La vérité si je montre

Séminaire IREM 27 avril 2016
Alain Busser

Implication

- Inventée par Diodore Cronos (IVe siècle avant J.-C.), l'implication « p implique q » signifie que q est au moins aussi vrai que p.

p	q	p implique q
V	V	V
V	F	F
F	V	V
F	F	V

Modus ponens

- De p et « p implique q » on déduit q

p	q	Si p alors q	p donc q
V	V	V	V
V	F	F	F
F	V	V	F
F	F	V	F

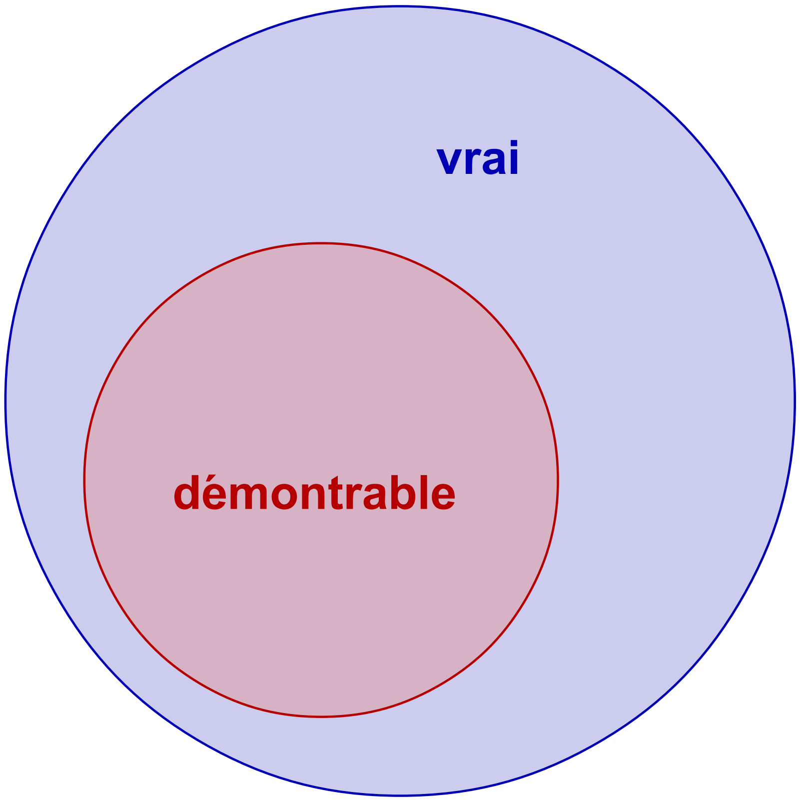
Théorie mathématique

Une théorie mathématique est formée

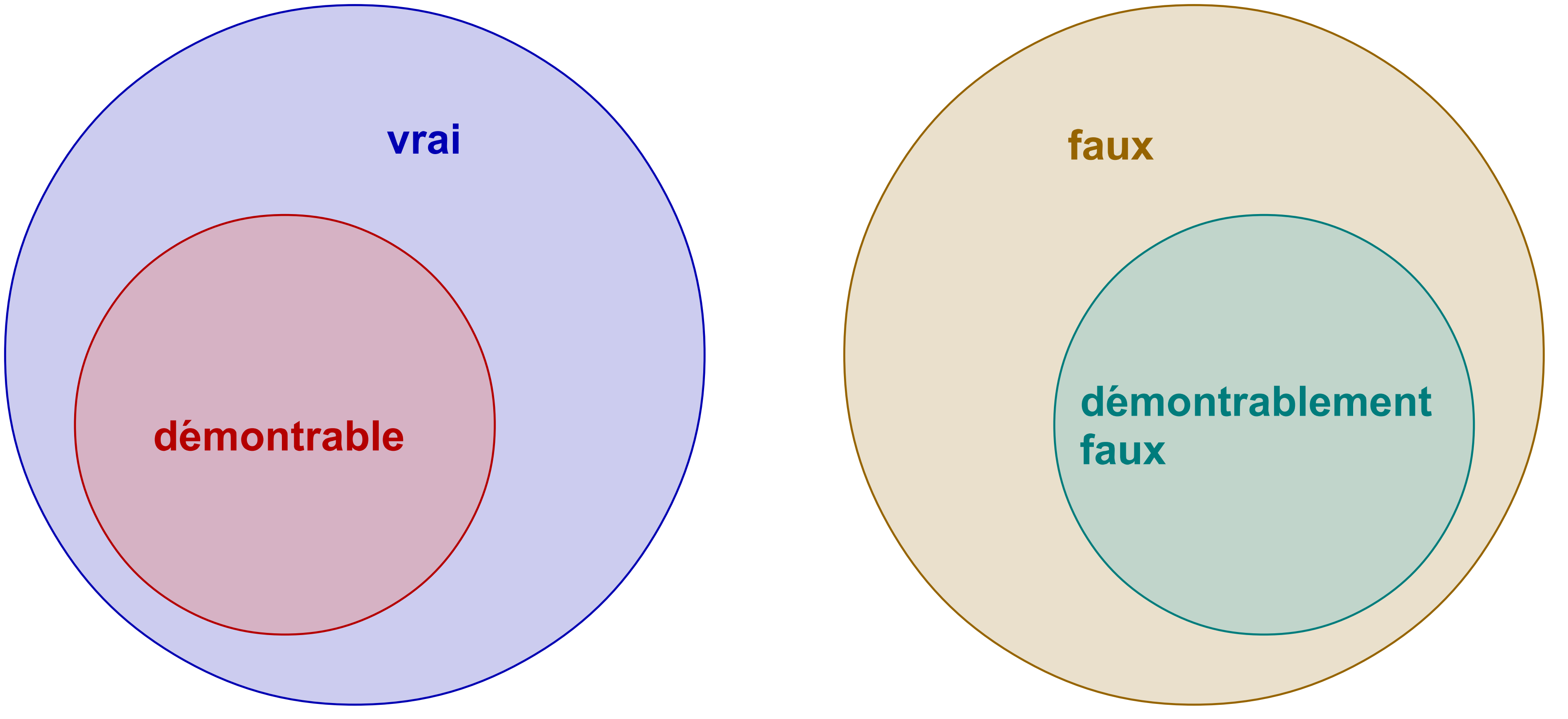
- D'axiomes, supposés vrais
- De théorèmes, déduits d'autres théorèmes par le modus ponens

Si les axiomes sont vrais, les théorèmes sont vrais

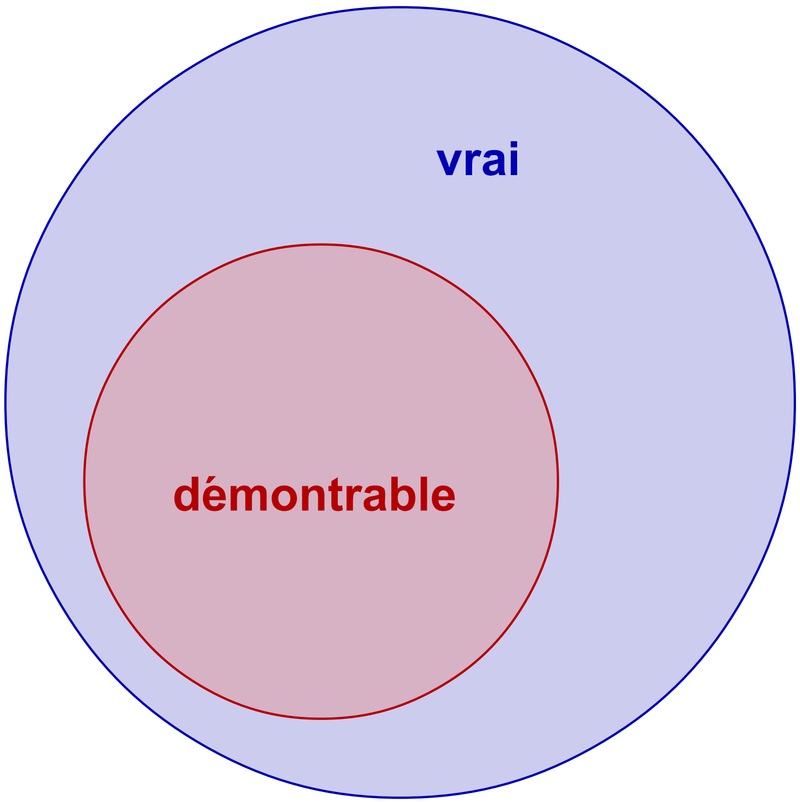
Métamathématique



Métamathématique



Métamathématique



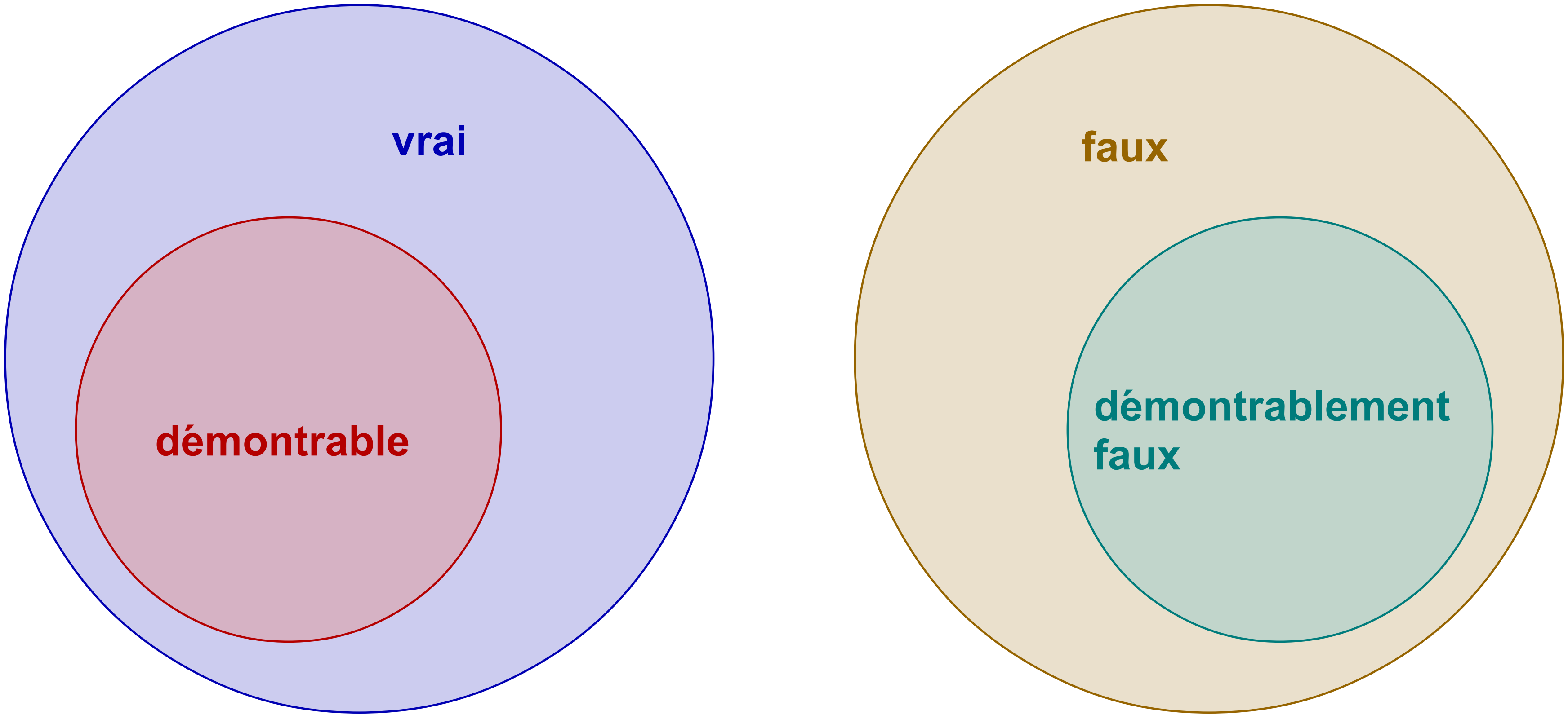
David Hilbert, en 1900 : Peut-on démontrer que tout ce qui est vrai, est démontrable ?

Définitions

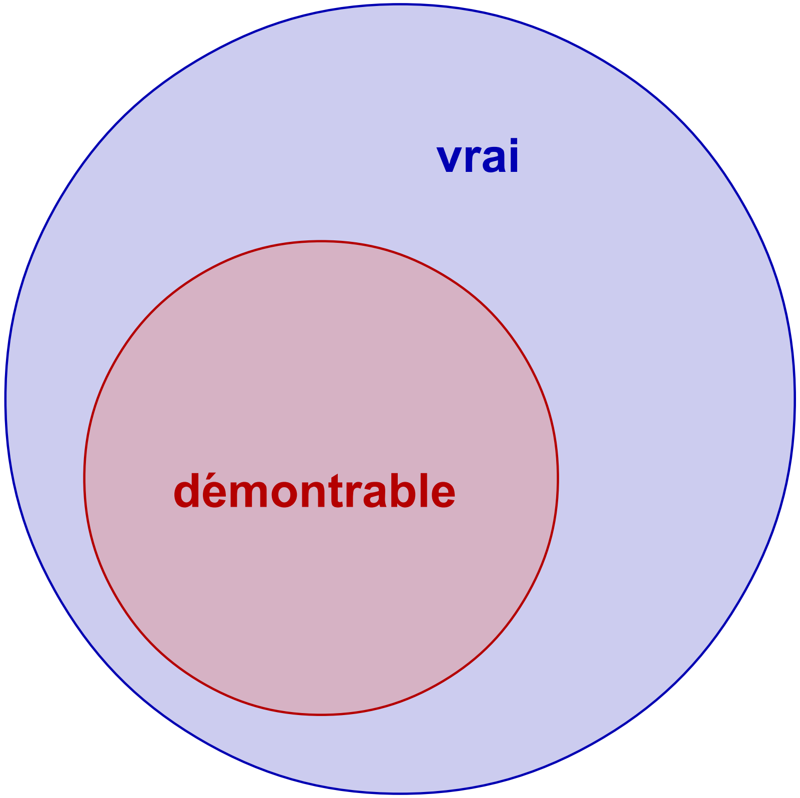
- Si une théorie comprend deux théorèmes contradictoires entre eux, on dit qu'elle est ***incohérente***.
- Si tout ce qui est vrai dans le langage d'une théorie, est un théorème, on dit que la théorie est ***complète***.

Si une théorie est incohérente alors elle est complète.

Non-contraction



Une théorie cohérente est-elle complète ?



Réponse : Ça dépend de la théorie.

La logique des propositions est complète

Emil Post a démontré en 1920
que toute tautologie
est démontrable.

De plus, la logique des
propositions est
décidable.

La logique des prédicats est complète

Kurt Gödel a démontré en 1930
que toute tautologie du
calcul des prédicats
(du premier ordre)
est démontrable.

La logique des prédicats est indécidable.

Alonzo Church a démontré
en 1936 que la logique des
prédicats
est indécidable.

La logique des prédicats est complète

Kurt Gödel a démontré en 1930
que toute tautologie du
calcul des prédicats
(du premier ordre)
est démontrable.

L'arithmétique est incomplète

Kurt Gödel a démontré en 1931 qu'il y a des propositions vraies en arithmétique, qui sont indémontrables par l'arithmétique.

« La présente proposition
est indémontrable »

L'arithmétique est incomplète

Kurt Gödel a démontré en 1931 qu'il y a des propositions vraies en arithmétique, qui sont indémontrables par l'arithmétique.

« L'arithmétique est cohérente »

L'arithmétique est incomplète

Les deux propositions suivantes sont équivalentes :

- On peut prouver (arithmétiquement) que l'arithmétique est cohérente.
- L'arithmétique n'est pas cohérente.

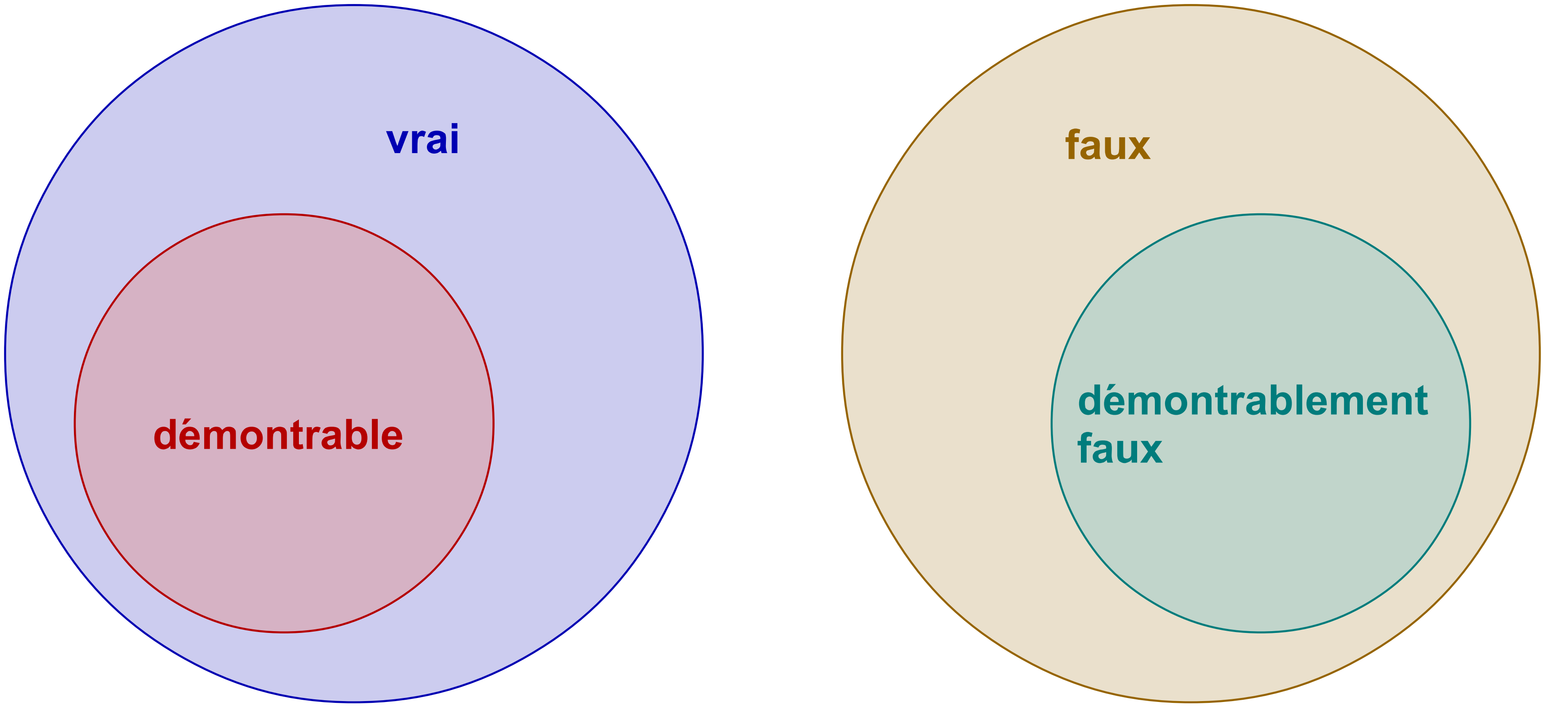
Théorème de Tarski

En 1936, Alfred Tarski
a démontré que la vérité
en arithmétique n'est pas
un prédicat arithmétique.

Logique intuitionniste

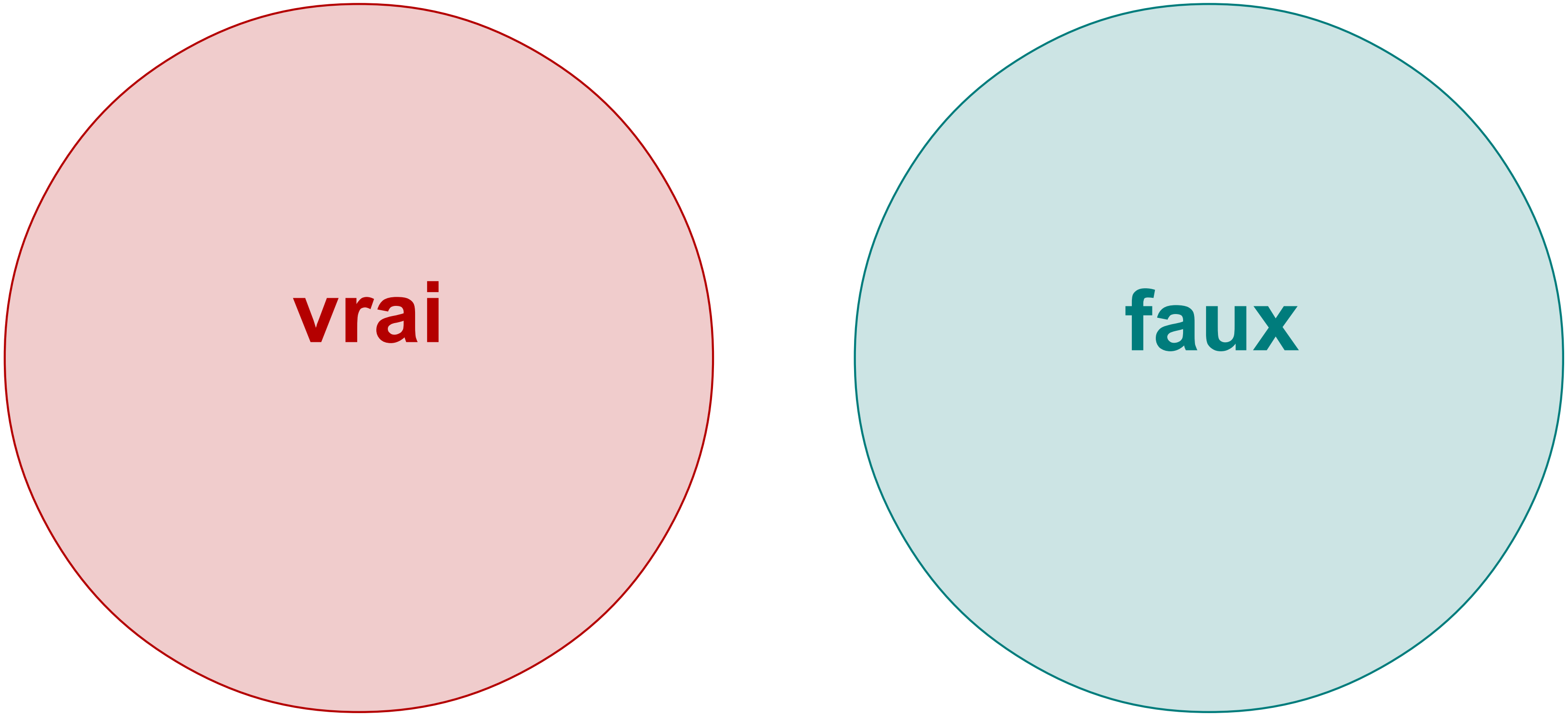
Luitzen Brouwer propose
en 1907 une logique
sans tiers exclu.
Elle consiste à ne considérer
comme vrai que ce qui est
démontrable.

Logique intuitionniste



On ne fait pas la différence entre le rouge et le bleu ni entre le cyan et le marron

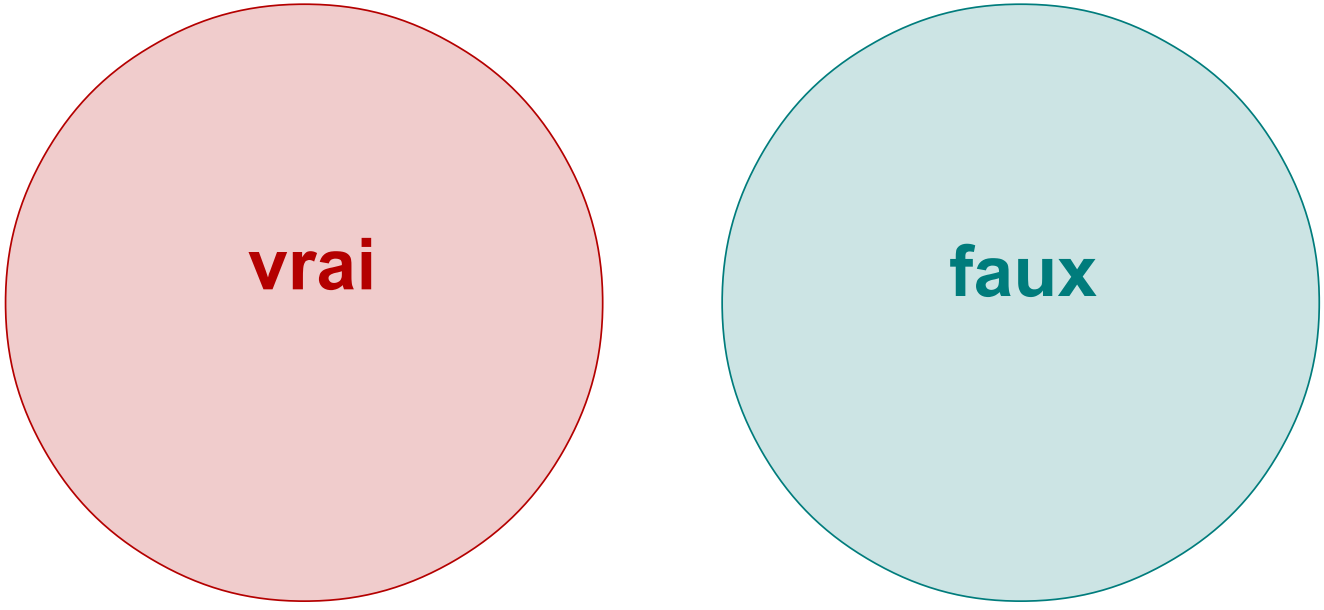
Logique intuitionniste



On ne fait pas la différence entre le rouge et le bleu ni entre le cyan et le marron

Double négation

- Si p est vraie, alors non(non p) est vraie aussi.
- Mais si non(non p) est vraie, p n'est pas forcément vraie (elle peut être indécidable).



Double négation

En 1933, Kurt Gödel a montré que
tout théorème de la logique classique
peut être démontré par la logique
intuitionniste :
La logique intuitionniste généralise
la logique classique.

Logiques ternaires

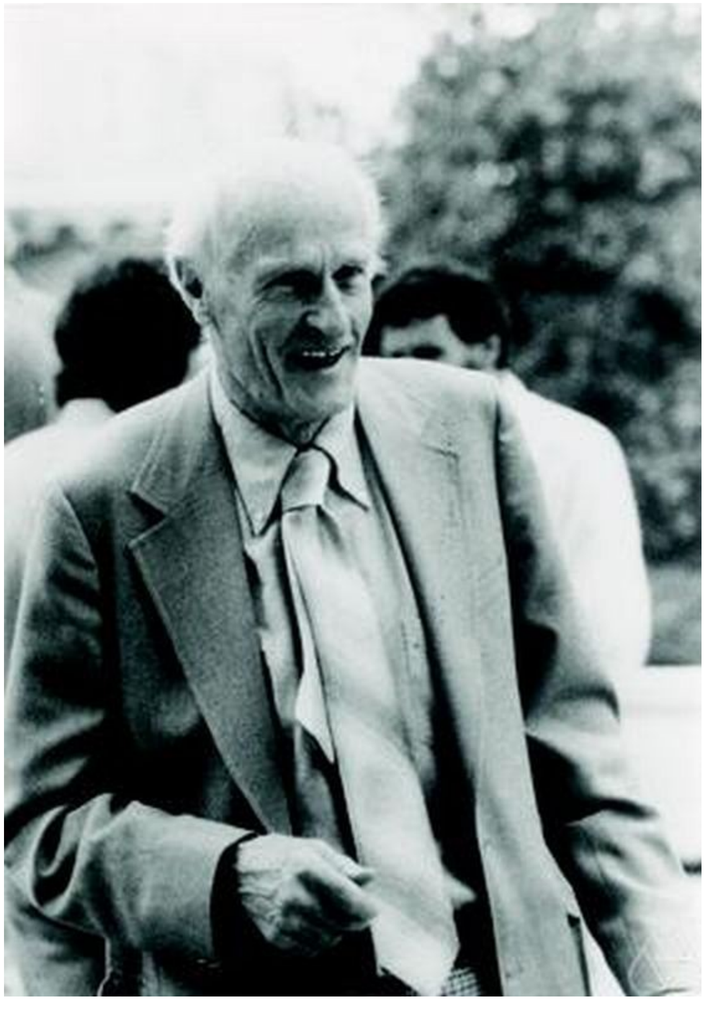
En 1921, Jan Łukasiewicz a proposé des tables de vérité à 3 niveaux :

- V pour vrai
- F pour faux
- I pour intermédiaire

Logiques ternaires

En 1938, Stephen Kleene a proposé des tables de vérité à 3 niveaux :

- V pour vrai
- F pour faux
- I pour indéterminé



Implications ternaires

Version Łukasiewicz

q p	V	I	F
V	V	I	F
I	V	V	I
F	V	V	V

Version Kleene

q p	V	I	F
V	V	I	F
I	V	I	I
F	V	V	V

Correspondance de Curry-Howard

Haskell Curry propose une équivalence entre preuves et algorithmes en 1958.
Mais son paradoxe est connu depuis 1942 :

Si cette proposition est vraie alors 2+2=5

Correspondance de Curry-Howard

Une proposition est vraie si on fournit un algorithme permettant de la prouver.
Par exemple, une preuve de « p implique q » est un algorithme transformant toute preuve de p en une preuve de q.

Calcul des constructions

En 1984, Thierry Coquand formalise mathématiquement la correspondance de Curry-Howard :
Le calcul des constructions (en abrégé CoC).
Il crée un logiciel de démonstrations mathématiques aujourd'hui appelé Coq.

Le logiciel Coq

Coq sert aussi à prouver qu'un programme ne comporte pas de bug. Mais comment prouver que Coq lui-même ne comporte pas de bug ?

Preuves par Coq

En 1995, Gilles Dowek soutient une thèse sur le calcul des constructions pour reprogrammer Coq et finalement devenir directeur de l'INRIA.

En 2007 il obtient le grand prix de philosophie de l'Académie Française pour son livre « les métamorphoses du calcul ».

La logique

Dans son livre, Gilles Dowek conclut que « changer les règles de déduction, abandonner le tiers exclu, revient à changer la signification [des] mots [et, ou, si...] »

Bibliographie

- Hao Wang : *a logical journey : From Gödel to philosophy*
- Douglas Hofstadter : *Gödel, Escher, Bach, les Brins d'une Guirlande Eternelle*.
- Raymond Smullyan : *Le livre qui rend fou*, et *ça y est, je suis fou*
- Gilles Dowek : *La logique*
- Pour la science : *Les chemins de la logique*, et la biographie de Gödel