



Une histoire de la logique mathématique: de la philosophie à l'informatique

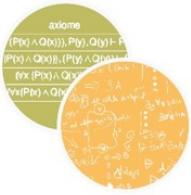
Christian Retoré

Professeur, Université de Montpellier



Les fondamentaux de la logique

La logique mathématique, de la philosophie à l'informatique



La logique est elle sulfureuse?

Lucifero: "Forse tu non pensavi ch'io LOICO fossi. Dante Alighieri (1265-1321) Comedia, Inferno XXVII



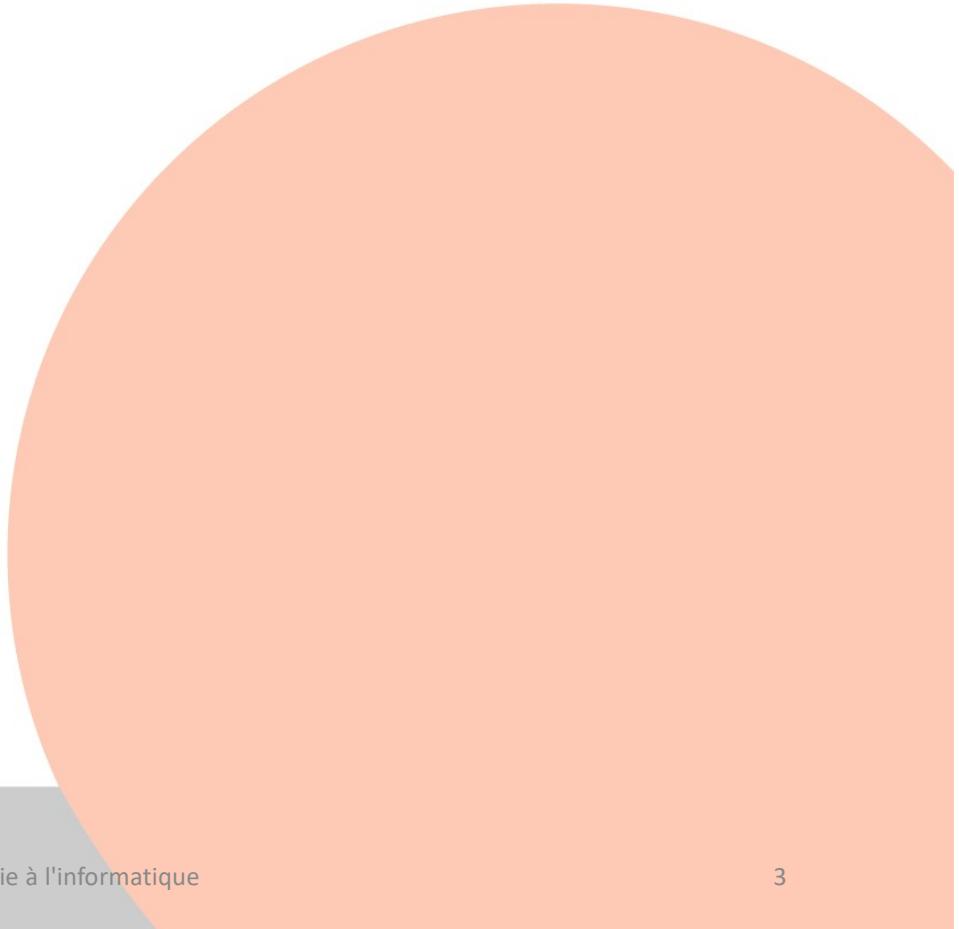
Une traduction pourrait être: "*sans doute ne savais tu pas que j'étais aussi bon logicien*".





La logique

- *En tout cas, en France, la logique est peu enseignée:*
 - *Philosophie?*
 - *Mathématiques?*
 - *Informatique?*
 - *Linguistique (sémantique) et philosophie du langage?*





Avant la logique « moderne »

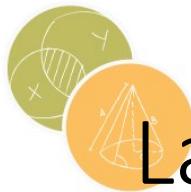
Aristote

L'antiquité après Aristote

Le Moyen-Âge et la scolastique

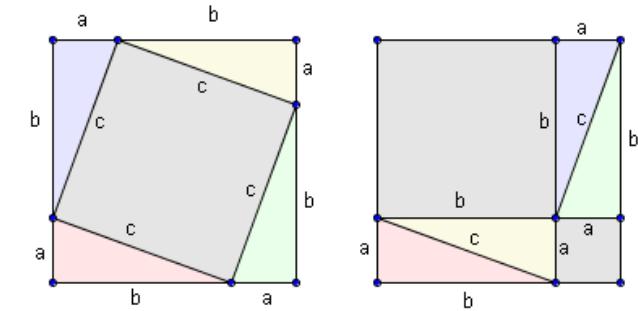
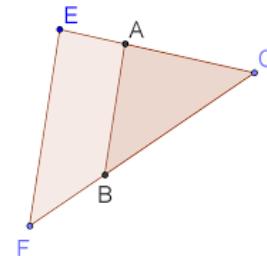
La logique algébrique (XVIIe XVIIIe XIXe)

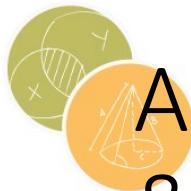




La logique

- Art de raisonner correctement
- Avec la rigueur des raisonnements mathématiques (Thalès, Pythagore,... VIIe siècle av. J.C)
- Dériver correctement des énoncés ...mais à partir de quels axiomes?
- Etude de la vérité dans une situation particulière, mais cela est plus récent.





Aristote (III av JC) l'antiquité & la scolastique (moyen âge)



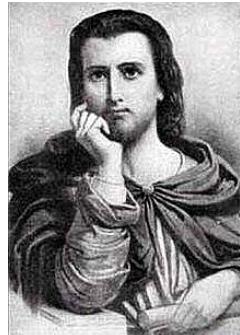
- Certains types d'énoncés:
 - A Tout A est B
 - E Certains A sont B
 - I Aucun A est B
 - O Tous les A ne sont pas B.
(ou Certains A ne sont pas B,
mais le **thème** est différent)





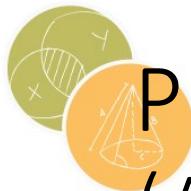
La scolastique (Antiquité et Moyen-Âge)

- Les fameux syllogismes (règles de déduction)
- Barbara :
 - *tout M est P,*
 - *or tout S est M,*
 - *donc tout S est P;*
- Baroco :
 - *tout P est M,*
 - *or quelque S n'est pas M,*
 - *donc quelque S n'est pas P*



Pierre Abélard
(1079-1142)





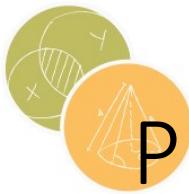
Principes (Aristote, Avicenne)



Avicenne ibn Sina (980-1037)

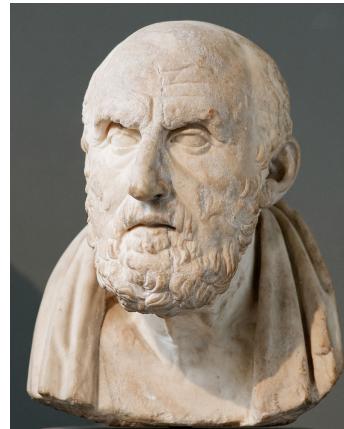
- Identité: Tout A est A
- Non contradiction NON (G et NON G)
"Tout personne niant le principe de non contradiction devrait être battue et brûlée jusqu'à ce qu'elle admette qu'être battu n'est pas la même chose que ne pas être battu, et qu'être brûlé n'est pas la même chose que ne pas être brûlé" Avicenne (980-1037) en réponse à des religieux souhaitant accommoder ce principe.
- Tiers exclus: pour tout énoncé G on a (G ou NON G) (**tertium non datur**)





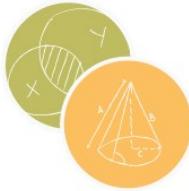
Principes (Stoïciens)

- Stoïciens (calcul propositionnel)
- Modus ponens:
 - Si A alors B
 - Or A
 - Donc B.
- Modus tollens:
 - Si A alors B.
 - Or NON B.
 - Donc NON A.
- **Ex falso quodlibet sequitur**



Chrysippe de Soles
logicien stoïcien
(280—206 av. JC, Anatolie).

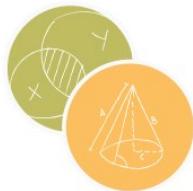




Place de la logique en philosophie

- A étudier en premier pour raisonner correctement
(Organon, Catégories,...)
- « *Celui qui souhaite atteindre la perfection humaine doit d'abord étudier la logique, puis les diverses branches des mathématiques dans l'ordre qui convient, puis la physique et enfin la métaphysique.* »
(Maimonides, XIIe)

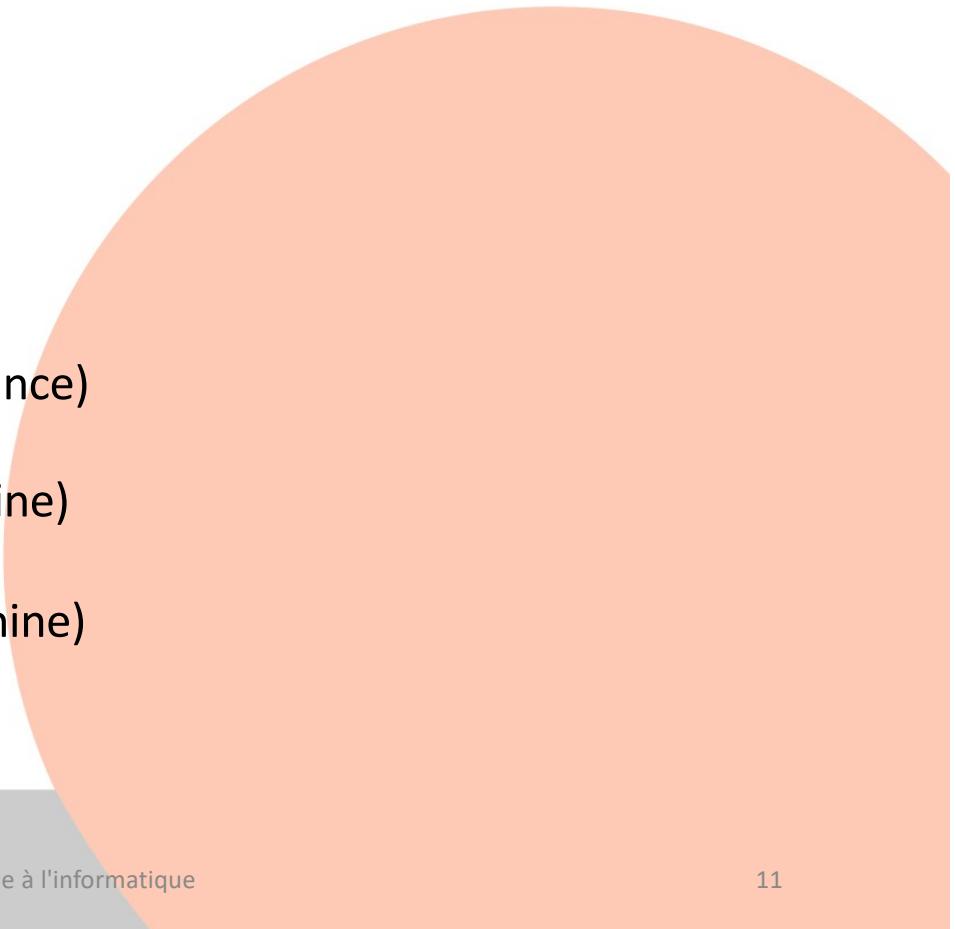




Logique algébrique Leibnitz et ses successeurs Boole, De Morgan, Pierce



- Précurseur: Leibniz (1646-1716)
- Lois et calculs
- Calcul propositionnel: tables de vérité
 - $X \rightarrow \text{VRAI}$: VRAI
(Si Rome est en Chine alors Paris est en France)
 - $\text{FAUX} \rightarrow X$: VRAI
(Si Rome est en Chine alors Paris est en Chine)
 - $\text{VRAI} \rightarrow \text{FAUX}$: FAUX
(si Paris est en France alors Rome est en Chine)





Logique algébrique anglo-américaine Boole, De Morgan, Pierce (XIXe)

- Pour les prédictats des règles parfois fausses

$$\forall x[I(x) \rightarrow (F(x) \vee M(x))]$$

\Leftrightarrow

$$\forall x(I(x) \rightarrow F(x)) \text{ ou } \forall x(I(x) \rightarrow M(x))$$

pensez à I=Individu F= femme M=homme ...





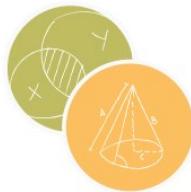
Le XXe siècle

La crise des fondements des mathématiques

Les débuts de la logique mathématique

La logique du premier ordre

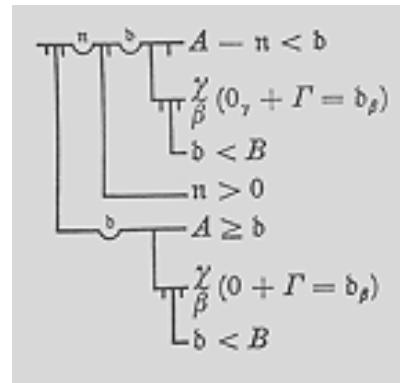




Calcul des prédictats (formules quantifiées)

Gottlob Frege (1848-1925)

- Formules avec des variables,
- Sur lesquelles on peut quantifier
- Incluent strictement les énoncés A E I O d'Aristote
- *Tout entier est la somme de quatre carrés:*
pour tout n il existe a b c et d tels que n=a²+b²+c²+d²
- Idéographie: notation pour les formules et les preuves





Formalisation des quantificateurs (Frege)

- Tout x est P : noté $(x) P(x)$ puis $\forall x P(x)$
« tout », « tous les », « chaque »
(et même « un »: « *un homme averti en vaut deux* »)
- Au moins un x est P : noté $\exists x P(x)$ puis
« certains » « quelques » « des » « un »
- Problème de formulation: pluriel / singulier
A-t-elle des enfants? Oui, deux. Oui, un.
Non, un.
A-t-elle un diplôme de maths? Oui, un.
Oui, Deux. # Non, deux.





Frege, Hilbert: les quantificateurs des mathématiques usuelles

- Une seule sorte d'individus:

- Tout A est B:

Pour tout X, SI X est A ALORS X est B
 $\forall X (A(X) \rightarrow B(X))$

- Certains A sont B:

Il existe X, tel X est A ET X est B.
 $\exists X (A(X) \text{ ET } B(X))$

$\exists X \forall Y P(X,Y)$ # $\forall X \exists Y P(X,Y)$





Règles de déduction Gottlob Frege (1848-1925) David Hilbert (1862-1943), Jacques Herbrand (1908-1931)

- **SI** on a établi $P(x)$ (sans rien supposer sur x)
ALORS on a $\forall x P(x)$ sous les mêmes hypothèses
(règle de généralisation ou d'abstraction
formalisation de Aristote)
- **SI** on a établit $\forall x P(x)$
ALORS on a $P(t)$ pour tout terme particulier





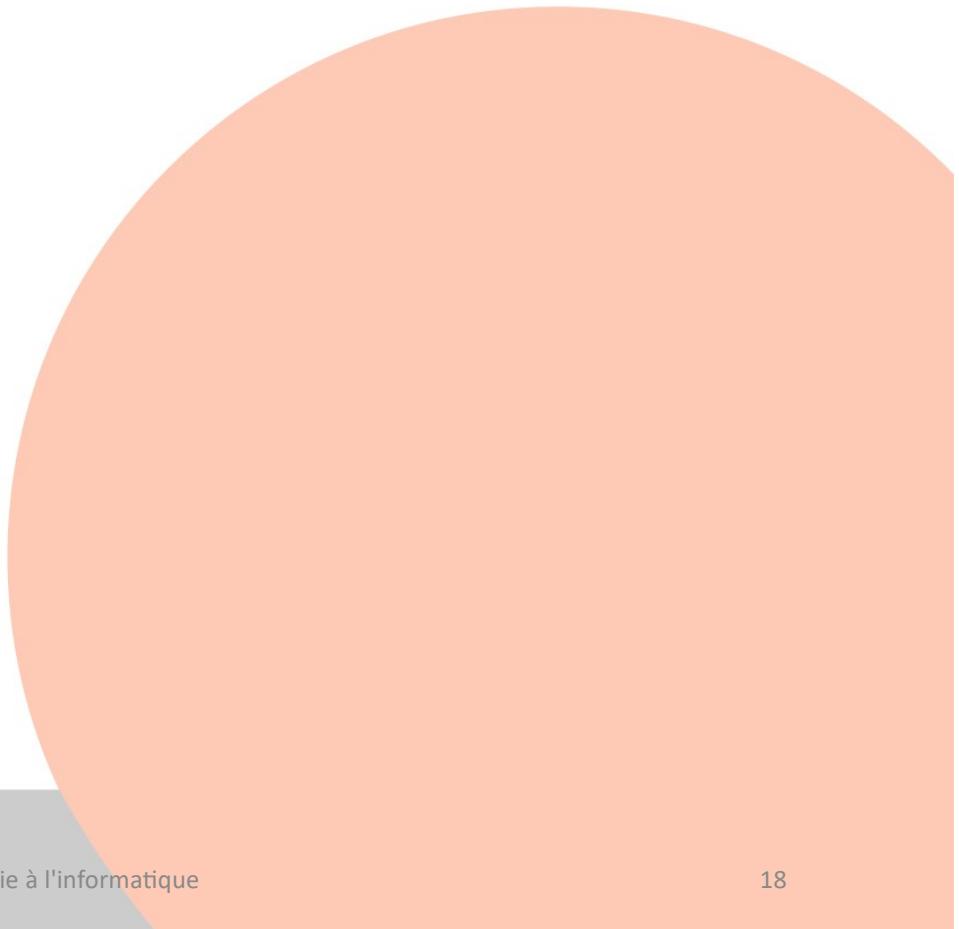
Frege, Hilbert, Herbrand,...

Règles de la quantification existentielle



Herbrand à 23 ans,
peu avant son fatal
accident d'alpinisme.

- SI on a établi $P(t)$ pour un terme particulier,
ALORS on a établi $\exists x P(x)$
- SI $P(x)$ (avec x quelconque) suffit pour obtenir A
ALORS $\exists x P(x)$ suffit pour obtenir A.

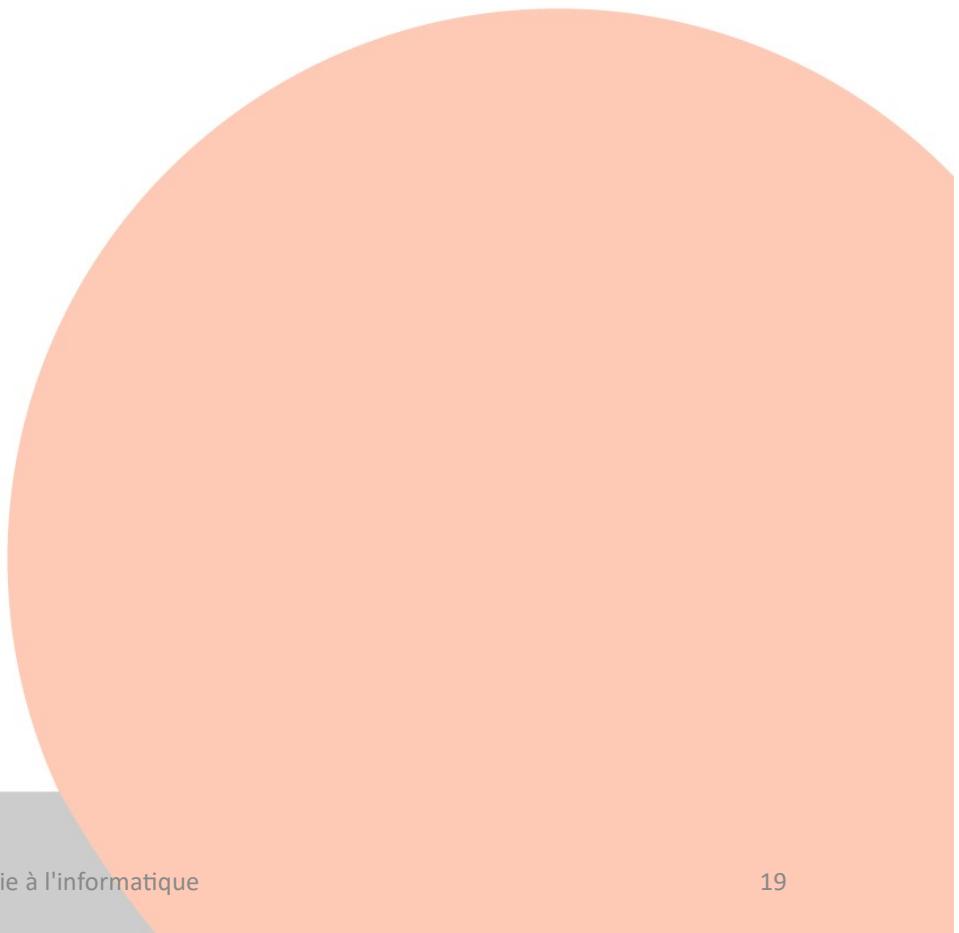


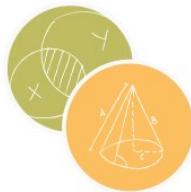


Vérité dans un modèle

Préambule: le calcul propositionnel (1/2)

- Suite des travaux de Boole (XIXe)
- Une interprétation:
 - On fixe la valeur, vrai ou faux de chaque proposition élémentaire
 - On en déduit la valeur dans cette interprétation des propositions complexes par les tables de vérités



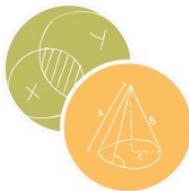


Vérité dans un modèle

Préambule: le calcul propositionnel (2/2)

- Validité:
 - Une proposition dérivable
(par exemple $p \rightarrow p$)
vaut vrai dans toute interprétation
- Plus tard: Complétude (1926):
 - Si une proposition vaut vrai dans toute interprétation, alors elle est dérivable
(Bernays, 1988-1977)

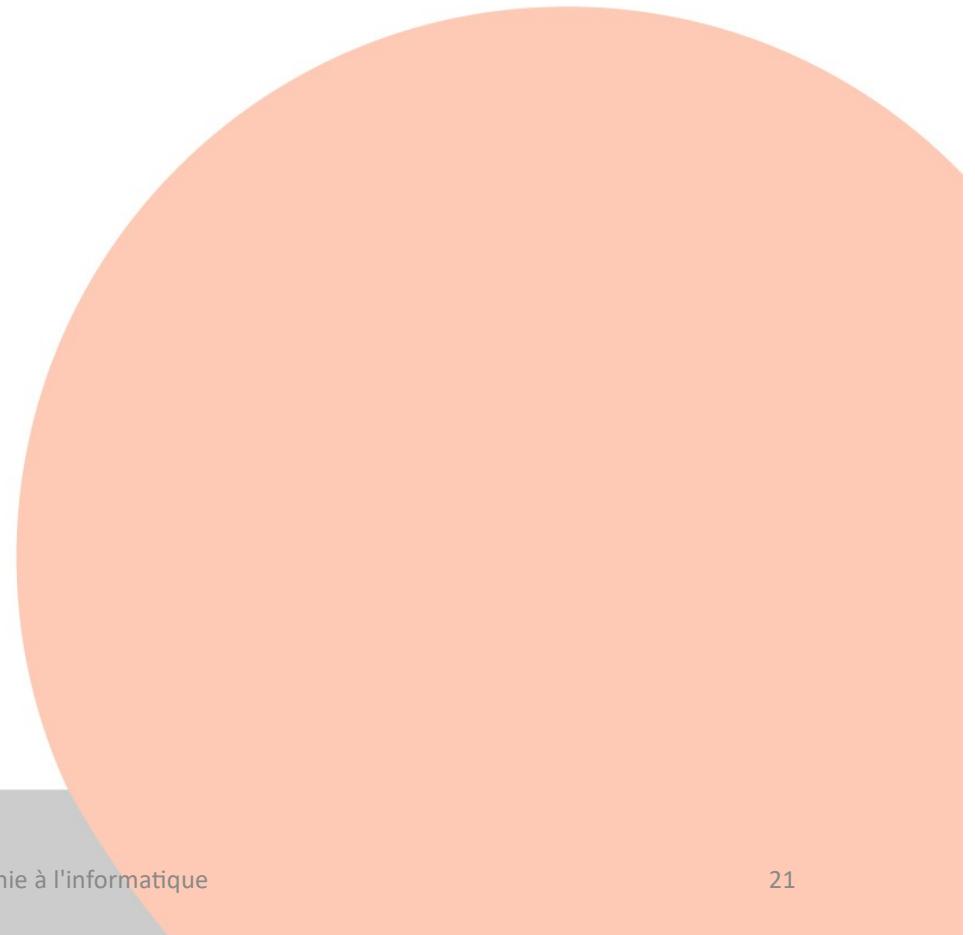




Calcul des prédictats: vérité dans un modèle 1/3

Leopold Löwenheim (1878-1957)

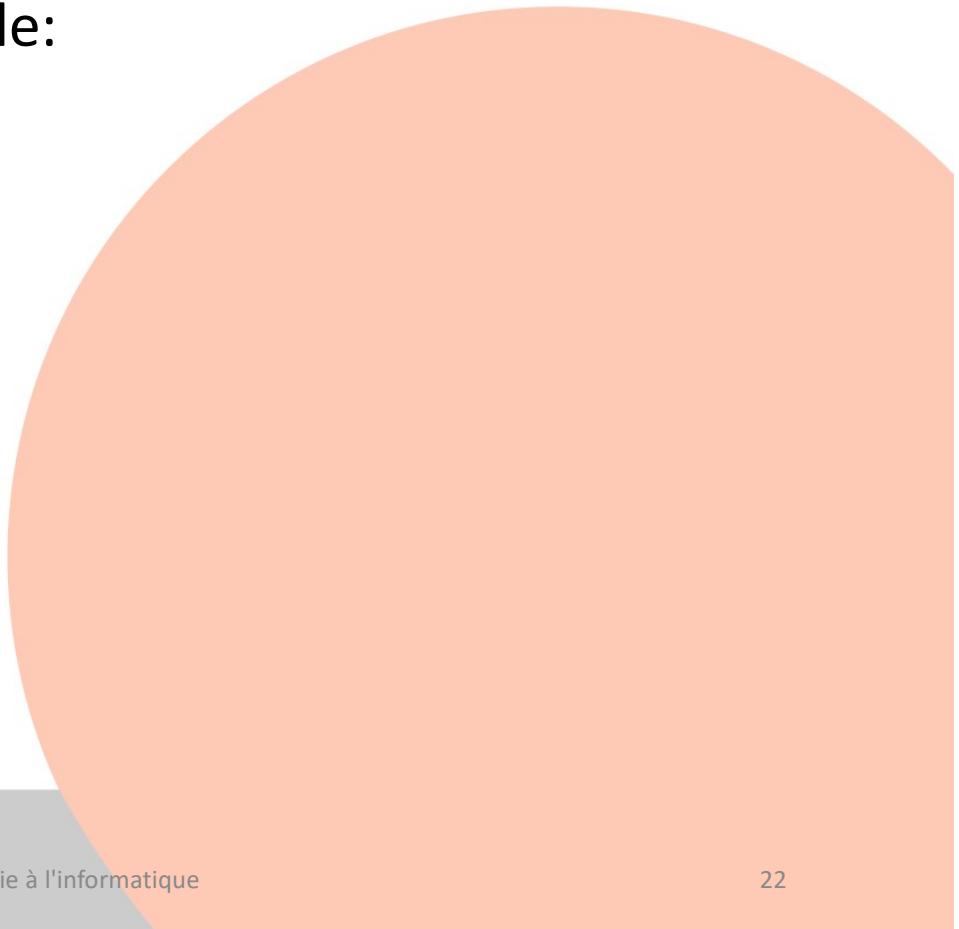
- La même chose, en plus compliqué:
 - Ensemble (domaine) par exemple les gens, les nombres, ...
 - Interprétation des constantes, des relations, ...
 - Dort: ensemble de personnes
 - Connaît: ensemble de couples de personnes
 - On peut vérifier dans un modèle donné que, par exemple:
 - Pour tout x il existe y , x connaît y et y dort;





calcul des prédictats vérité dans un modèle 2/3

- Il y a des formules vraies dans TOUT modèle:
 - SI il existe x tel que pour tout y
 x soit en relation R avec y
ALORS pour tout y il existe un x
tel que x soit dans la relation R avec y
 - C'est-à-dire $\exists x \forall y R(x,y) \Rightarrow \forall y \exists x R(x,y)$



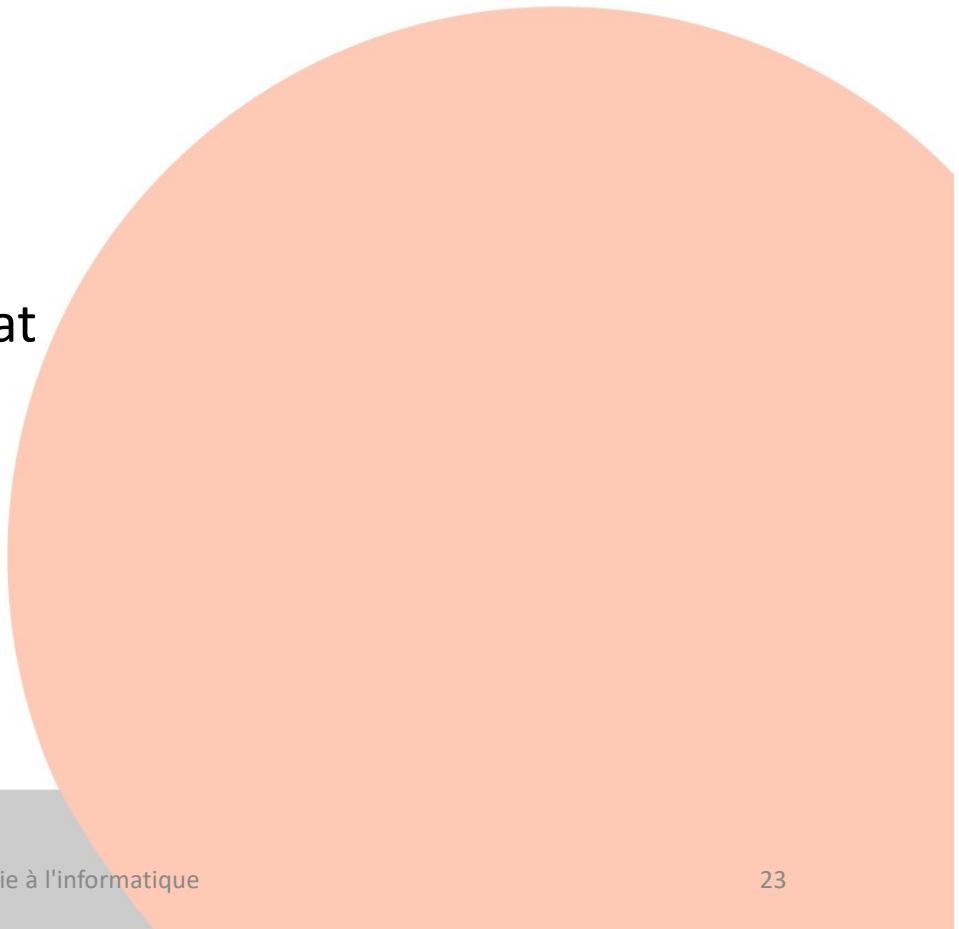


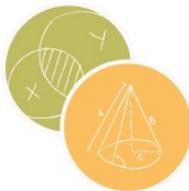
Calcul des prédictats vérité dans un modèle 3/3

- Validité: Toute formule démontrable formellement est vraie dans tout modèle.,.
- **Complétude (Gödel, 1929) :**
Toute formule vraie dans tout modèle est formellement démontrable:
nous montrerons à la fin de ce cours ce résultat qui relie preuves et modèles.



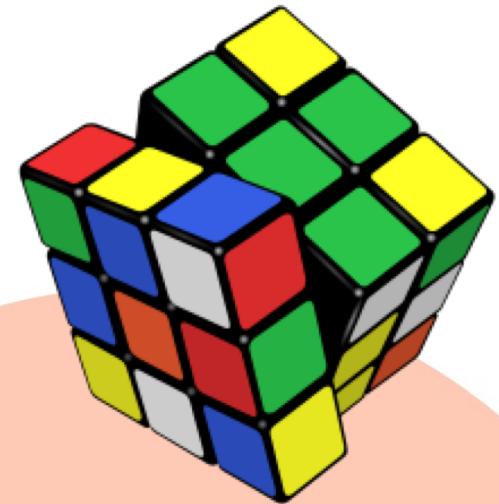
Cet énoncé dont la signification était peu claire à l'époque découle aussi des travaux de 1923 de Thoralf Skolem (1887-1963), ci-contre, comme Gödel l'avait remarqué.





Exemple de modèle

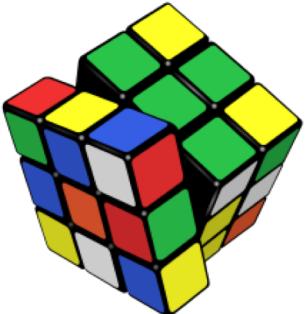
- Un groupe est un ensemble doté d'une opération binaire $*$ satisfaisant:
 - $\forall x \forall y \forall z. (x * y) * z = x * (y * z)$ [$*$ associative]
 - $\exists e. x * e = x$ et $e * x = x$ [il y a un élément neutre]
 - $\forall x \exists y x * y = e$ et $y * x = e$ [tout élément a un inverse]
- Exemple de groupes:
 - les rotations du plan,
 - les permutations d'un ensemble,
 - les entiers relatifs avec l'addition,
 - les transformations du Rubik's cube ...
- Les axiomes de groupes sont vrais dans tout groupe.



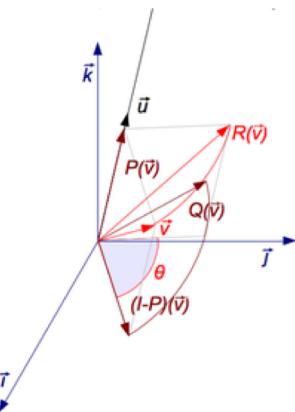


Sens du théorème de complétude

- Une propriété est **vraie dans tous les groupes** si et seulement si cette propriété est **démontrable à partir des axiomes de groupe**.
- Le **théorème de complétude résultat central** de ce cours relie modèles et preuves.



+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

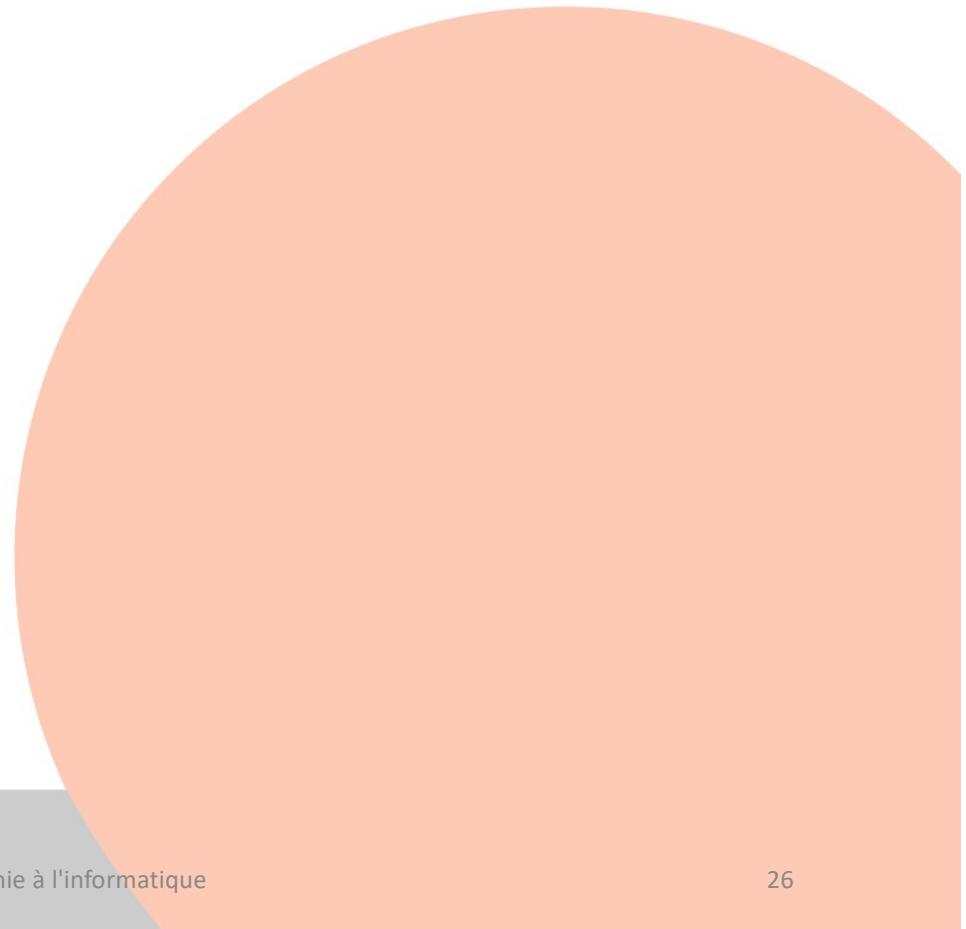
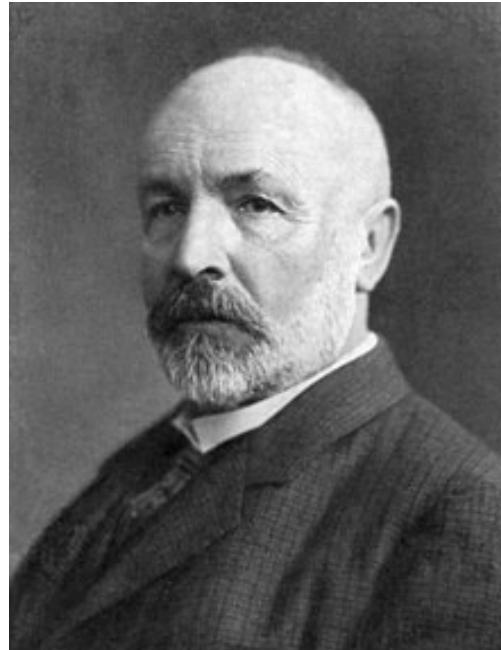




Fondements des mathématiques

Georg Cantor (1845-1918)

- Logique ... Ensembles?
Fondements des mathématiques
Ensemble: base d'un modèle
- Infinis, plusieurs sortes de nombres:
Ordinaux, Cardinaux
- Il y a plusieurs sortes d'infinis
certains infinis sont « beaucoup » plus grands que d'autres infinis.

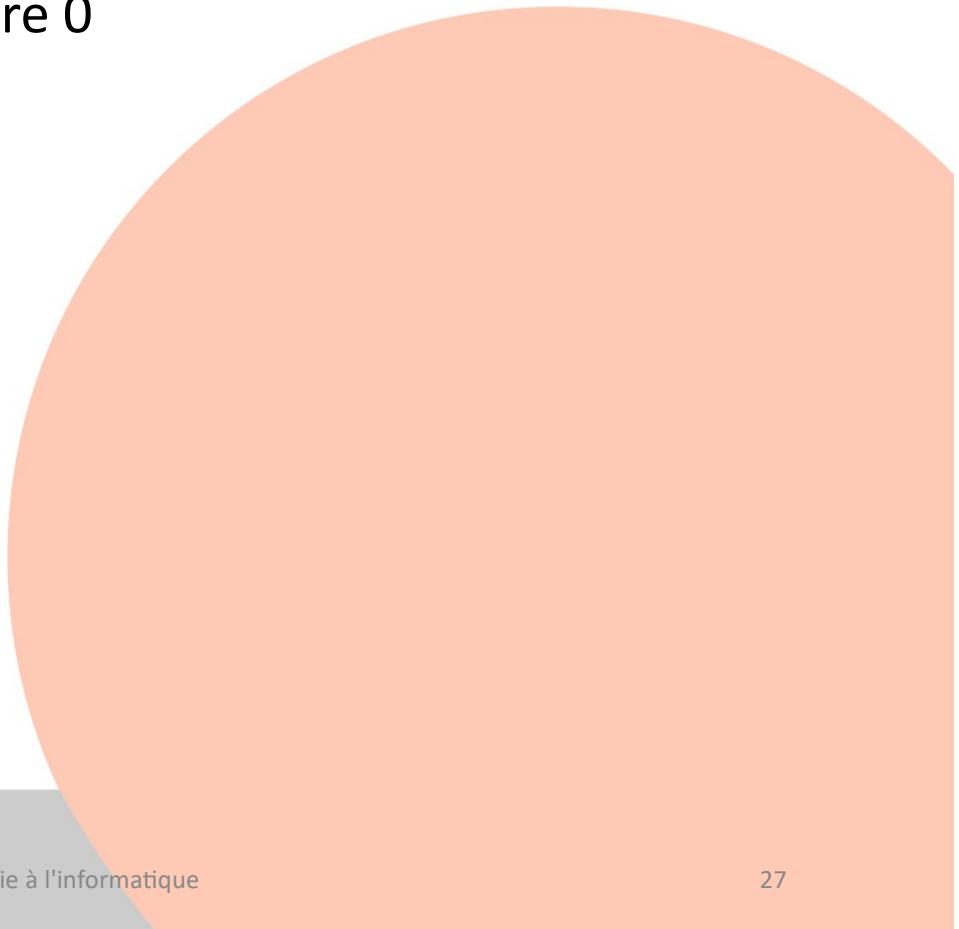




il y a plus de nombres réels que d'entiers

Georg Cantor (1845-1918)

- Si nous avions une liste des nombres réels entre 0 et 1 (développements décimaux infinis, sans 999999...)
 1. 0,5786086346780965431346789098764666...
 2. 0,8861453781936528901766189918714428...
 3. 0,86235038947294745484946849947452...
 4. 0,5618903412252820282534176444510186...
- 0,6939....
($n^{\text{ième}}$ chiffre $\neq n^{\text{ième}}$ chiffre du $n^{\text{ième}}$ nombre)
- 0,6939... n'est pas dans la liste!!!
- Contradiction, donc il n'y a pas de telle liste.
Il y a plus de réels que d'entiers

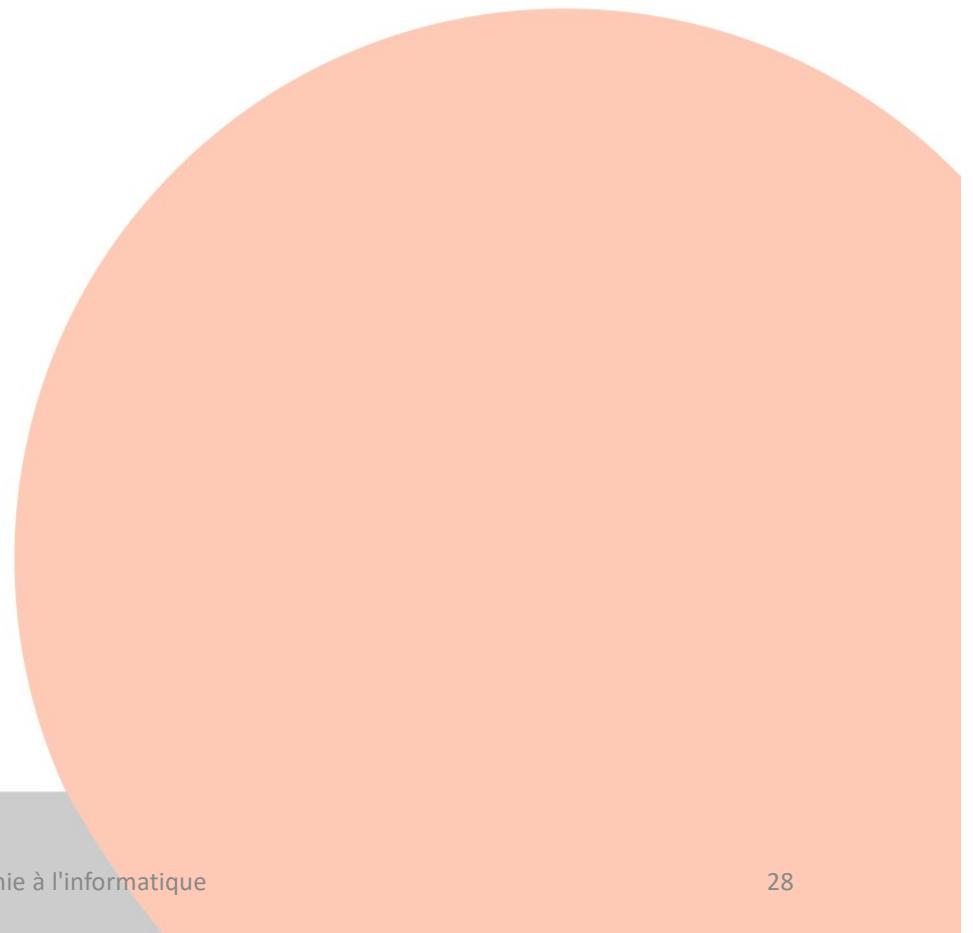




Giuseppe Peano (1858-1932)

Axiomatisation de l'arithmétique

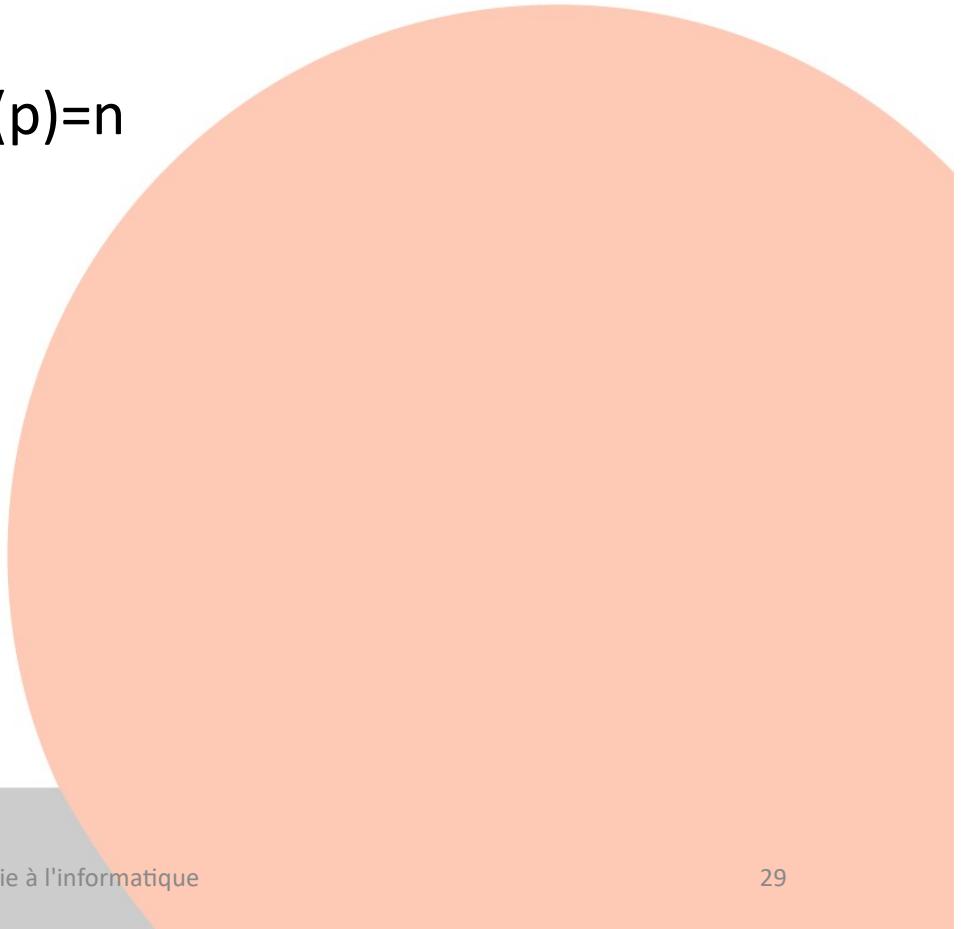
- Esperanto
mathématique ...
- Arithmétique:
symboles:
 - 0 (zéro)
 - fonction S: successeur
(l'entier suivant)
 - + (addition)
 - x (multiplication)

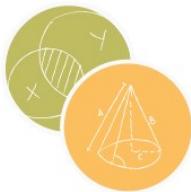




Axiomes de l'arithmétique

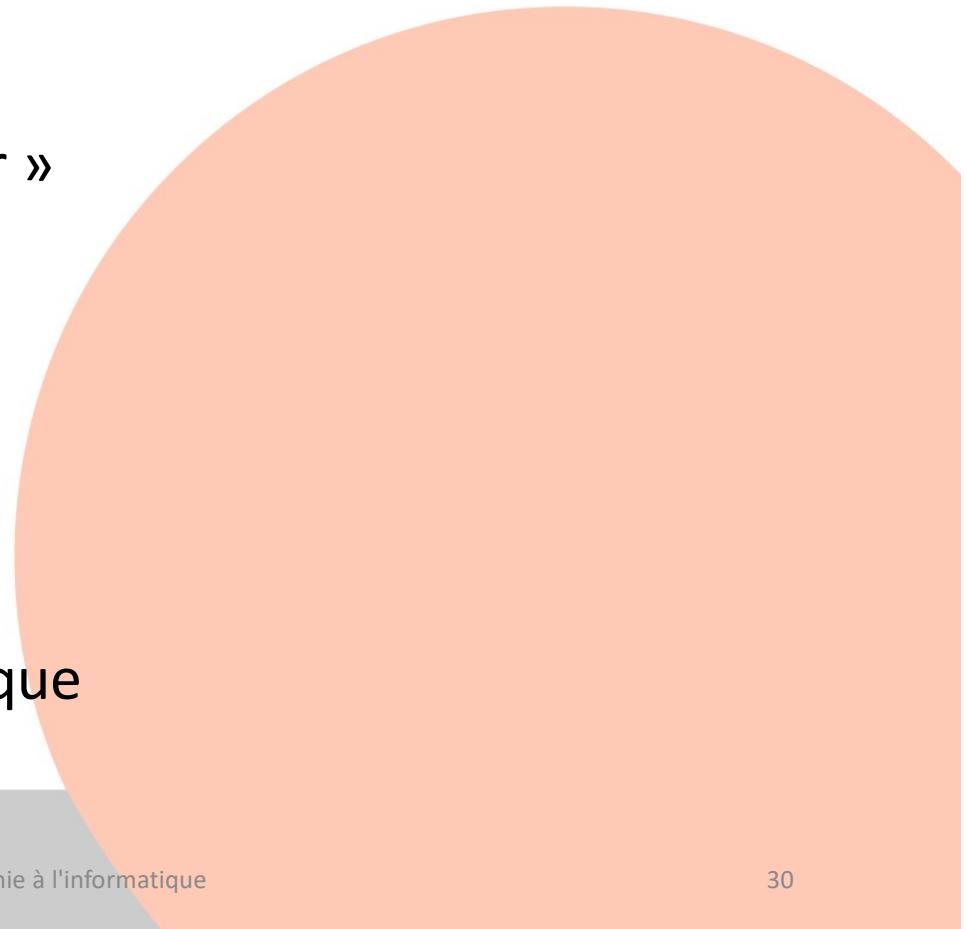
- $\forall n \quad S(n) \neq n$
- $\forall n \quad$ si $n \neq 0$ alors il existe p tel que $S(p) = n$
- $\forall n \forall p \quad$ si $S(n) = S(p)$ alors $n = p$
- $\forall n \quad n + 0 = n$
- $\forall n \forall p \quad n + S(p) = S(n + p)$
- $\forall n \quad n \times 0 = 0$
- $\forall n \forall p \quad n \times S(p) = (n \times p) + n$

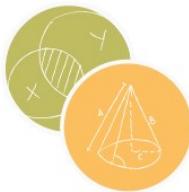




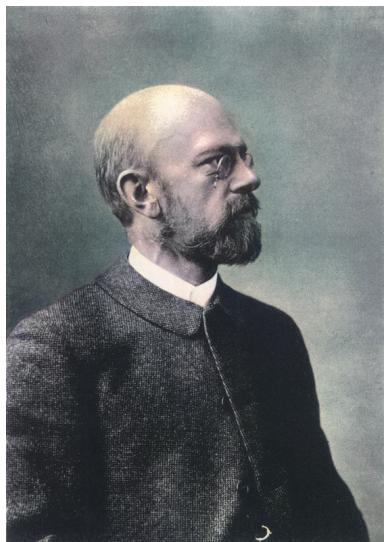
... ainsi que le schéma d'axiomes de récurrence!

- Récurrence:
pour établir que
« la propriété $P(\dots)$ est vraie de tout entier »
- il suffit de
 - Montrer qu'elle est vraie de 0
 - Montrer qu'elle passe au successeur:
si $P(n)$ alors $P(S(n))$ — avec $S(n)=n+1$.
- C'est un **schéma** d'axiome:
il faut UN axiome
pour CHAQUE formule $P(_)$ de l'arithmétique

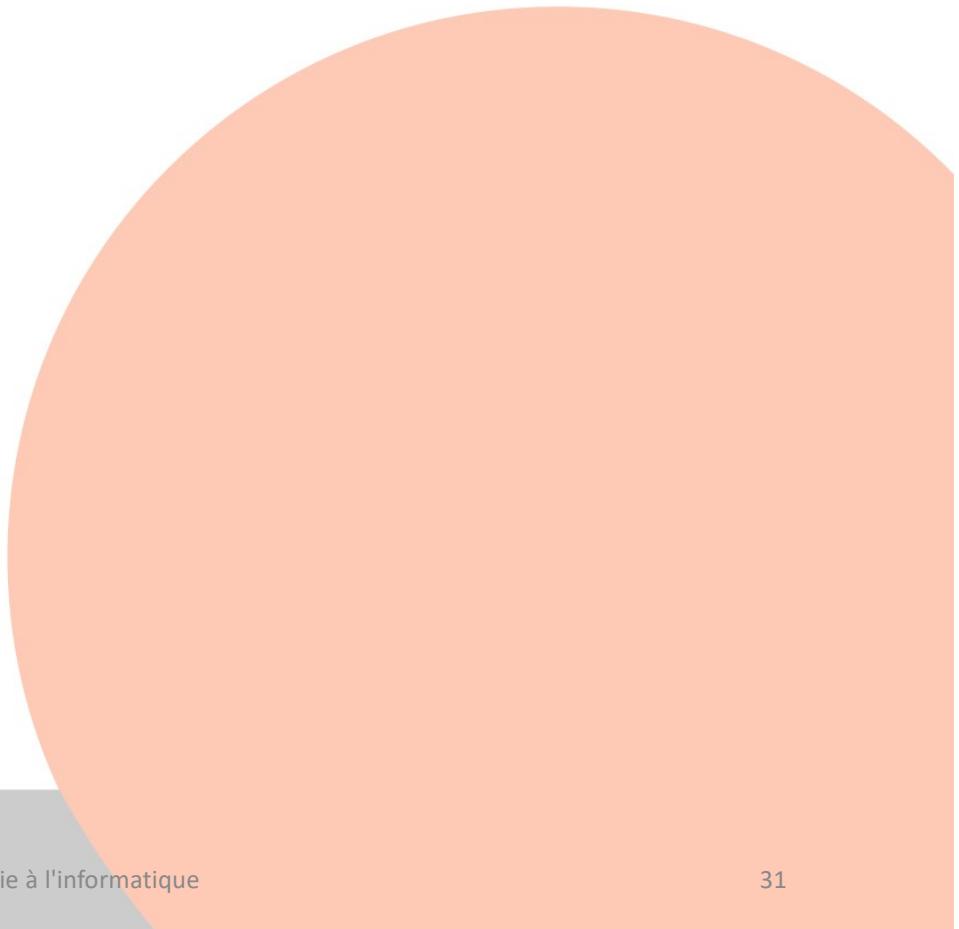


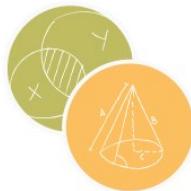


David Hilbert (1862-1943) et le programme éponyme (1900)



- En 1900 à Paris 23 problèmes majeurs
- Programme de fondements des mathématiques:
 - Etablir la cohérence des mathématiques
 - Un langage et une axiomatique minimales



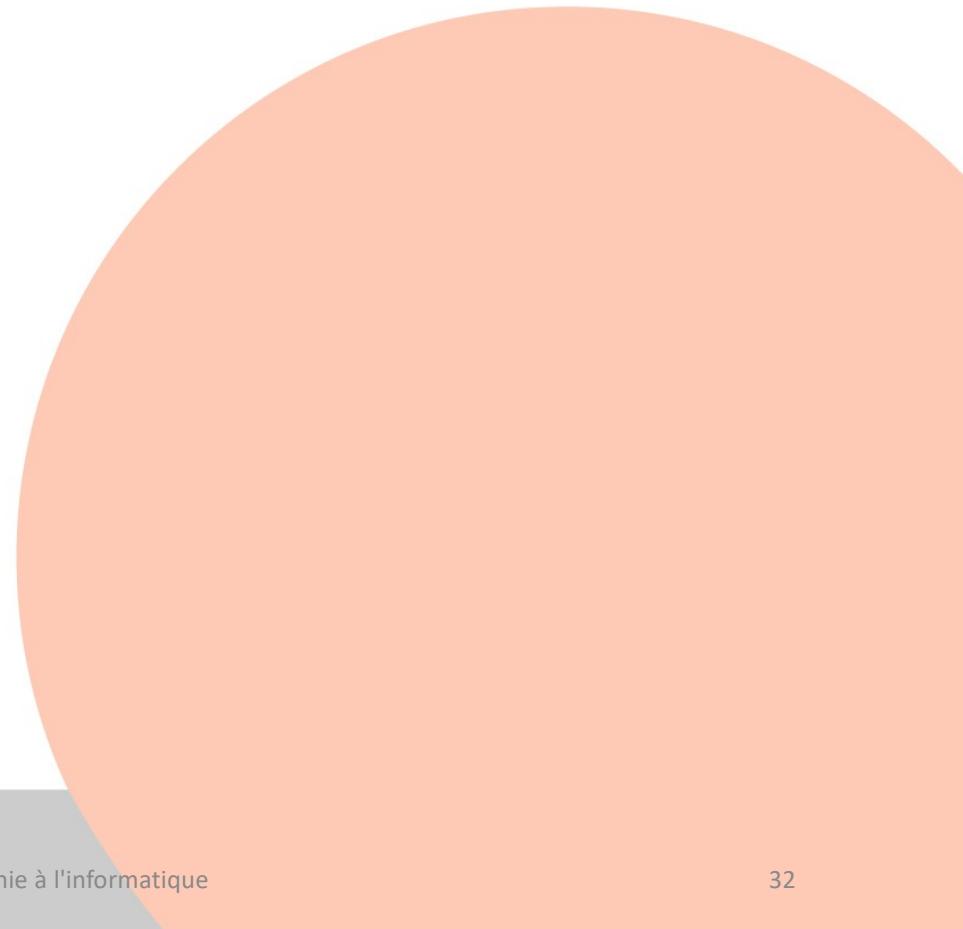


David Hilbert (1862-1943) et son programme: les preuves formelles à l'honneur

Montrer en raisonnant sur les preuves
(de manière finitaire) que

les axiomes
ne conduisent jamais
à une proposition fausse
(par ex. $0=1$)

par les règles
de déduction formelle

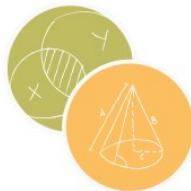




Bertrand Russell (1872-1970)

- *Principia mathematica* (1910-1913)
avec Whitehead formalisation/
axiomatisation purement logique des
mathématiques
 - L'entier 2 arrive après 200 pages...
- Paradoxe de Russell:
 - $U = \{X / X \notin X\}$
 - $U \in U ?$
 - $U \notin U ?$
 - Schéma de compréhension
restreint.





Théorie axiomatique des ensembles

Zermelo (1871-1953) puis Fraenkel (1891-1965)

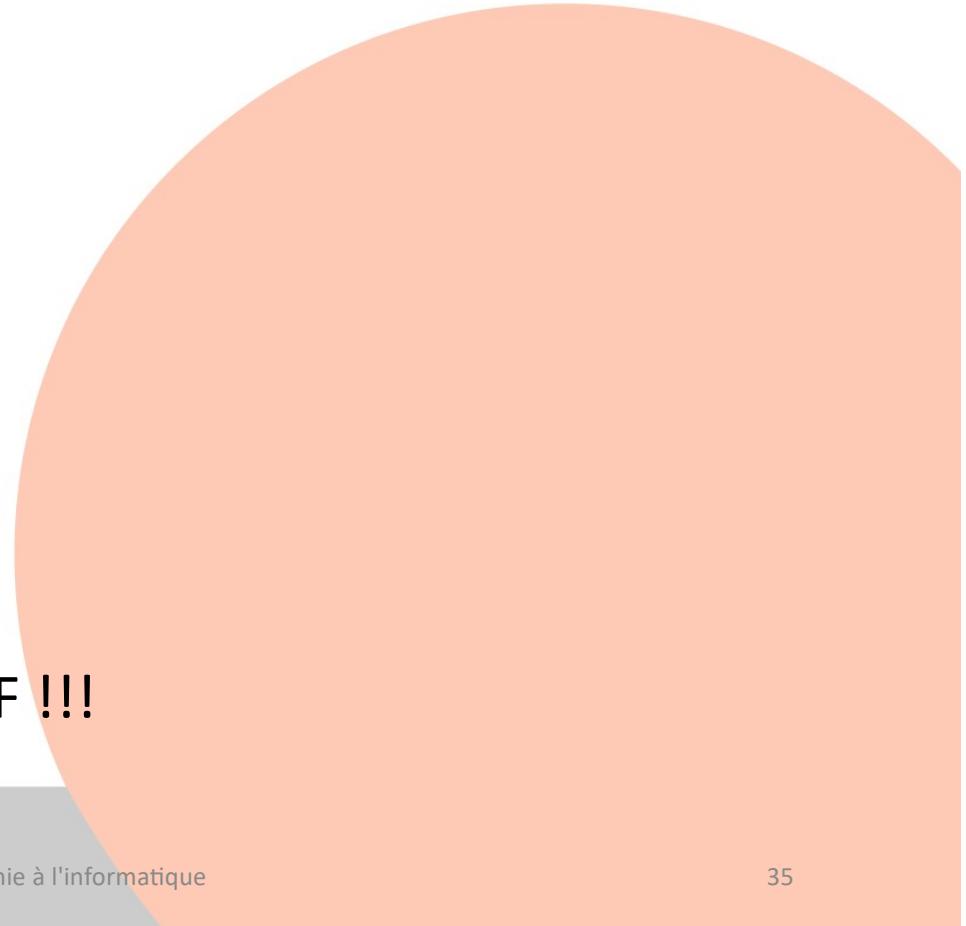
- 1 seul symbole: $X \in Y$ (X appartient à Y) (et =)
- Deux ensembles sont égaux s'ils ont les mêmes éléments
- Il existe un ensemble sans élément (le vide)
Formellement: $\exists y \forall x x \notin y$
- Paire, union, ensemble des parties

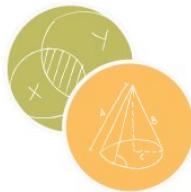




ZF: la théorie des ensembles de Zermelo-Fraenkel

- Axiome de l'infini:
il existe N qui contient \emptyset et
tel que si $x \in N$ alors $(x \cup \{x\}) \in N$
 N contient:
 $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$
 $0, \quad 1, \quad 2, \quad \quad \quad 3$
- Schéma de compréhension restreint:
 $\{X \in Y \mid P(X)\}$ est un ensemble
(fin du paradoxe de Russell)
- TOUTES les mathématiques se font dans ZF !!!

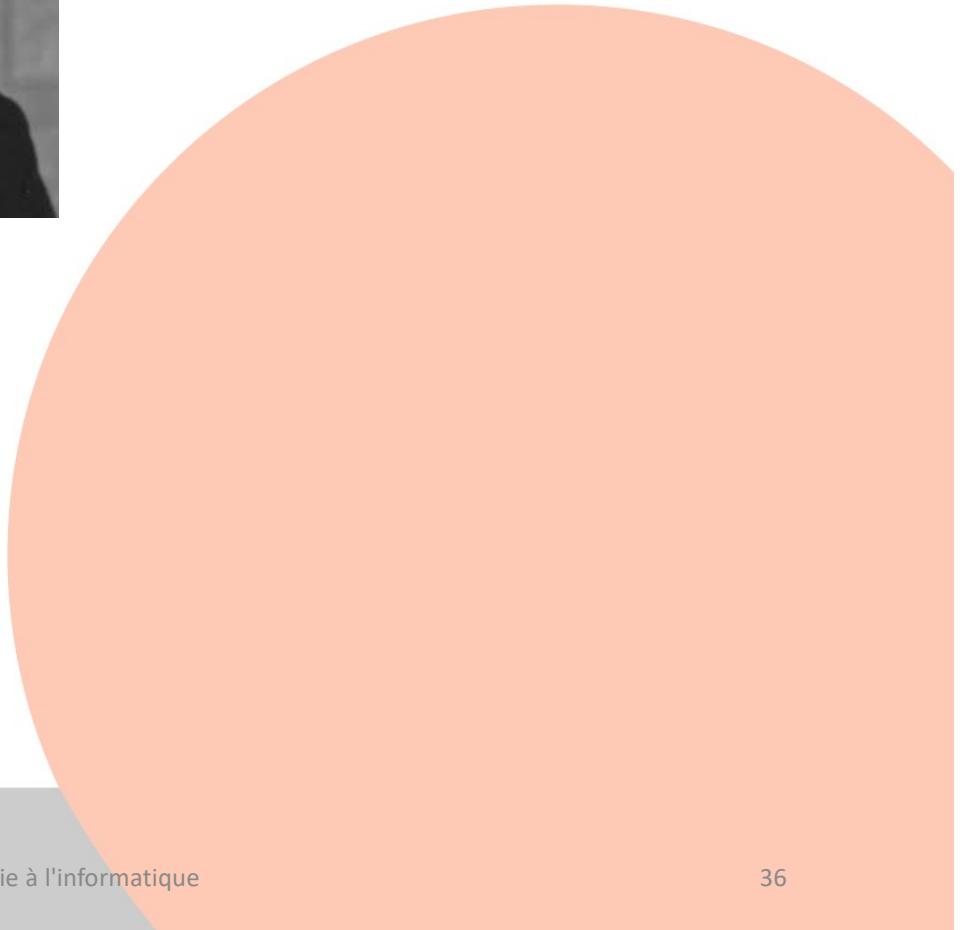


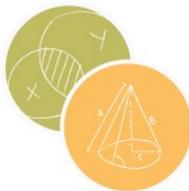


Luitzen Egbertus Jan Brouwer (1881-1966) et l'intuitionnisme



- Rejet du tiers exclus:
 - A ou non A
 - Différent de non (A et non A)
 - « ou » intuitionniste: plus exigeant
- Même chose pour le « il existe »
 - Existe x $P(x) = P(0)$ ou $P(1)$ ou $P(2)$...
 - Ne se déduit pas de
« NON pour tout X non $P(x)$ »

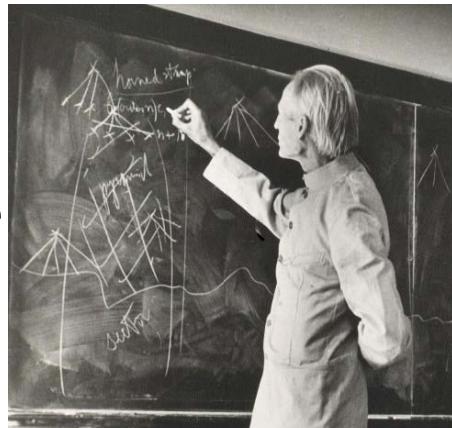




L.E.J. Brouwer et l'intuitionnisme

- Raisonnement constructif qui calcule ou approche la solution
- Ex. théorème des valeurs intermédiaires par dichotomies successives (Newton) (la preuve par l'absurde ne construit pas de solution)

Outre ses travaux sur le constructivisme Brouwer a produit un célèbre résultat de topologie en raisonnant par l'absurde, sans aucun argument constructif !!!





Kurt Gödel (1906-1978)

- Compatibilité de l'axiome du choix et de l'hypothèse du continu (univers tournants en relativité générale)
- Complétude de la logique du premier ordre et compacité (dans ce cours)
- Incomplétude de l'arithmétique (dans ce cours)
 - Certaines formules de l'arithmétique ne sont ni démontrables ni réfutables
 - En particulier la cohérence de la l'arithmétique (et qui peut s'exprimer dans l'arithmétique) n'est pas démontrable dans l'arithmétique.



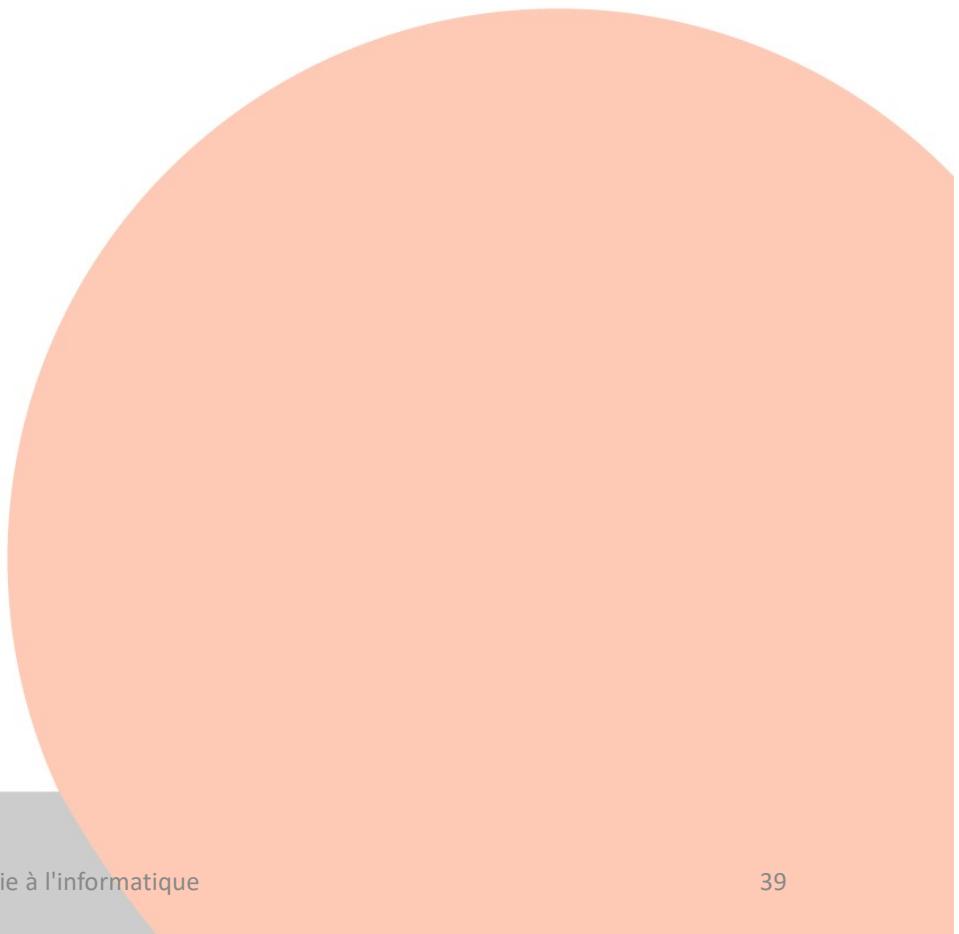
**Kurt Gödel
avec Albert
Einstein, son
unique ami de
Princeton**





En résumé: fondamentaux de ce cours

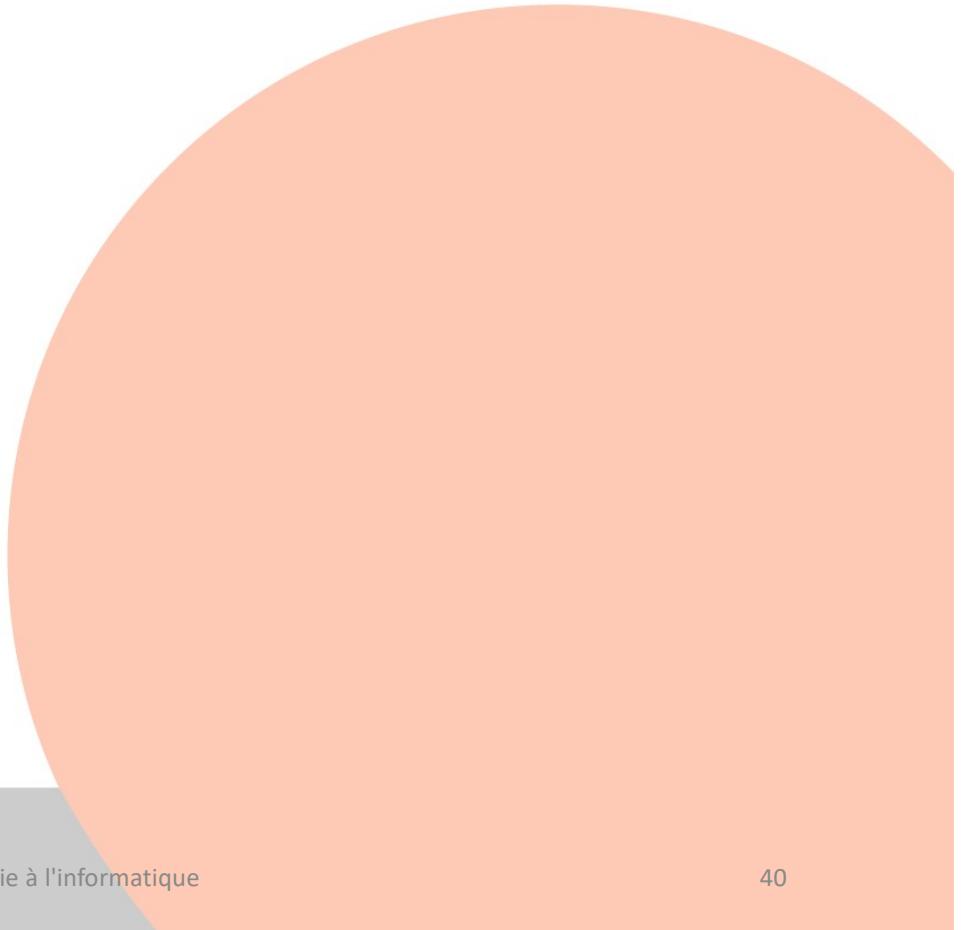
- Preuves (Frege, Hilbert, Herbrand, Gentzen)
- Modèles (Löwenheim, Tarski)
- Complétude de la logique du premier ordre (Gödel, Herbrand)
- *Compacité (Gödel):*
étant donné une famille de formules dont chaque partie finie admet un modèle, toute la famille admet un modèle
- Incomplétude de l'arithmétique de Peano.
(Gödel)





D'autres fondamentaux (pour un autre cours)

- Théorie des ensembles,
ordinaux, cardinaux
(Cantor, Zemelo-Fraenkel, Gödel)
- *Lowenheim Skolem:*
une théorie qui admet un modèle infini
en admet de toute cardinalité infinie





Logique, informatique et calculabilité

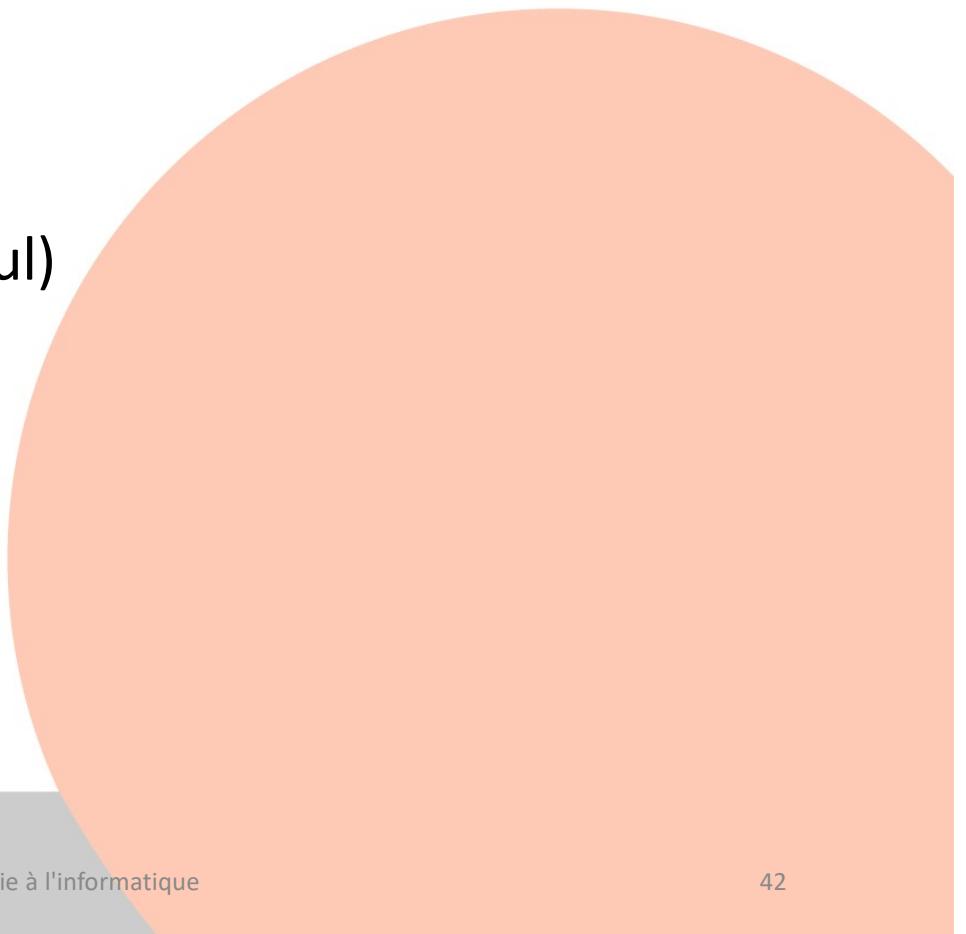
Les ordinateurs sont issus de la notion de calculabilité et non l'inverse.





Et l'informatique dans tout ça?

- Informatique? Science? Technologie ?
 - Données (\rightarrow informatique)
 - Calcul (\rightarrow computer science)
- Mécanisation du raisonnement (et du calcul) dans le programme de Hilbert
- Formalisation, codage,...(cf. Gödel)
- DÉCIDABLE ~ CALCULABLE





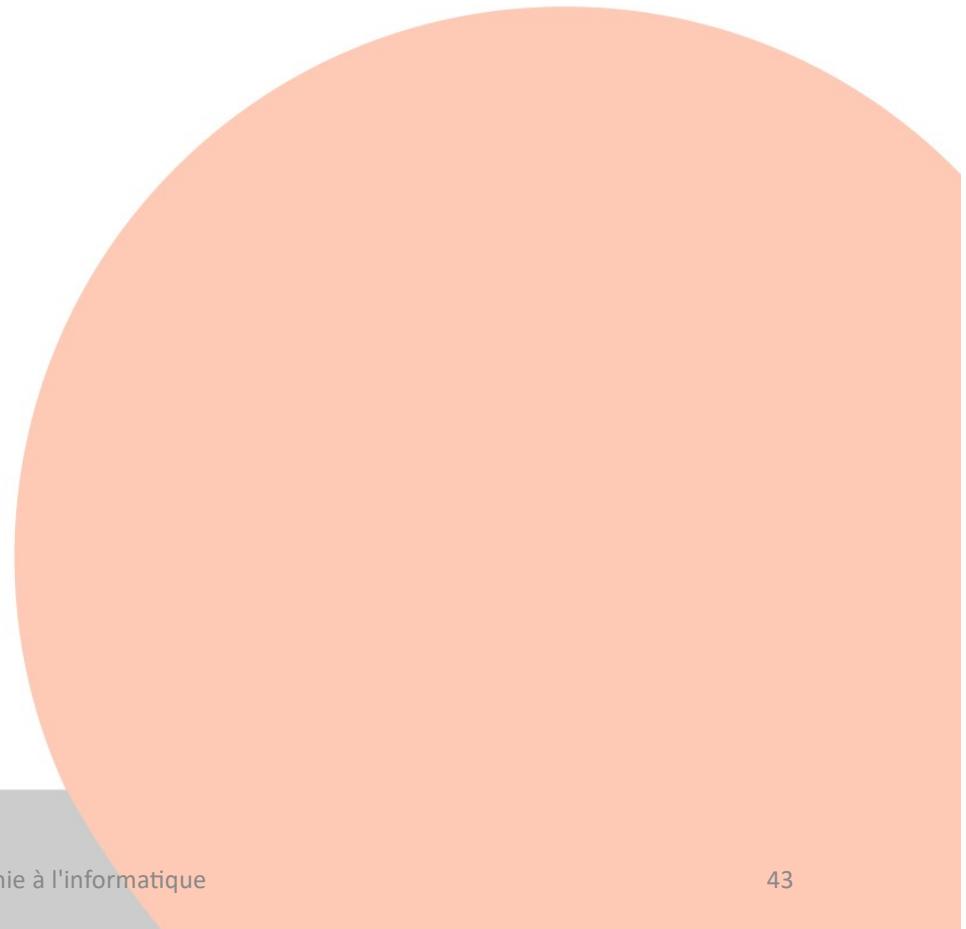
Lien entre informatique et logique

- **Génie logiciel:**

- vérification de programmes,
- preuves de programme,
- construction de programme certifiés
- ...

- **Intelligence artificielle:**

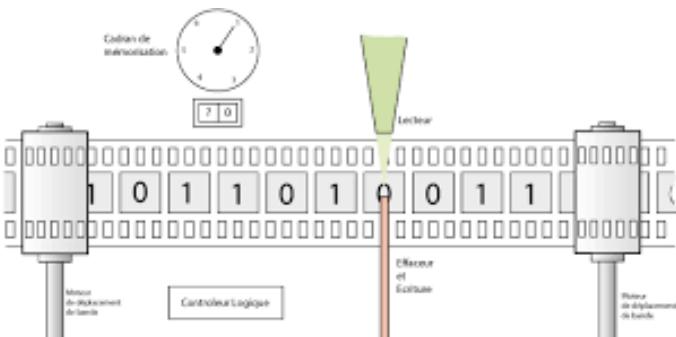
- modélisation du raisonnement
(systèmes experts, jeux,...)
- sémantique du langage naturel,
- ...

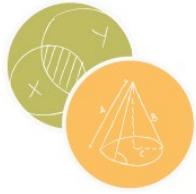




Machine abstraite 1936 Alan Turing (1912-1954)

- Ruban avec des 0 et des 1
(qui peuvent « tout » représenter via divers codages)
- Tête qui parcourt le ruban
- Etats: un état initial, plusieurs états finaux





Machine de Turing



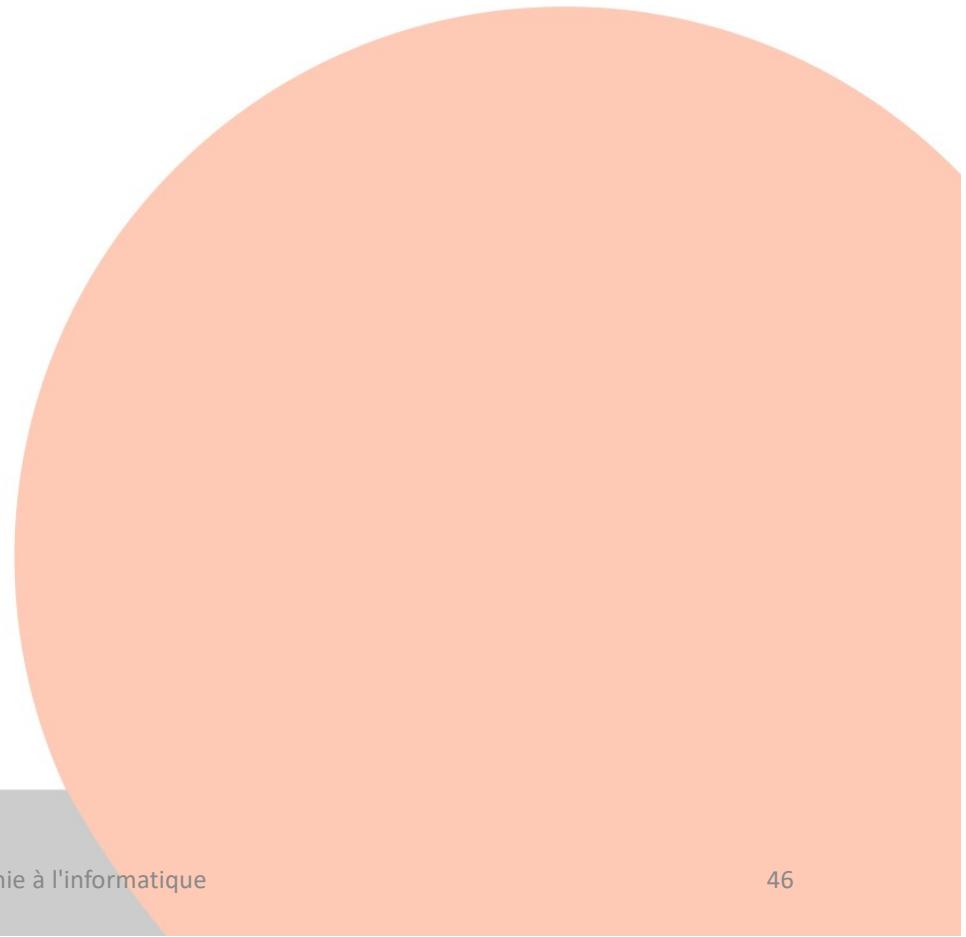
- Actions
 - lire, écrire (0, 1, rien),
 - déplacer (gauche, droite, rien),
 - Changement d'état
- Instructions:
si dans tel état si on lit tel caractère
alors on fait telle écriture,
on déplace la tête et on va dans tel état.





Machines de Turing: ça termine? ou pas?

- Il n'y a pas de machine de Turing qui étant donnés (sur un ruban):
 - Un entier m qui code une machine de Turing M
(un texte finit décrit la machine,
et il se représente par un nombre entier)
 - Et un entier n
 - Répond 1 si la machine M s'arrête (atteint
un état final) sur l'entrée n et 0 sinon.

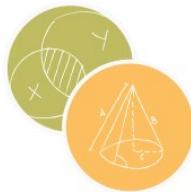




Machine de John von Neuman (1903-1957)

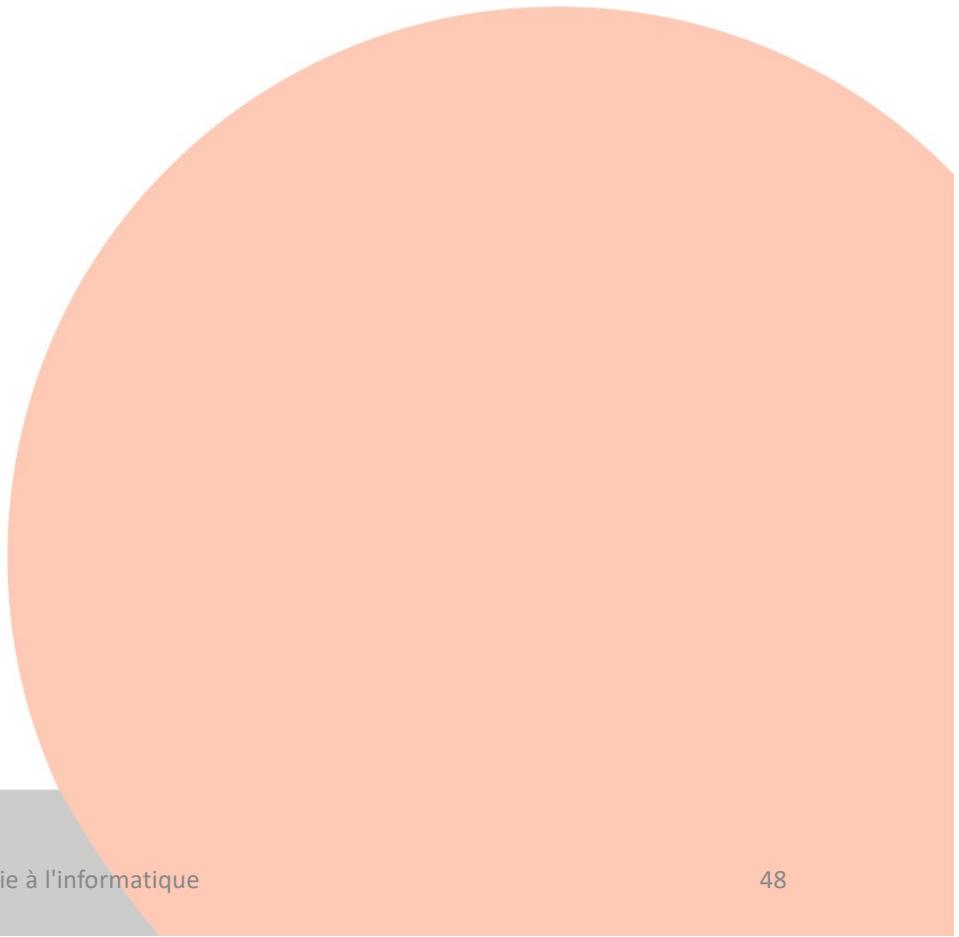
- 1 processeur
- 1 mémoire : données + programme
- Contrôleur qui dicte la séquence des opérations
- Nos ordinateurs fonctionnent toujours ainsi, mais ils communiquent entre eux.





Le lambda calcul ou la calculabilité à la Church (1903-1995)

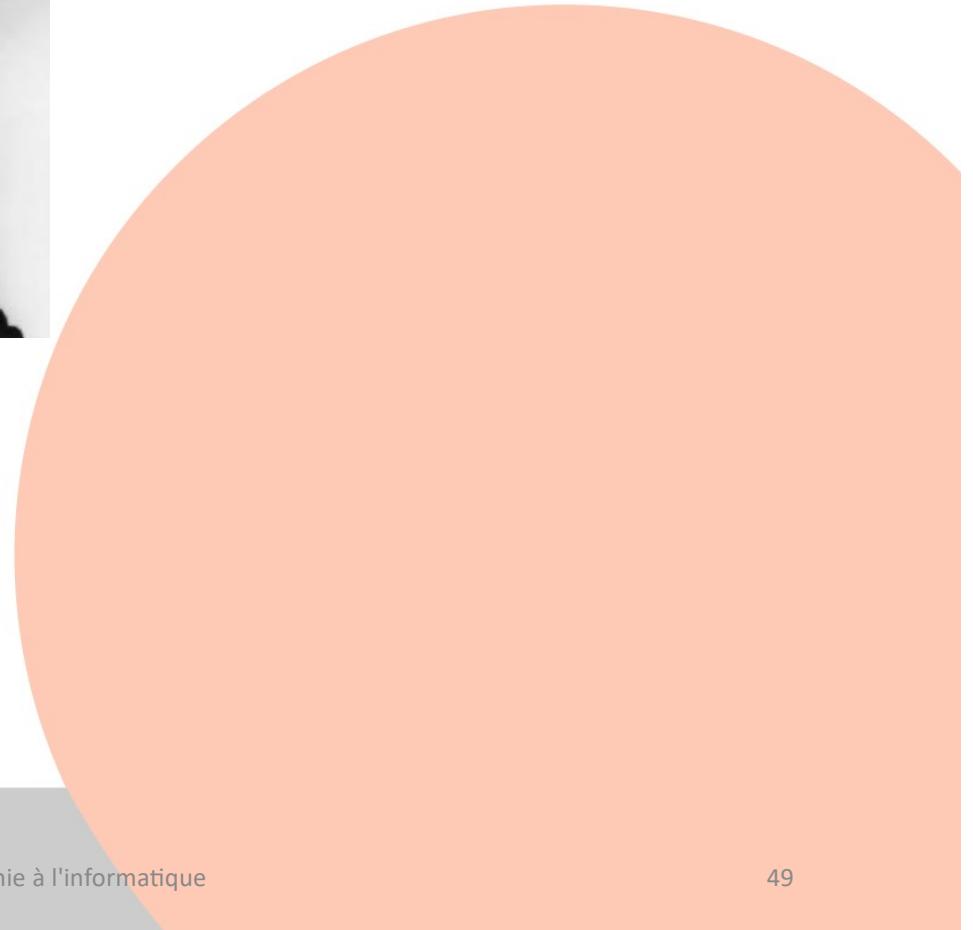
- Du point de vue des ensembles, un nombre entier est la classe des ensembles ayant le même nombre d'éléments.
- En lambda calcul le nombre n est défini ainsi:
appliquer n fois une fonction F à quelque chose:
 $f(f(f(x))) : 3$
 $S(S(S(0))) : 3$
 $mère(mère(mère(Jean))) : 3$





Le lambda calcul de Church

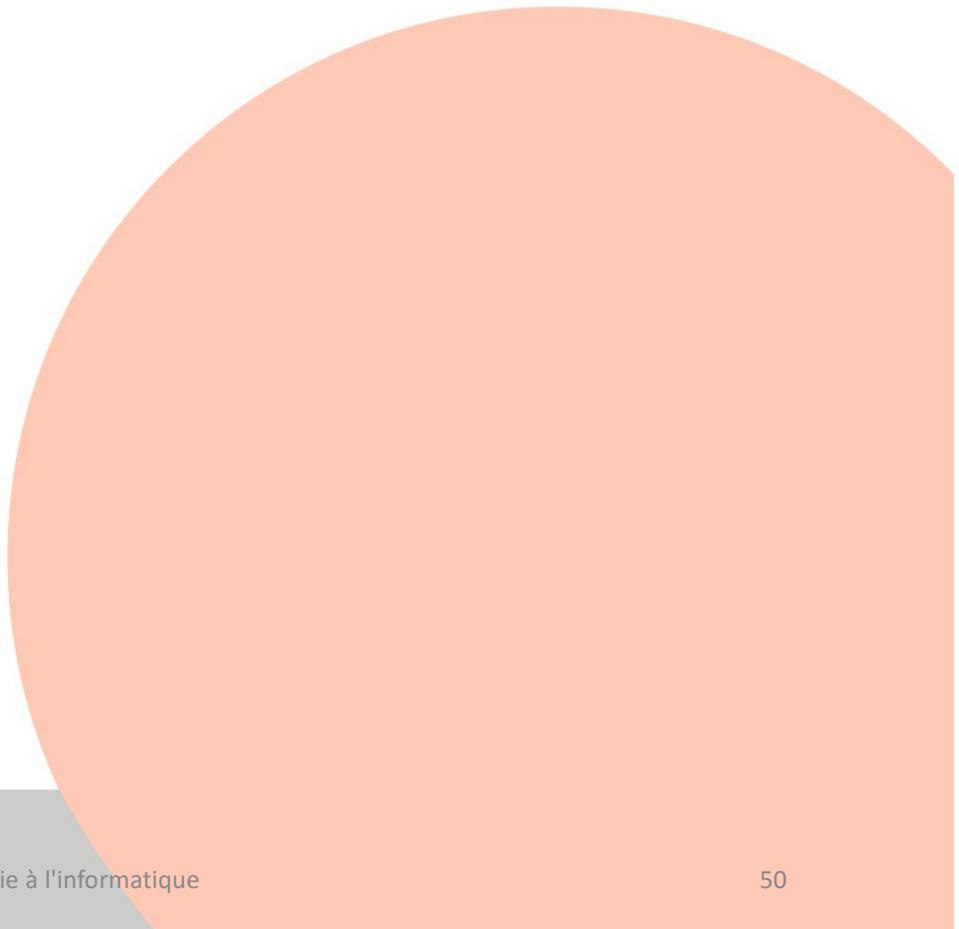
- En lambda calcul tout est fonction/action
- 3: $(\lambda f \lambda x (f(f(f(x))))$
- S: $\lambda n \lambda f \lambda x f(n \ x \ f)$
- +: $\lambda n \lambda p \lambda f \lambda x n(p \ x \ f) \ f$
- Calculer c'est remplacer la variable par sa valeur... $(\lambda x. (x+3)) \ 5 \rightarrow 5+3$ [substitution]





Thèse de Church Turing

- La machine de Turing et le lambda calcul de Church sont équivalents (Kleene)
- Pour montrer cela on montre que ces deux modèles calculent les fonctions récursives générales de Gödel-Herbrand-Kleene
- ***Les deux rendent exactement compte de tout ce qui se calcule automatiquement.***

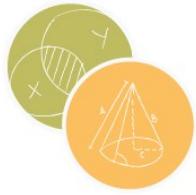




Gros plan: de la logique intuitionniste aux programmes certifiés

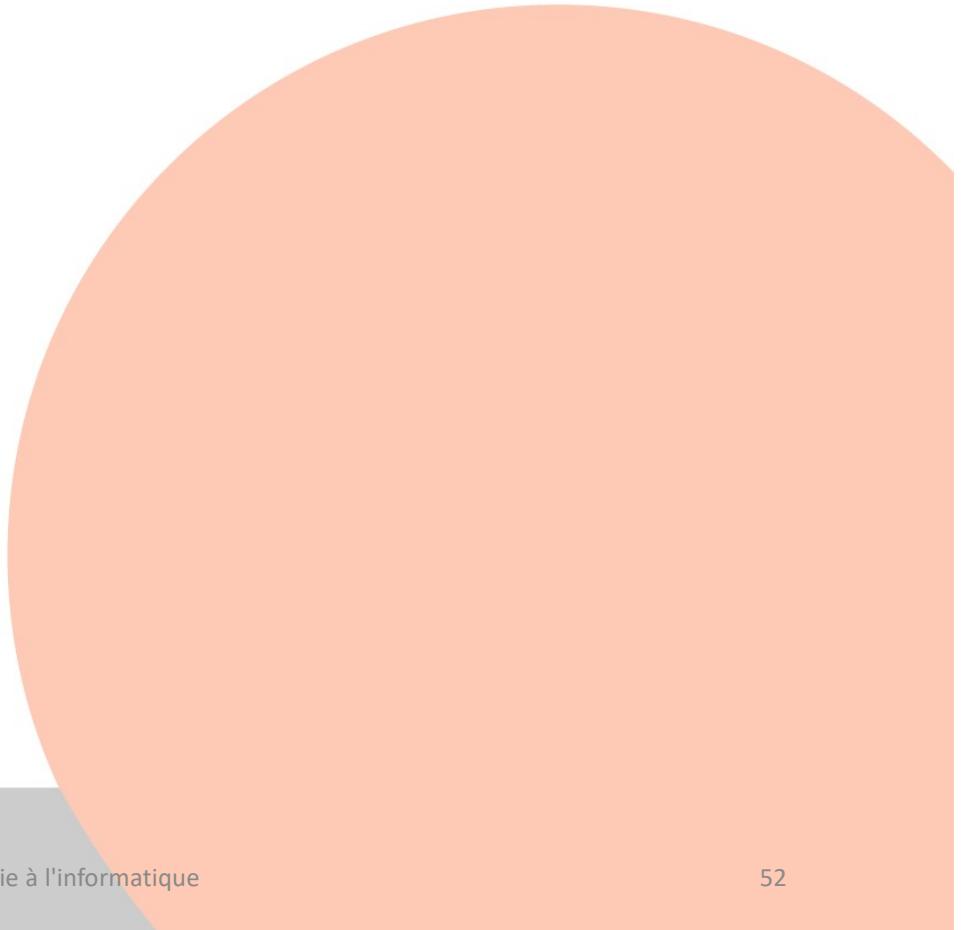
Preuves, types et programmes

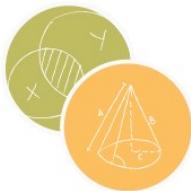




La déduction naturelle

- Déductions sous hypothèses
- Des règles simples comme ci-après.
- Bizarrement, la logique sous jacente est intuitionniste et non classique:
- $((a \rightarrow b) \rightarrow a) \rightarrow a$ n'est pas démontrable
- Mais démontrable classiquement:
 - Si a vrai OK
 - Si a faux $(a \rightarrow b)$ vrai donc $((a \rightarrow b) \rightarrow a)$ est faux OK





La déduction naturelle:
inventée par **Gerhard Gentzen** (1909-1945), ...
simplifiée **Dag Prawitz** (1936-...), ...

- Idée: manipuler des jugements avec hypothèses:
 $\Gamma \vdash A$
sous les hypothèses Γ , on a A





23 siècles après Aristote des règles de déduction simples, enfin!

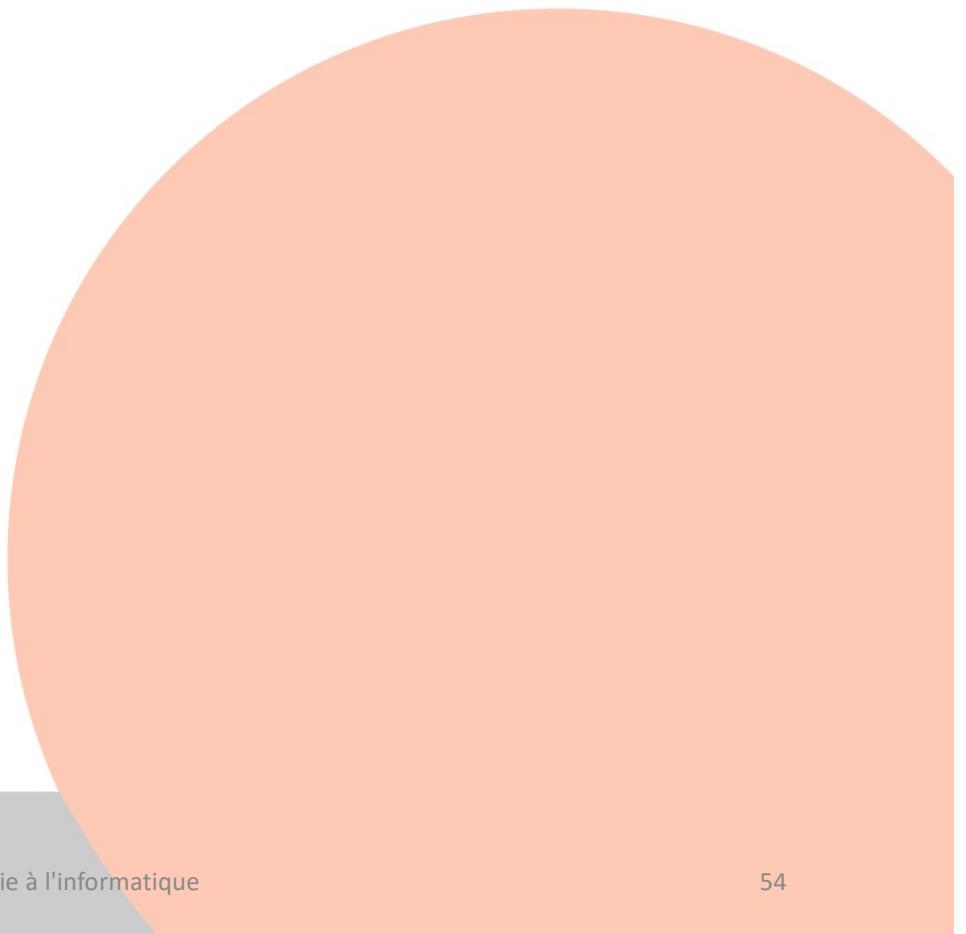
- Axiome $A \vdash A$ (si A alors A )

- Modus ponens:

Si $\Gamma \vdash A$ et $\Delta \vdash A \rightarrow B$
alors $\Gamma, \Delta \vdash B$

- Abstraction:

Si $\Delta, A \vdash B$
Alors $\Delta \vdash A \rightarrow B$





Règles de déduction:

A $A \rightarrow B$

B

Occurrences d'hypothèse A (barrées après la règle)

B

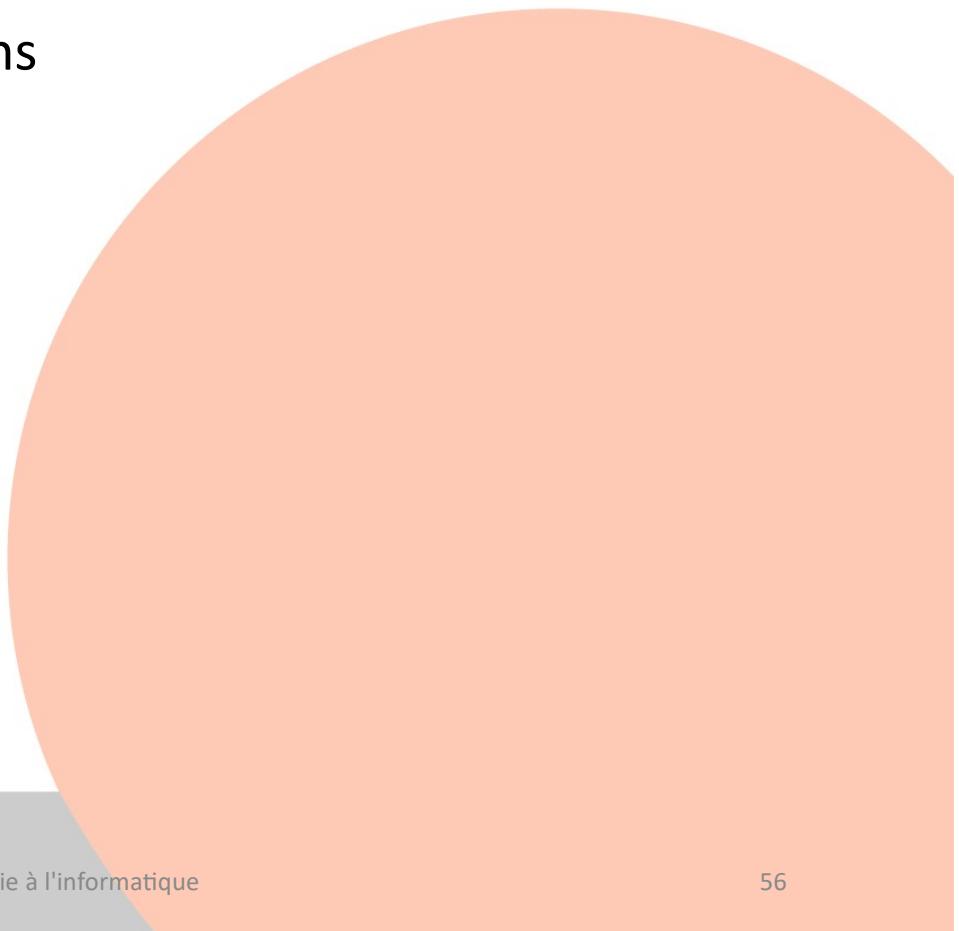
$A \rightarrow B$





La déduction naturelle: un formalisme simple mais puissant

- Système suffisant pour dériver les propositions intuitionnistes valide (écrites avec \rightarrow)
- Suffisant pour représenter les entiers!
(mieux en quantifiant sur les propositions)





La correspondance de Curry (1900-1982) & (Howard 1926-...)

$x A \ 1 \ f A \rightarrow A \ 2$



$f(x) A \ f A \rightarrow A \ 2$

$f(f(x)) A \ f \ A \rightarrow A \ 2$



$f(f(f(x))) A$

1

$\lambda x \ f(f(f(x))) (A \rightarrow A)$

2

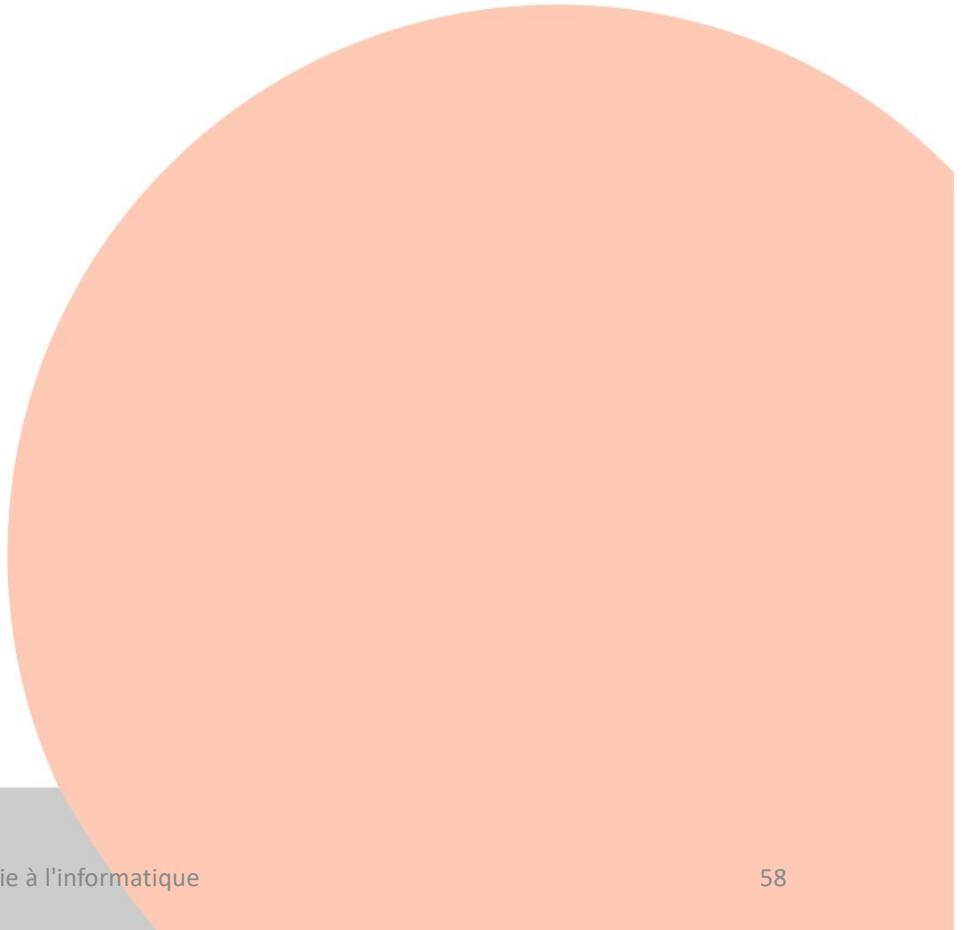
$\lambda f \lambda x \ f(f(f(x))) (A \rightarrow A) \rightarrow (A \rightarrow A)$





Entiers et fonctions

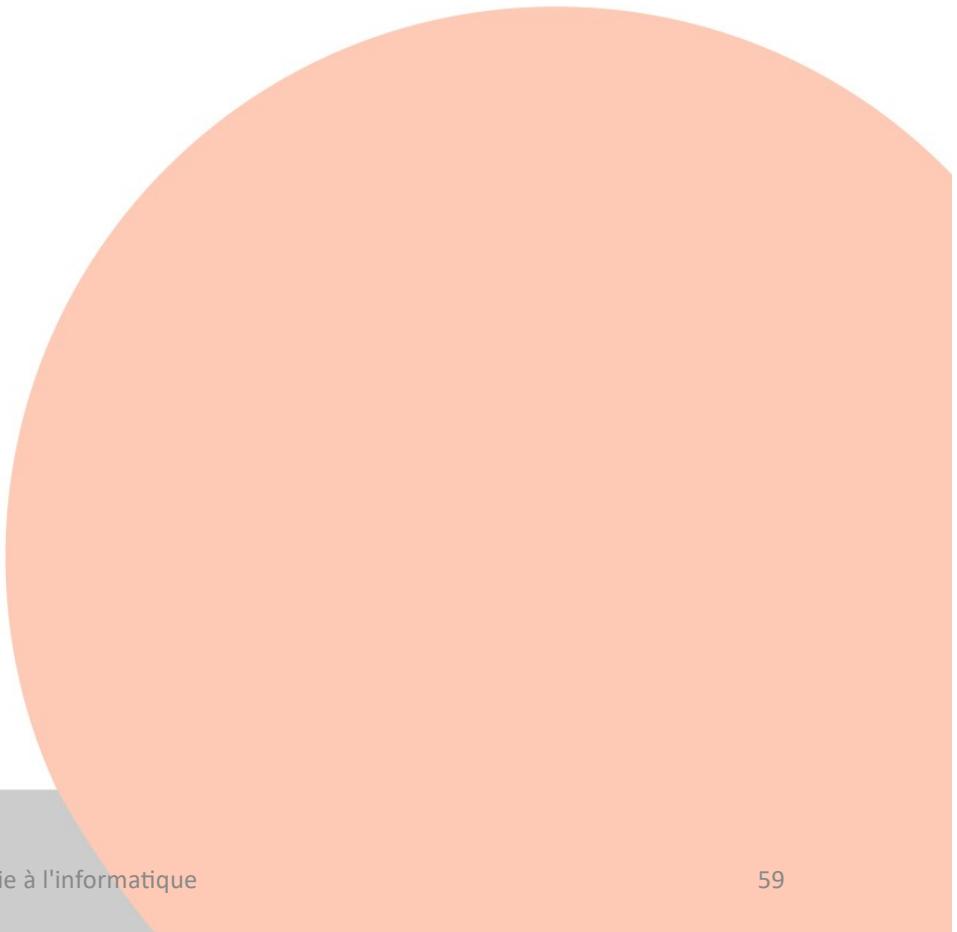
- $(A \rightarrow A) \rightarrow (A \rightarrow A)$ type entier
- Notre preuve de : $(A \rightarrow A) \rightarrow (A \rightarrow A)$ consiste en 3 applications de $A \rightarrow A$ à A ... c'est donc l'entier 3 du lambda calcul de Church
- On peut l'écrire $(\lambda f:A \rightarrow A \ \lambda x:A \ (f(f(f(x))))$
- $(\lambda x^A t[x]^B)^{A \rightarrow B} u^A$ devient $t[u]: B$





Propriété de la réduction: normalisation et évaluation

- Terminaison (tout programme termine!)
 - Confluence (peu importe la stratégie)
 - Forme normale unique (vers la même valeur)
-
- Dans le pire des cas, l'évaluation est lente, hyper exponentielle en fonction de la taille du terme.
 - Pour faire un vrai langage de programmation avec des programmes qui bouclent ;-) on ajoute un opérateur de point fixe (programmes récursifs)





Correspondance logique \leftrightarrow calcul

LOGIQUE

Formule A

Preuve d de A

Normalisation de d
(remplacement
des hypothèses
par leur preuve)

INFORMATIQUE

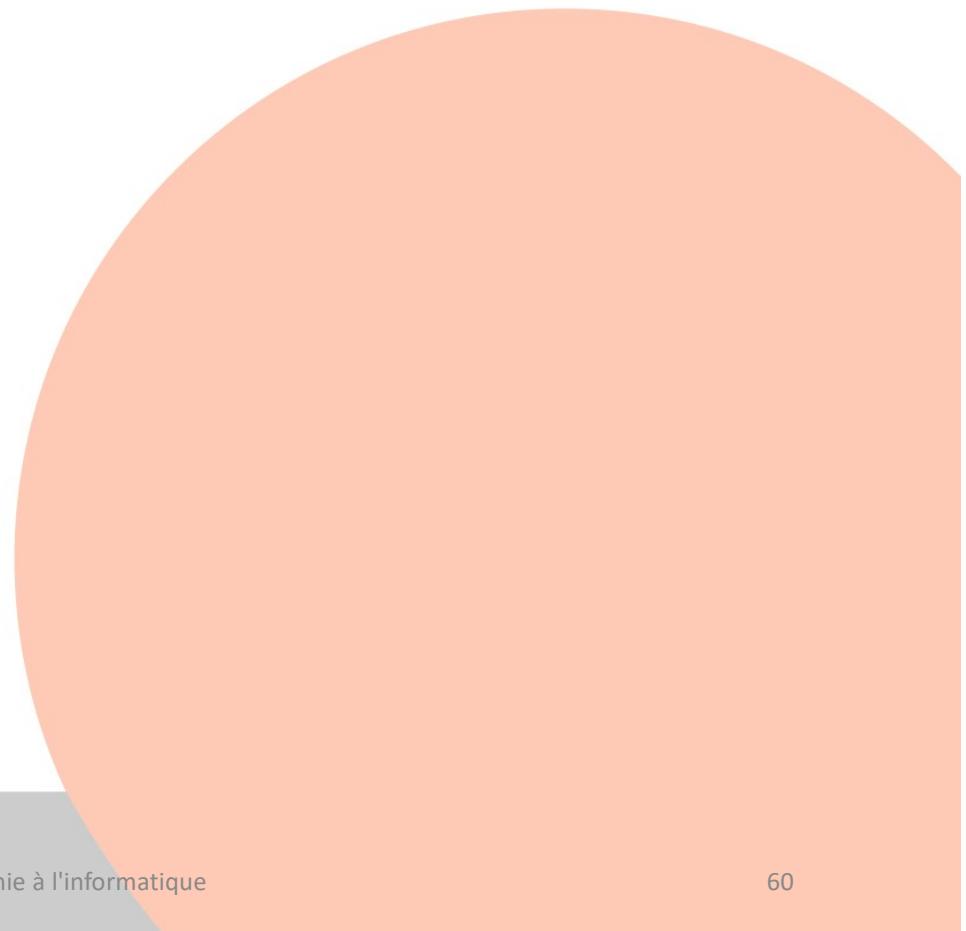
Type A

Programme d de type A

Evaluation de d
(substitution
des variables
par leur valeur)

Ex: EXP 2 3 \rightarrow 8

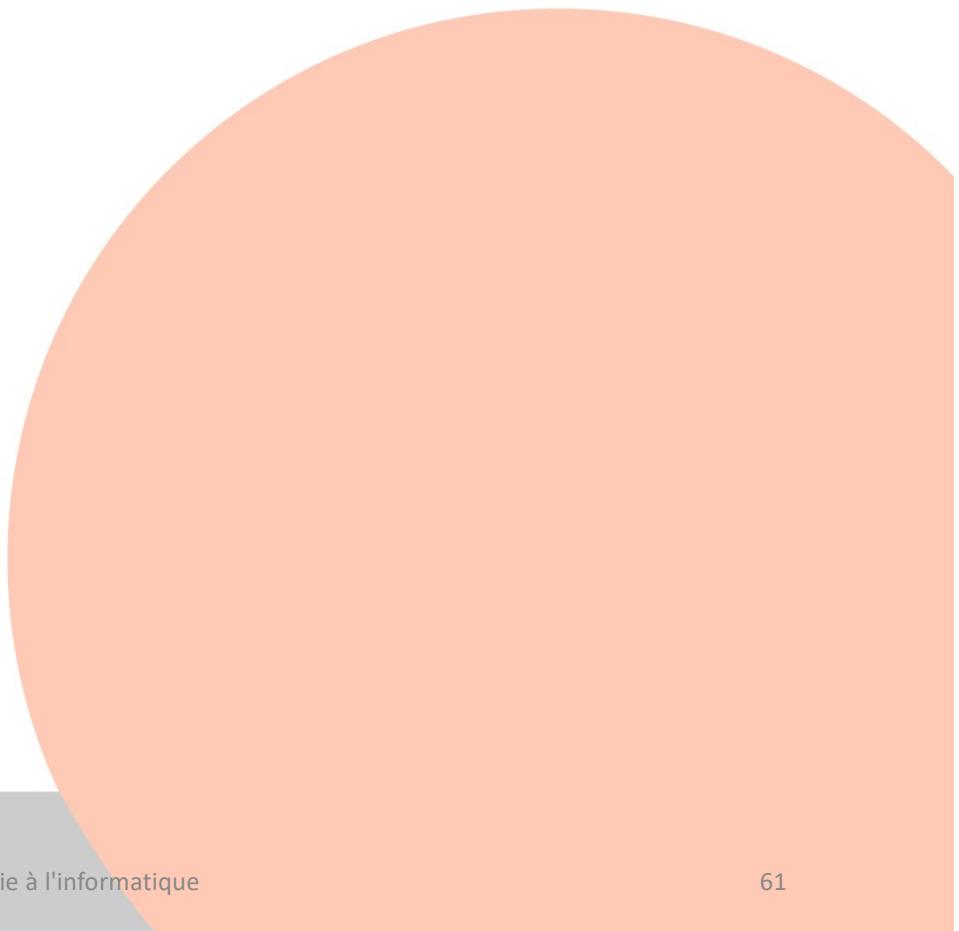
chaque expression est un lambda terme/ une preuve





Programmes certifiés: les preuves vues comme des programmes

- Santé, aéronautique, finances,
protocoles de connexion...
- **il faut des programme sûrs**
 - Vérification
 - **Extraction de programmes depuis les
preuves**
- **Assistant de preuve Coq: 1 &2**





De la preuve au programme certifié

- **Procédure:**

1. On écrit la spécification du programme: (équations)
2. On démontre formellement que pour tout x de type A il existe un y de type B tel que $P(x,y)$ en utilisant les règles de la logique et les équations
Par ex. $F(0,Y)=Y$ $F(SX,Y)=S(F(X,Y))$ (addition)
3. On ne garde que la partie propositionnelle une preuve de $A \rightarrow B$
4. On construit le lambda terme de type $A \rightarrow B$

- **Le programme obtenu (lent mais 100% sûr) fait exactement ce qu'il est supposé faire.**





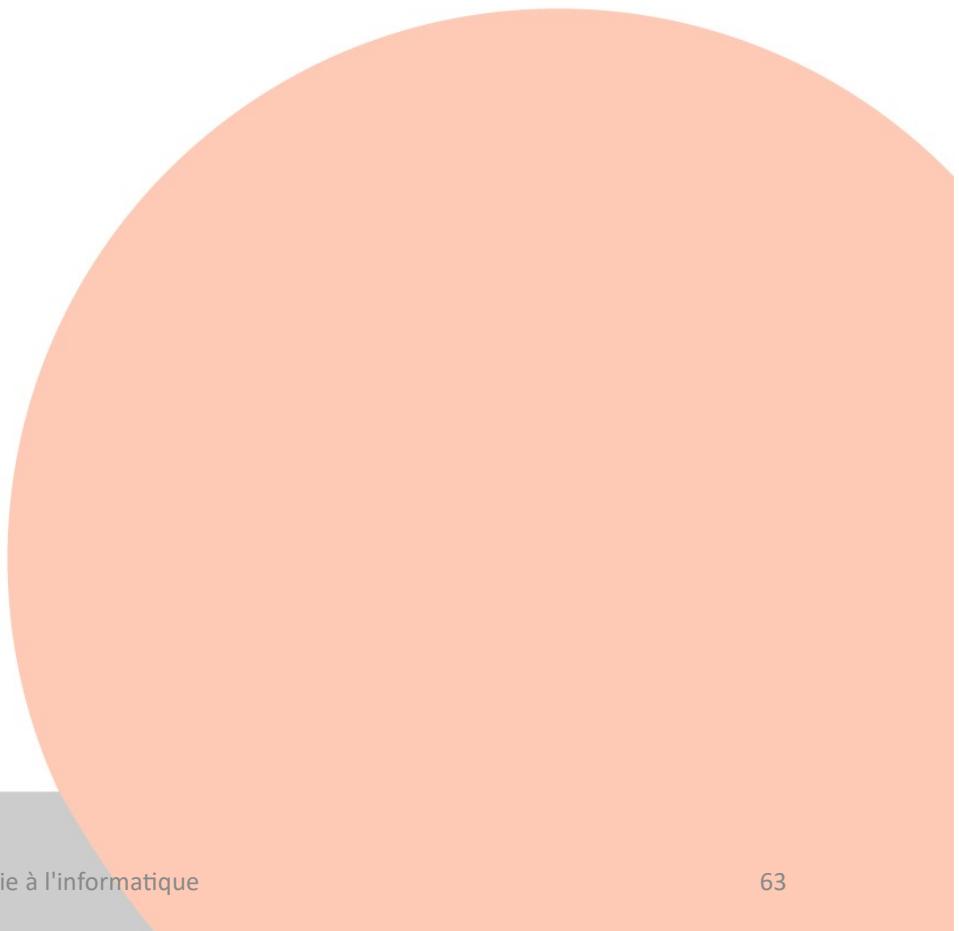
Programmer = prouver (1/2) (proofs as programs)

Ecrivons une fonction f des entiers dans les entiers.

satisfaisant $f(0)=S(0)$ $f(Sx)=(S(S(S(x))))$

N est un entier s'écrit:

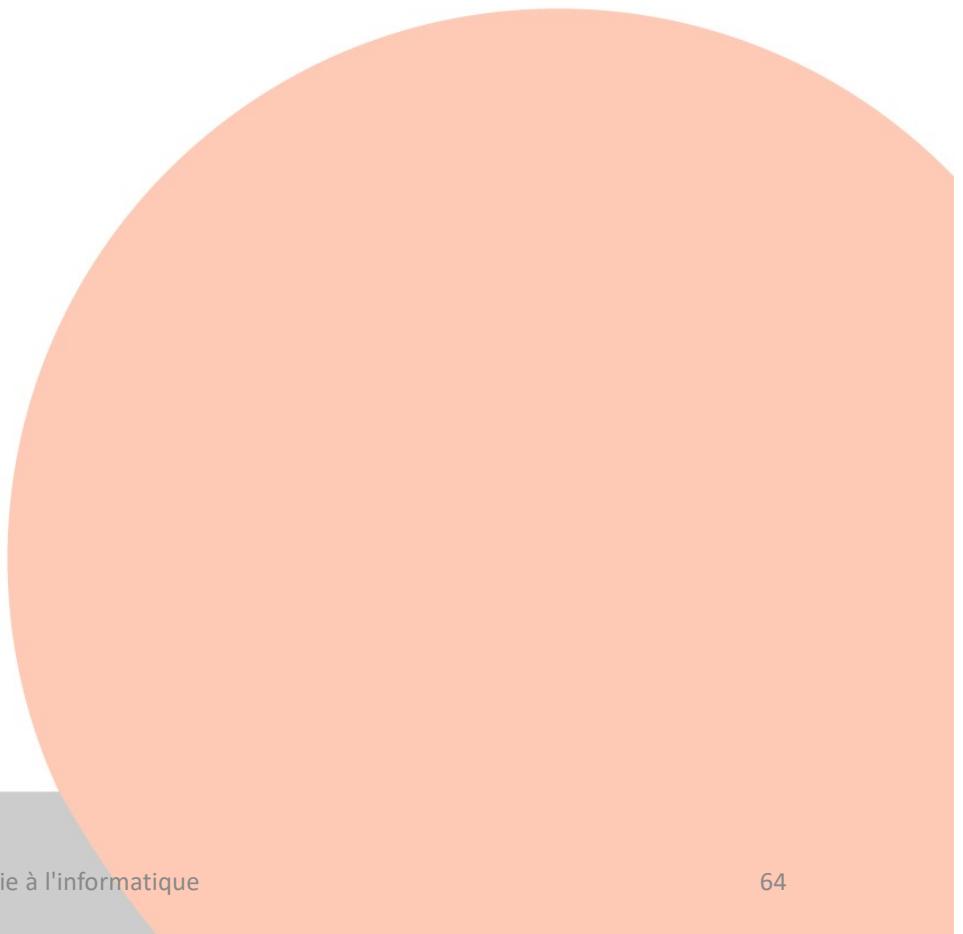
$N(p): \forall X [X(0) \& (\forall y X(y) \rightarrow X(Sy))] \rightarrow X(p)$
« p satisfait toute propriété X qui est vraie de 0 et qui passe au successeur »





Programmer = prouver (2/2) (proofs as programs)

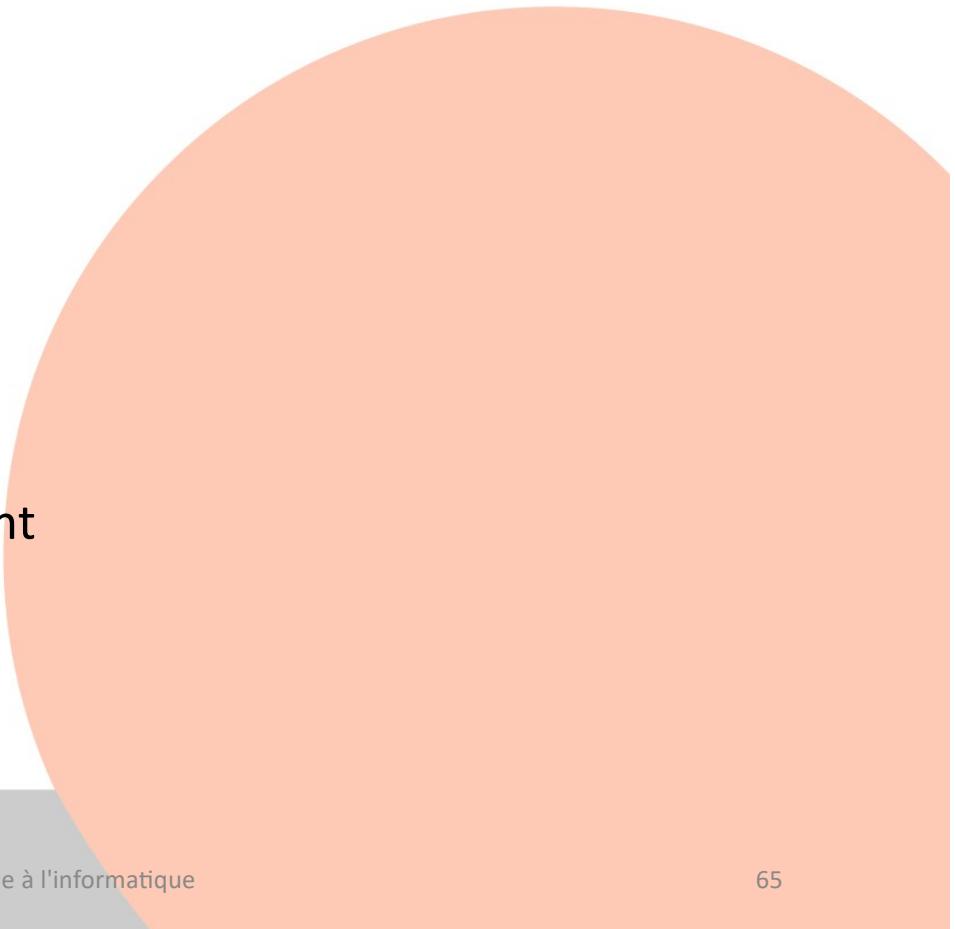
1. On écrit la spécification du programme:
par exemple $f(0)=S(0)$ $f(Sx)=(S(S(S(f(x))))$
2. On démontre formellement $\forall x$
 $N(x) \rightarrow N(f(x))$
en utilisant exclusivement la logique
et la définition de f (Coq?)
3. On ne garde que la partie propositionnelle
4. On construit le lambda terme \underline{f}
5. Lambda terme \underline{f} appliqué à un entier \underline{n} du
lambda calcul, se réduit en l'entier $\underline{3n+1}$
lambda calcul





Preuves: des fondements des maths à la logique du calcul

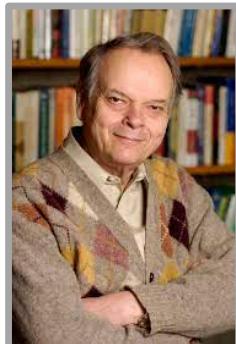
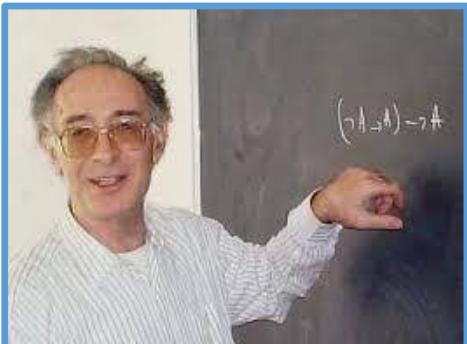
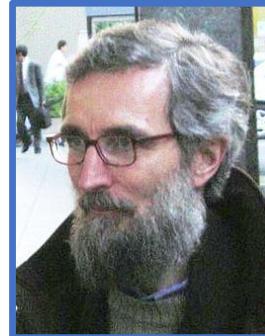
- Initialement: cohérence des mathématiques
- Contenu calculatoire (en logique intuitionniste)
- Programmes fonctionnels typés
 - Temps de calcul élevé
 - Mais totalement sûrs (par ex. circuits aéronautiques)
- La normalisation (tout programme termine) établit la cohérence du système logique sous jacent
→ elle s'établit donc en dehors du système d'après le théorème d'incomplétude de Gödel.





Preuves

- Fondements des maths / informatique dès 1970
 - Jean-Yves Girard (1947-...) *mon directeur de thèse*
 - John Reynolds (1935-2013)
 - Per Martin-Löf (1942-...) Vladimir Voevodski (1966-2017)
 - Jean-Louis Krivine (1939-...)
 - Gérard Huet (1947-...)

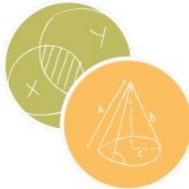




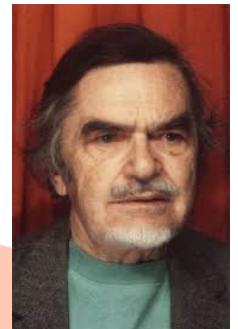
2^e Gros plan: Calcul du sens d'une phrase

Approche logique et compositionnelle
de la grammaire et du sens





Analyse grammaticale: preuve formelle Joachim Lambek (1922-2014)



- Logique sous structurelle, sensible
 - aux ressources (mots catégories grammaticales)
 - à l'ordre desdites ressources
- Analyse de $S =$ preuve que S est une phrase
- Un lexique associe à chaque mot des formules (son comportement grammatical, ses manières de se combiner avec d'autres mots)
- Les catégories sont écrites avec deux symboles:
 - / « sur », « diviser »
 - \ « sous», « antididiviser »





Calcul de Lambek (1958)

grammaire universelle
à 4 règles seulement

$$\frac{A/B \quad B}{A} [/E]$$

$$\frac{\dots [B]^n}{\frac{A}{A/B} [/I]^n}$$

$$\frac{B \quad B \setminus A}{A} [\setminus E]$$

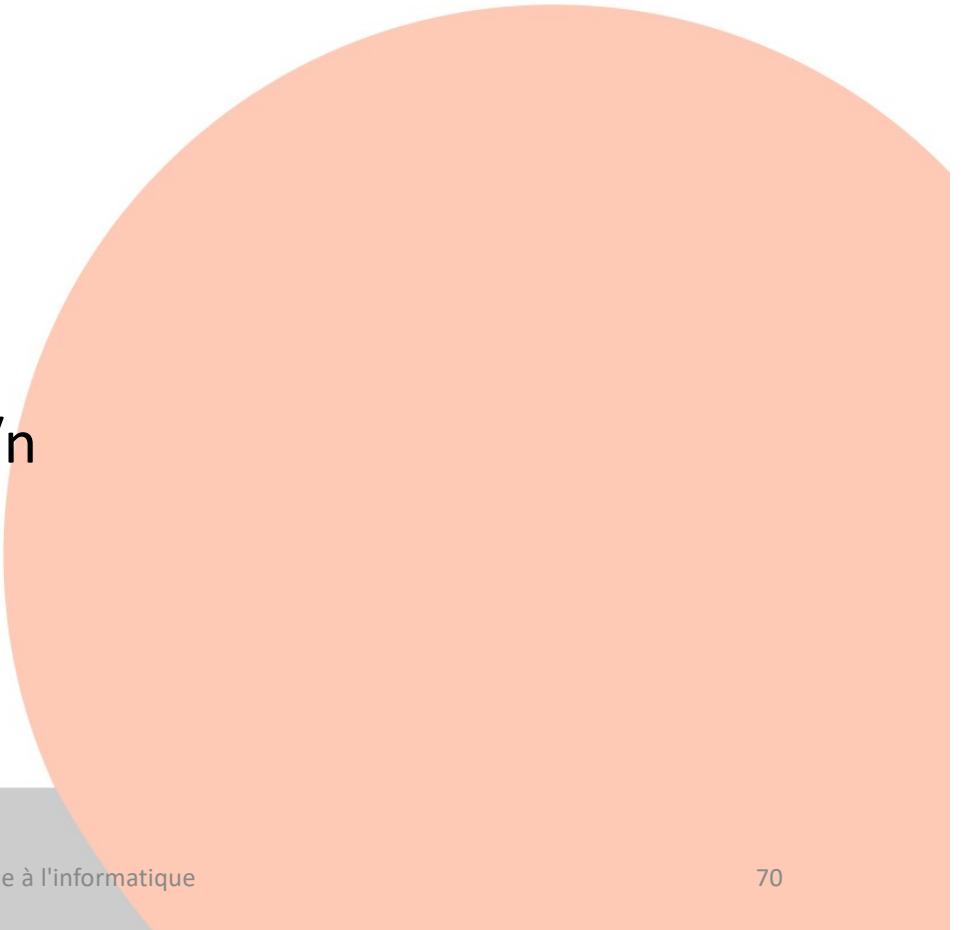
$$\frac{[B]^n \dots}{\frac{A}{B \setminus A} [\setminus I]^n}$$





Lexique syntaxique

- Les enfants prendront une pizza.
- Enfant(s), pizza: n
- Prendront: (np\|S)/np
- (tous) les, un : S/(np\|S)/n ou ((S/np)\|S)/n

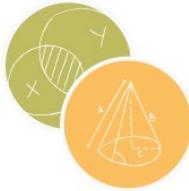




Parallèle: logique || grammaire (découvert vers le IIIe s av. JC)

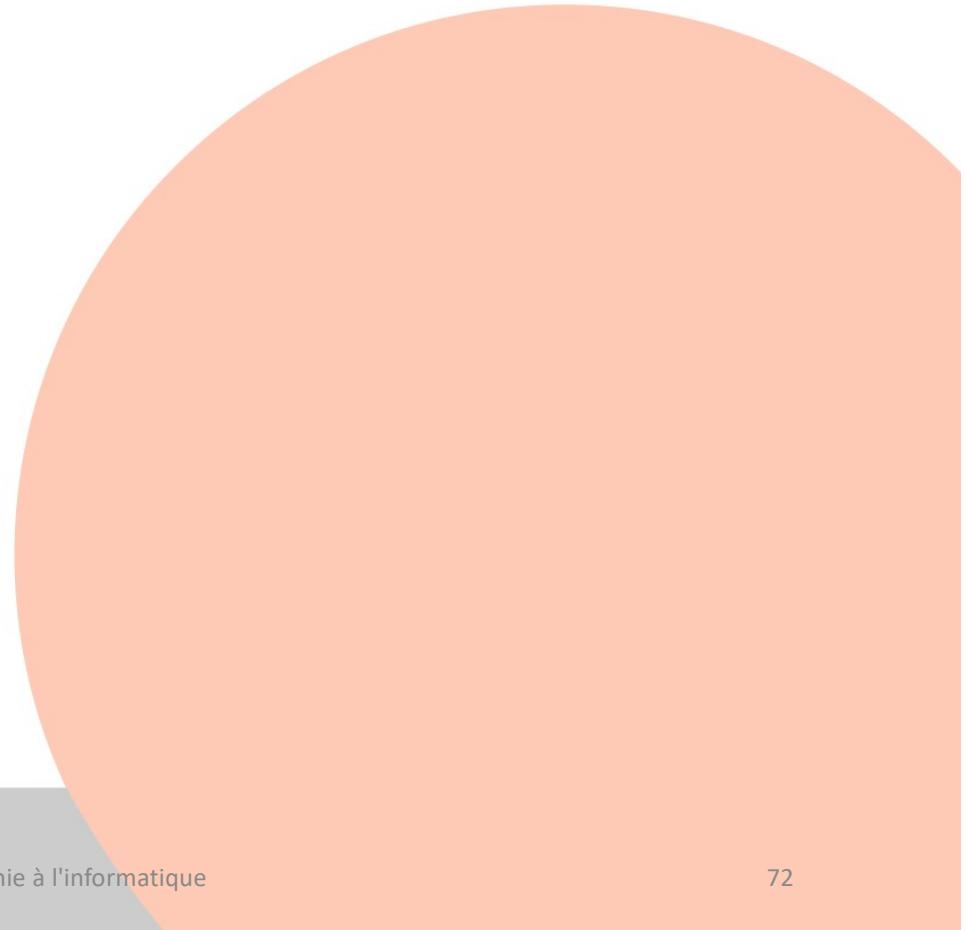
- n: nom commun: prédicat unaire
- np\S Verbe intransitif : prédicat unaire
- (np\S)/np Verbe transitif: prédicat binaire
- np Groupe nominal: individu
- np Nom propre: individu
- n\n Adjectif: prédicat ou prédicat de prédicat
- S/(np\S)/n ou (S/np)\S/n :
déterminant, quantificateur,
prend deux prédicats unaires et rend une proposition

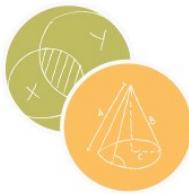




Un soupçon de sémantique (\exists)

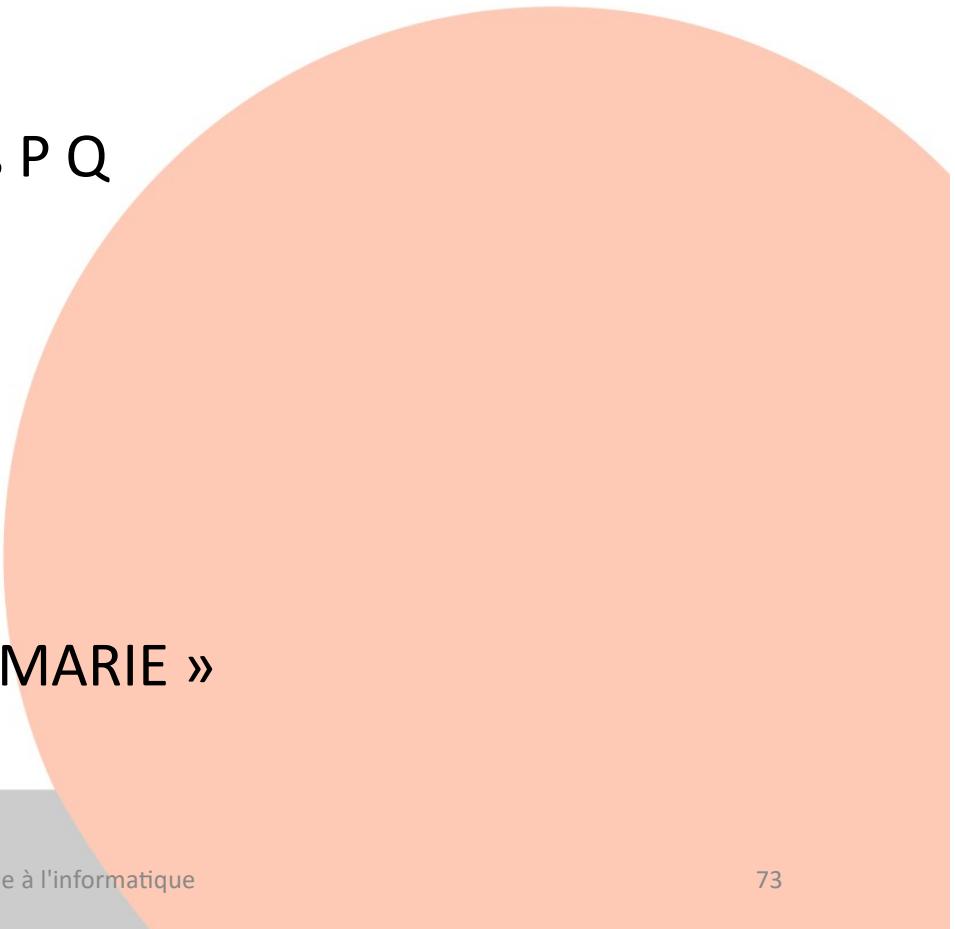
- UN chat dort.
- UN prend deux prédictats unaires P Q et rend une proposition :
 - Syntaxe $S/(np\backslash S)/n$
 - Sémantique $(e \rightarrow t) \rightarrow (e \rightarrow t) \rightarrow t$
 $P \qquad \qquad Q$
 - λ -terme $\lambda P \lambda Q \ \exists x (Px \ \& \ Qx)$
- UN construit la proposition
« au_moins_un P est_aussi Q »
« au_moins_un CHAT DORT »





Un soupçon de sémantique (\forall)

- Marie connaît TOUS_LES élèves.
- TOUS_LES prend deux prédictats unaires P Q et rend une proposition :
 - Syntaxe $((S/\text{np})\backslash S)/n$
 - Sémantique $(e \rightarrow t) \rightarrow (e \rightarrow t) \rightarrow t$
 $P \qquad \qquad Q$
 - λ -terme $\lambda P \lambda Q \forall x (Px \Rightarrow Qx)$
- TOUS_LES construit la proposition
« tous_les P sont Q »
« tous_les ENFANTS sont CONNUS_DE_MARIE »

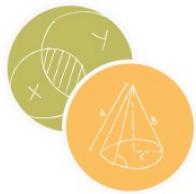




Exemple 1/4 lexique (syntaxe et sémantique)

mot	<i>catégorie syntaxique</i> <i>type sémantique</i> u^* <i>sémantique : λ-term of type u^*</i> x^v <i>signifie</i> x (<i>variable, constante</i>) de type v
les	$(S/(np\setminus S))/n$ (subject) $((S/np)\setminus S)/n$ (object) $(e \rightarrow t) \rightarrow ((e \rightarrow t) \rightarrow t)$ $\lambda P^{e \rightarrow t} \lambda Q^{e \rightarrow t} (\forall^{(e \rightarrow t) \rightarrow t} (\lambda x^e (\Rightarrow^{t \rightarrow (t \rightarrow t)} (P x)(Q x))))$
une	$((S/np)\setminus S)/n$ (object) $(S/(np\setminus S))/n$ (subject) $(e \rightarrow t) \rightarrow ((e \rightarrow t) \rightarrow t)$ $\lambda P^{e \rightarrow t} \lambda Q^{e \rightarrow t} (\exists^{(e \rightarrow t) \rightarrow t} (\lambda x^e (\wedge^{t \rightarrow (t \rightarrow t)} (P x)(Q x))))$
enfant(s)	n $e \rightarrow t$ $\lambda x^e (\text{enfant}^{e \rightarrow t} x)$
pizza	n $e \rightarrow t$ $\lambda x^e (\text{pizza}^{e \rightarrow t} x)$
prendront	$(np\setminus S)/np$ $e \rightarrow (e \rightarrow t)$ $\lambda y^e \lambda x^e ((\text{prendront}^{e \rightarrow (e \rightarrow t)} x)y)$





Exemple 2/4 analyse syntaxique = preuve

$$\frac{\frac{(S/(np\backslash S))/n \quad n}{(S/(np\backslash S))} /_e \quad \frac{(np\backslash S)/np \quad [np]^1}{(np\backslash S)} /_e}{\frac{S}{S/np} /_i(1)} /_e \quad \frac{\frac{((S/np)\backslash S)/n \quad n}{(S/np)\backslash S} \backslash_e}{\frac{}{} \backslash_e}$$

Preuve du calcul de Lambek bien sûr !

Le λ -terme correspondant est :

$\exists \forall = (\text{une pizza})(\lambda o^e(\text{les enfants})(\text{prendront } o))$

Lambda terme typé de Church, bien sûr!





Exemple 3/4 Normalisation → formule logique

$$\begin{aligned} & (\text{une pizza})(\lambda o (\text{les enfants})(\text{prendront } o)) \\ &= (\lambda Q^{e \rightarrow t} (\exists^{(e \rightarrow t) \rightarrow t} (\lambda x^e (\wedge^{t \rightarrow (t \rightarrow t)} ((\text{pizza}^{e \rightarrow t} x)))) (Q x))) \\ & \quad (\lambda o \forall^{(e \rightarrow t) \rightarrow t} (\lambda w^e (\Rightarrow^{t \rightarrow (t \rightarrow t)} (\text{enfant}^{e \rightarrow t} w)) (((\text{prendront}^{e \rightarrow (e \rightarrow t)} w) o) \\ &= (\exists^{(e \rightarrow t) \rightarrow t} (\lambda x^e (\wedge^{t \rightarrow (t \rightarrow t)} ((\text{pizza}^{e \rightarrow t} x)))) \\ & \quad ((\lambda o \forall^{(e \rightarrow t) \rightarrow t} (\lambda w^e (\Rightarrow^{t \rightarrow (t \rightarrow t)} (\text{enfant}^{e \rightarrow t} w)) (((\text{prendront}^{e \rightarrow (e \rightarrow t)} w) o) \\ &= (\exists^{(e \rightarrow t) \rightarrow t} (\lambda x^e (\wedge^{t \rightarrow (t \rightarrow t)} ((\text{pizza}^{e \rightarrow t} x)))) \\ & \quad (\forall^{(e \rightarrow t) \rightarrow t} (\lambda w^e (\Rightarrow^{t \rightarrow (t \rightarrow t)} (\text{enfant}^{e \rightarrow t} w)) ((\text{prendront}^{e \rightarrow (e \rightarrow t)} w) x)))))) \end{aligned}$$

Normalisation:
 β -réduction de Church

ce qui s'écrit communément :

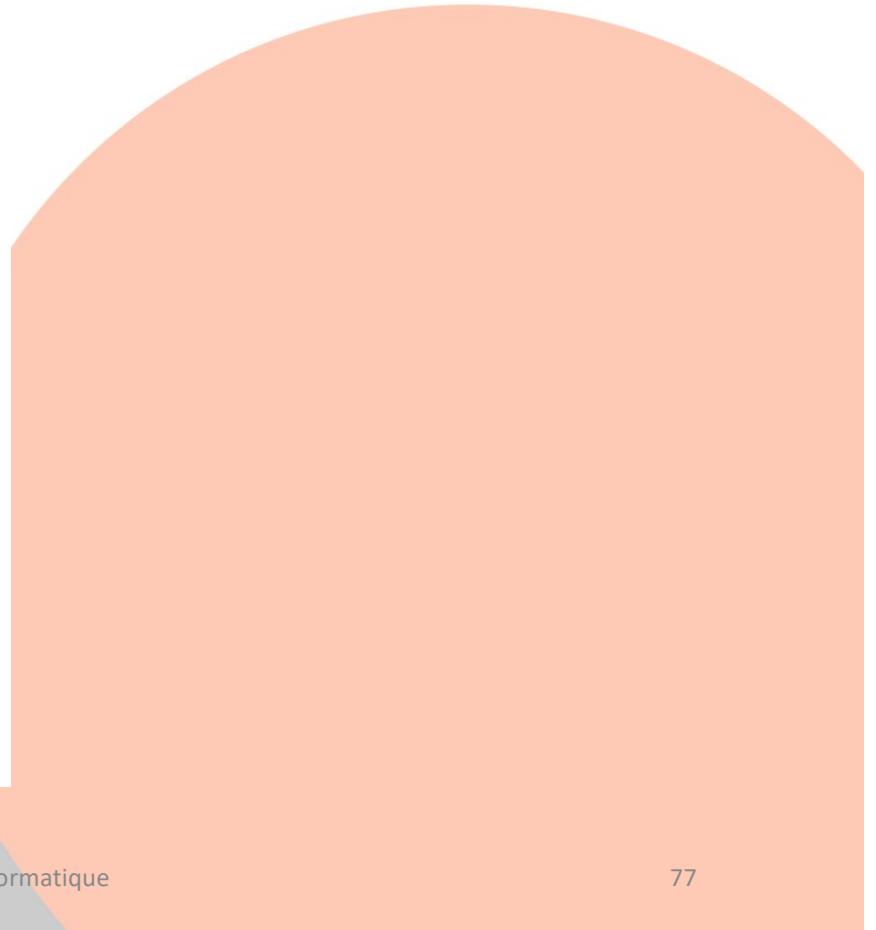
$$\exists x. \text{pizza}(x) \wedge \forall w. (\text{enfant}(w) \Rightarrow \text{prendront}(w, x))$$





Exemple 4/4 une 2^e analyse (sans calcul)

$$\frac{\frac{\frac{\frac{[np]_1}{(np \setminus S)/np} /_e [np]^2}{(np \setminus S)} \setminus_e \frac{\frac{S}{S/np} /_i (2)}{(S/np) \setminus S} /_e \frac{((S/np) \setminus S)/n - n}{(S/np) \setminus S} \setminus_e}{(S/(np \setminus S))/n - n} /_e}{(S/(np \setminus S))} /_e S$$



On trouve l'autre interprétation :

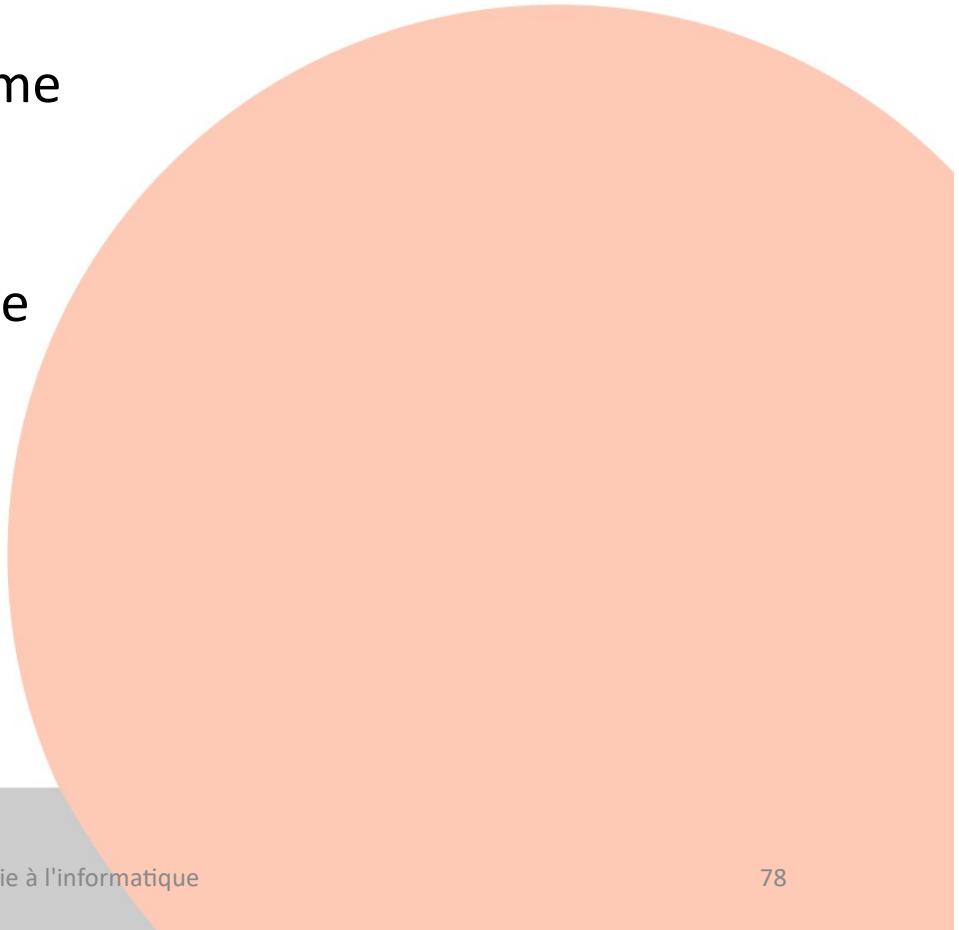
$$\forall u. \text{enfants}(u) \Rightarrow \exists x. \text{pizza}(x) \wedge \text{prendront}(u, x)$$

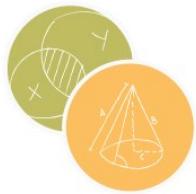




Commentaires sur grammaire et logique

- Analyse syntaxique = **preuve**
- Lambda terme sémantique d'un mot / syntagme
= **preuve incomplète**
- Lambda terme sémantique après réduction
= formule logique
= **preuve de la correction de la formule logique**
- Processus calculable (algorithme)
correction assurée de la sémantique
(si les informations lexicales soient correctes)
- Compositionnalité du sens:
réduction de lambda termes typés
=> preuves décrivant des **formules**



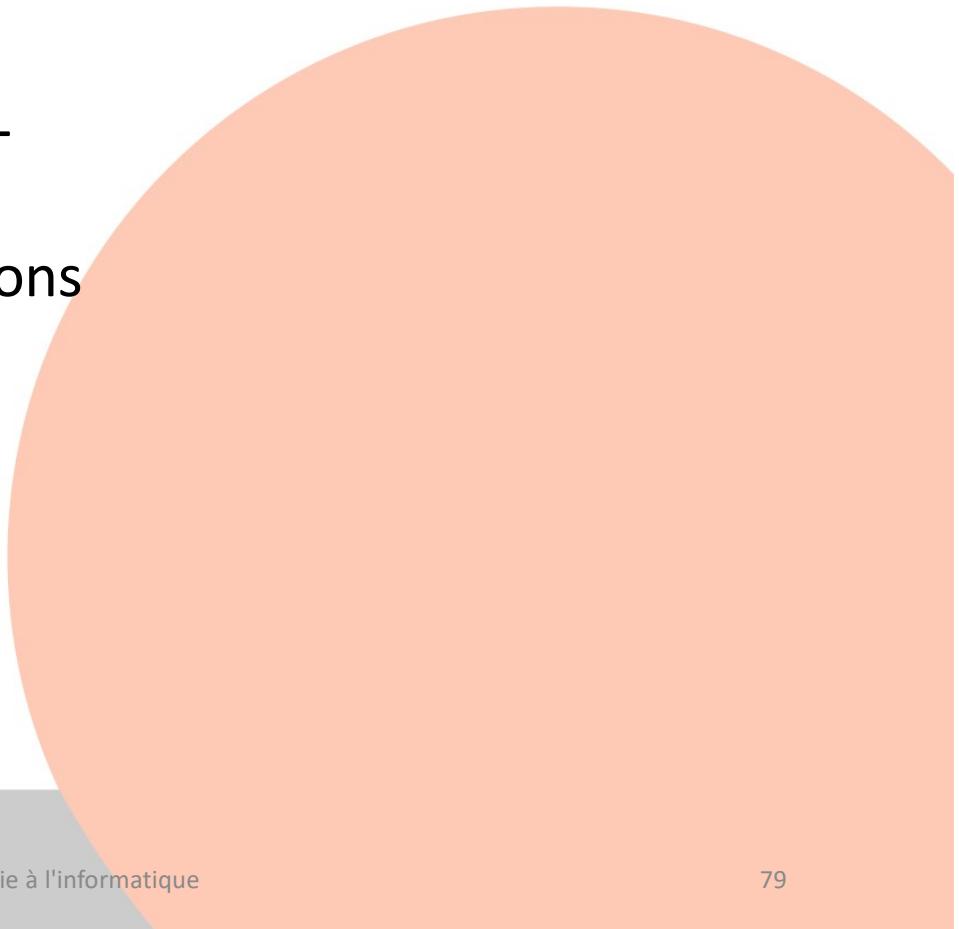


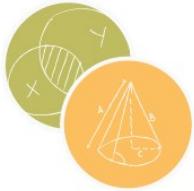
Et en pratique?

- Ça marche!
- Analyseur à large échelle du français GRAIL
(Richard Moot CNRS LIRMM UM)
- Sémantique = formule logique \neq connotations
- Intégration du sens lexical?

J'ai fini mon livre.

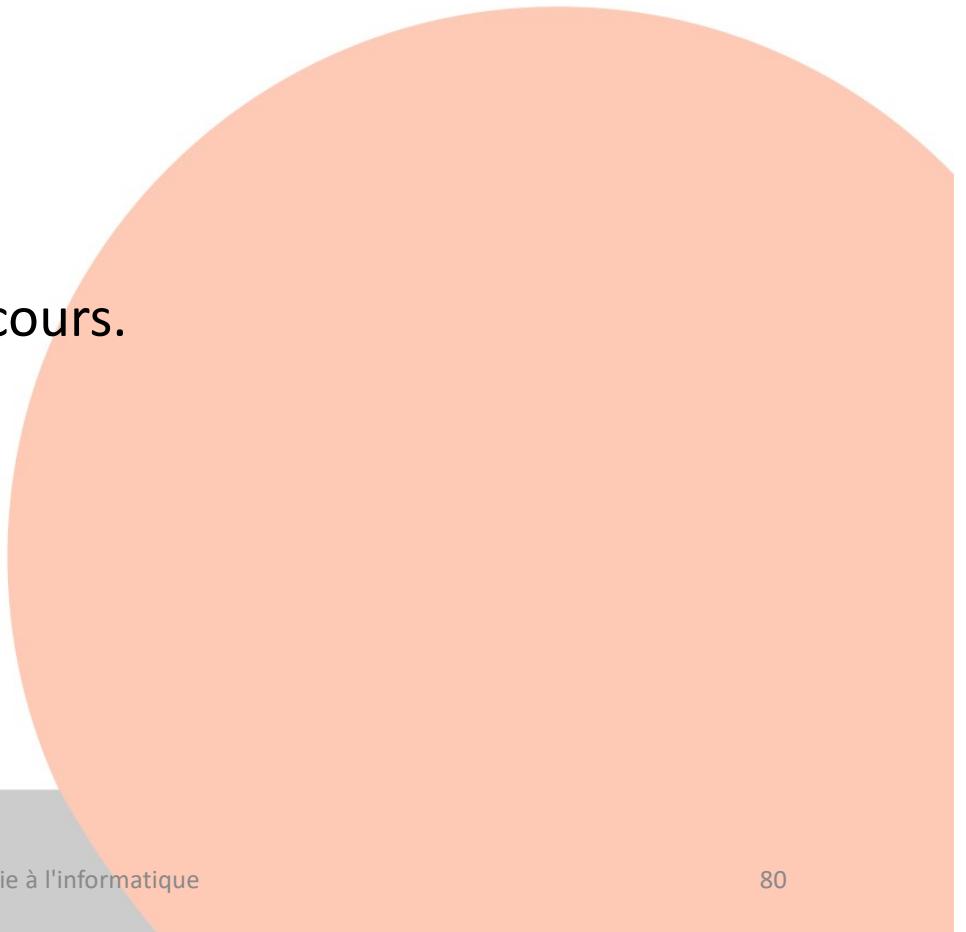
Événement: lire, écrire, ...?





Interprétation des phrases analysées

- Phrases → formules, et ensuite?
 1. Que peut on en déduire?
 2. Sont elles vraies?
 3. Contredisent-elles d'autres phrases?
- 1, 3 preuves comme dans ce cours.
- 2,3 modèles, interprétations comme dans ce cours.
- Certaines logiques utilisées en traitement automatique des langues ne sont pas présentées dans ce cours:
 - Les logiques sous structurelles (pour la syntaxe),
 - Les logiques modales (pour la sémantique).





Difficultés d'analyse et d'interprétation

Geach était-il l'élève de Wittgenstein ?

Wikipédia: Geach [...]

En 1941, IL épousa la philosophe Elizabeth Anscombe, grâce à LAQUELLE IL entra en contact avec Ludwig Wittgenstein.

Bien qu'IL N'ait JAMAIS suivi l'enseignement académique de CE DERNIER, cependant IL EN éprouva fortement l'influence.





"Contrariwise,
if it was so, it might be;
and if it were so, it would be;
but as it isn't, it ain't.
That's logic."
Lewis Carroll (1832-1898)

Merci de votre attention. Des références suivent.

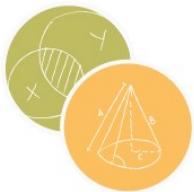




Quelques références

- **BD LOGICOMIX** de Apostolos Doxiadis, Christos H. Papadimitriou, Alecos Papadatos, and Annie di Donna Vuibert 2010
*Les principaux logiciens du début du XXe sont mis en scène.
Pas technique, mais des annexes permettent d'aller plus loin.*
- **Roman** La déesse des petites victoires
de Yannick Grannec Editions Anne Carrière. 2012
Prix des libraires 2013.
*Gödel vu par sa femme.
Très bonne reconstitution de la vie scientifique
à Vienne puis à Princeton,
avec des personnages comme Einstein
(l'unique ami de Gödel), von Neuman, Morgenstern,...
Très bon roman per se.*





Pour aller plus loin

- **Essai:** Pierre Cassou-Noguès Les démons de Gödel : Logique et folie Seuil 2015
Toujours sur Gödel, plus scientifique que le roman de Yannick Grannec.
- **Article original et commentaires:**
K. Gödel, E. Nagel, J. Newman, J.-Y. Girard
Le théorème de Gödel. Seuil 1997
- **Essai:** Gilles Dowek Les démonstrations et les algorithmes: introduction à la logique et à la calculabilité. 2010 Ecole polytechnique.
Très bon ouvrage de vulgarisation.

