s'obtient en remplaçant dans D les utilisations de ϕ par D'

- λ-calcul
  - syntaxe:

$$M \quad ::= \lambda x.\, M \mid M\, M' \mid x$$

  - règle de calcul: la β-réduction

$$(\lambda x.\, M)\; M' \quad \to \quad M[M'/x]$$

λ-calcul simplement typé et preuves

- règles de typage du λ-calcul simplement typé (uniquement $\to$)

$$\dfrac{}{\Gamma, x : A \vdash x : A} \qquad \dfrac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x.\, M : A \to B}$$

$$\dfrac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash M' : A}{\Gamma \vdash (M\, M') : B}$$

dans ce cas les Γ sont des $x : A, y : B \to C, \ldots$

- à chaque fois qu'on écrit une preuve d'un séquent $\Gamma \vdash A$, on peut écrire le typage d'un terme du λ-calcul M tel que $\Gamma \vdash M : A$

  et inversement

- le λ-calcul peut être vu comme une syntaxe pour les preuves en déduction naturelle

Correspondance de Curry-Howard

- Church: λ-calcul dans les années 30, comme une théorie logique
- rapidement, c'est devenu un *modèle de calcul* (cf. machine de Turing)
  - langages de programmation fonctionnelle (1960: LISP)
- Curry Howard De Bruijn observent (années 60) les correspondances suivantes

logique	programmation
preuve	programme fonctionnel
formule	type
élimination des coupures	β-réduction
preuve sans coupure	valeur

  - écrire un programme, c'est décrire une preuve
  - exécuter un programme, c'est simplifier une preuve
  - le λ-calcul simplement typé

Correspondance preuves/programmes

$$\dfrac{}{\Gamma, A \vdash A}\,\text{Ax} \qquad \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,{\to}\text{-I} \qquad \dfrac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,{\to}\text{-E}$$

$$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,{\wedge}\text{-I} \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,{\wedge}\text{-E}_g \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,{\wedge}\text{-E}_d$$

- il n'est pas difficile de rajouter des couples au λ-calcul pour "être en face" de la déduction naturelle ($\pi_l\langle M, M'\rangle \to M, \ldots$)
- ajouter la disjonction?

$$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,{\vee}\text{-I}_g \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,{\vee}\text{-I}_d$$

$$\dfrac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,{\vee}\text{-E}$$

  - et côté λ-calcul? types somme

Quelle logique?

- à chaque fois qu'on construit une preuve, on lui associe un *témoin* (le λ-terme) correspondant à cette preuve
  - en particulier, une preuve de $A \vee B$ est soit une preuve de A, soit une preuve de B
- on ne peut dériver le tiers exclu $\quad \vdash A \vee \neg A$
- au λ-calcul simplement typé correspond la logique intuitionniste
  - en logique classique, on peut prouver l'existence d'un objet en montrant une contradiction à partir de sa non existence
  - ici les preuves peuvent être plus complexes
  - mais une preuve peut être transformée en un algorithme

Aparté: SKI

- Hilbert travaillait avec les axiomes
  $\vdash A \to B \to A \qquad$ et
  $\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- trois termes du λ-calcul:
  - $I = \lambda x.\, x$
  - $K = \lambda x.\, \lambda y.\, x$
  - $S = \lambda x \lambda y \lambda z.\, ((x\, z)\, (y\, z))$
- exercices: que fait SII? et SKK?
- le système comprenant les deux axiomes de Hilbert + le *modus ponens* (qui représente l'application) est *complet* pour la logique intuitionniste

  tout cela en version typée

Un calcul, une logique

- λ-calcul simplement typé: logique intuitionniste (pas de tiers exclu)
- enrichissements
  - systèmes de types plus riches, jusqu'au *Calcul des Constructions* (T. Coquand)
    système d'aide à la preuve Coq: développement interactif de preuves
    - on énonce un résultat (on donne un type)
    - on construit la preuve (le λ-terme)
      (ainsi, λ c'est "supposons que...")
    - on extrait un programme de la preuve

    Coq est (plus ou moins) un λ-calcul avec un système de types très riche

    au passage, le λ-calcul simplement typé est terminant, et Coq aussi
    élimination des coupures
  - λ-calcul étendus
    - continuations: logique classique
    - au-delà: J.-L. Krivine,...

Résultat des courses

Hilbert a perdu (Gödel)