Calculs et raisonnements de l'Antiquité à la théorie de la démonstration

Gilles Dowek

I. Dialogue sur les deux grands systèmes mathématiques

Giovanni : Comment juger que la proposition « $21 \times 2 = 42$ » est vraie ?

Muhammad : Il faut effectuer la multiplication.

David : Mais, dans la logique des prédicats, il n'y a qu'une manière de juger qu'une proposition est vraie : c'est de construire une démonstration de cette proposition.

Muhammad : Alors, il faudrait construire une démonstration de la proposition « $21 \times 2 = 42$ » ? C'est absurde. Même Poincaré reconnaît que pour juger qu'une telle proposition est vraie, il n'est pas nécessaire de construire une démonstration.

David : Peu importe ce que pense Poincaré : dans la logique des prédicats, il n'y a qu'une manière de juger qu'une proposition est vraie : c'est d'en construire une démonstration. D'ailleurs Peano a posé des axiomes qui permettent de construire une démonstration de cette proposition.

Muhammad : Alors, l'algorithme de la multiplication ne sert à rien ? Il ne fait pas partie du savoir mathématique ?

David : Si, mais il y tient un rôle secondaire de méthode de construction automatique de démonstrations de propositions closes de la forme $t \times u = v$ et $\neg(t \times u = v)$, qui constituent un fragment décidable, mais minuscule, de l'arithmétique.

Un rôle secondaire

- Les conditions de vérité d'une proposition et la signification des symboles du langage sont définies par les règles de déduction et les axiomes
- Le calcul vient dans un second temps et joue un rôle purement heuristique

C'est le cas aujourd'hui... mais cela ne l'a pas toujours été

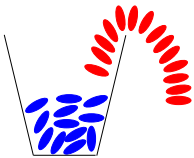
Dans les mathématiques anciennes (Mésopotamie, Égypte, Chine, etc.) le savoir mathématique est exclusivement constitué d'algorithmes

La seule manière de juger de la vérité d'une proposition est d'exécuter un algorithme

Deux questions :

- Pourquoi a-t-on eu soudainement besoin de faire des démonstrations ?
- Comment savait-on, à cette époque, que ces algorithmes étaient corrects ?

La correction de l'algorithme de l'addition



Correct parce que paraphrase de la définition

$$\begin{array}{r} 12 \\ 14 \\ \hline 26 \end{array}$$

Mais comment sait-on que cela calcule l'addition ?

Au minimum 

Même Bourbaki

...la découverte de tels procédés de résolution, dont la généralité transparaît sous les applications numériques particulières, n'a pu s'effectuer sans un minimum d'enchaînements logiques (peut-être pas entièrement conscients...

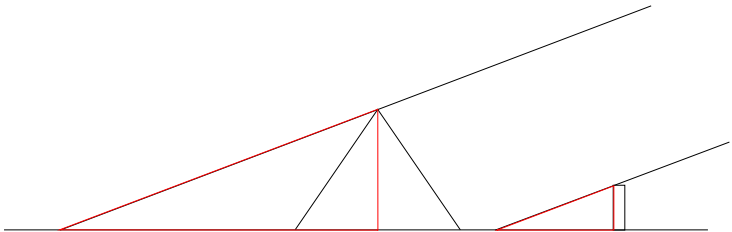
Un cas plus embêtant : l'algorithme de Pythagore

Pour calculer la longueur de l'hypoténuse d'un triangle rectangle de côtés de longueur a et b

- calculer le carré de a
- calculer le carré de b
- calculer leur somme
- calculer la racine carrée de cette somme

Peut-on savoir que cet algorithme est correct sans connaître le théorème de Pythagore ?

Un cas mieux documenté : l'algorithme de Thalès



Un théorème des mathématiques grecques, mais aussi une histoire égyptienne, racontée par des Grecs (et des Latins) : Pline, Putarque et Diogène Laërce

Un algorithme pour mesurer la hauteur de la pyramide

Dont la correction est le théorème de Thalès

Répond à la seconde question

- Pourquoi a-t-on tout à coup eu besoin de faire des démonstrations ?
- Comment savait-on à cette époque que ces algorithmes étaient corrects ?

Mais aussi à la première

Pourquoi le calcul a-t-il été dévalorisé par rapport au raisonnement à partir des Grecs ?

Parce que les Grecs n'aimaient pas beaucoup les comptables et les arpenteurs (?)

Le mathématicien comme grand prêtre (Pythagore) : le nombre quitte sa fonction pratique pour prendre une fonction mystique

II. Le calcul contre attaque

Mais avec beaucoup de maladresse

Le programme de Hilbert : (pour résoudre le problème de la cohérence) revenir aux mathématique anciennes où la seule manière de juger de la vérité d'une proposition est d'exécuter un algorithme

Pas possible dès que l'on a $+$, $\times$ et $\exists$ (Church, Turing, Matiiassevitch)

Une meilleure idée

Au lieu de remplacer le raisonnement par le calcul

Les faire vivre ensemble

Vivre ensemble

Pas besoin des axiomes (de Peano)

$$\forall x\ (x + 0 = x)$$

$$\forall x \forall y\ (x + S(y) = S(x + y))$$

Mais de règles de calcul (de réduction, de réécriture)

$$x + 0 \longrightarrow x$$

$$x + S(y) \longrightarrow S(x + y)$$

Vivre ensemble

Ainsi pour juger vraie la proposition

$$21 + 21 = 42$$

On commence par la calculer

$$42 = 42$$

que l'on démontre à partir de l'axiome $\forall x\ (x = x)$

Calcul et déduction

On veut

$$\frac{\Gamma \vdash 2 \times 2 = 4}{\Gamma \vdash \exists x\, (2 \times x = 4)}\ \exists\text{-intro}$$

mais aussi

$$\frac{\Gamma \vdash 4 = 4}{\Gamma \vdash \exists x\, (2 \times x = 4)}\ \exists\text{-intro}$$

Règles de déduction

Remplacer la règle

$$\frac{\Gamma \vdash (t/x)A}{\Gamma \vdash \exists x\, A}\ \exists\text{-intro}$$

par

$$\frac{\Gamma \vdash B}{\Gamma \vdash \exists x\, A}\ \exists\text{-intro si } B \equiv (t/x)A$$

où la relation $\equiv$ est définie par un ensemble de règles de calcul
Une théorie est formée

- d'axiomes
- de règles de calcul

Une idée qui a plusieurs origines

- Démonstration automatique (Knuth et Bendix, Boyer et Moore, Plotkin, Andrews et Huet...)
- La substitution d'ordre supérieur (Russell, Whitehead, Church, Henkin, Prawitz...)
- La théorie des types (Martin-Löf, Coquand-Huet...)

III. Un exemple de théorie calculatoire : l'arithmétique

Les axiomes de l'arithmétique

Les axiomes de l'égalité

3

$$\forall x \forall y \, (S(x) = S(y) \Rightarrow x = y)$$

4

$$\forall x \, \neg(0 = S(x))$$

5 (schéma de récurrence)

$$(0/w)A \Rightarrow \forall x \, ((x/w)A \Rightarrow (S(x)/w)A) \Rightarrow \forall y \, ((y/w)A)$$

Les axiomes de l'addition et de la multiplication

$$\forall y \, (0 + y = y)$$

$$\forall x \forall y \, (S(x) + y = S(x + y))$$

$$\forall y \, (0 \times y = 0)$$

$$\forall x \forall y \, (S(x) \times y = (x \times y) + y)$$

Utiliser ces axiomes pour démontrer $\forall y\ (y + 0 = y)$?

Au lycée

Cas de base : $0 + 0 = 0$
conséquence de l'axiome $\forall y\ (0 + y = y)$

Hérédité : $\forall x\ (x + 0 = x \Rightarrow S(x) + 0 = S(x))$
conséquence de l'axiome $\forall x\ \forall y\ (S(x) + y = S(x + y))$

Mais comment sait-on que

$$0 + 0 = 0 \Rightarrow \forall x\,(x + 0 = x \Rightarrow S(x) + 0 = S(x)) \Rightarrow \forall y\,(y + 0 = y)\ ?$$

C'est une instance du schéma de récurrence

$$(0/w)A \Rightarrow \forall x\,((x/w)A \Rightarrow (S(x)/w)A) \Rightarrow \forall y\,((y/w)A)$$

pour $A = w + 0 = w$

Quatre très faciles

$$0 + y \longrightarrow y$$

$$S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0$$

$$S(x) \times y \longrightarrow (x \times y) + y$$

Deux faciles

3

$$\forall x \forall y \, (S(x) = S(y) \Rightarrow x = y)$$

4

$$\forall x \, \neg(0 = S(x))$$

$$Pred(0) \longrightarrow 0$$

$$Pred(S(x)) \longrightarrow x$$

$$Positive(0) \longrightarrow \bot$$

$$Positive(S(x)) \longrightarrow \top$$

Le schéma de récurrence

$$(0/w)A \Rightarrow \forall x\,((x/w)A \Rightarrow (S(x)/w)A) \Rightarrow \forall y\,((y/w)A)$$

Remplacer ce schéma par un axiome unique

Plusieurs sortes : une pour les nombres entiers et une nouvelle pour les “classes” (ensembles) de nombres entiers
Un symbole de prédicat ϵ pour l’appartenance

Récurrence

$$\forall c\,(0 \,\epsilon\, c \Rightarrow \forall x\,(x \,\epsilon\, c \Rightarrow S(x) \,\epsilon\, c) \Rightarrow \forall y\; y \,\epsilon\, c)$$

Les classes qui contiennent 0 et sont closes par S contiennent tout

Le schéma de compréhension

Besoin d'un schéma pour construire les classes

$$\forall x_1 ... \forall x_n \exists c \forall y \ (y \in c \Leftrightarrow A)$$

A ne contient pas ϵ

Un schéma $\longrightarrow$ un axiome + un schéma : le progrès n'est pas évident

Mais...

Le schéma de compréhension peut se skolémiser

$$\forall x_1 ... \forall x_n \exists c \forall y \ (y \in c \Leftrightarrow A)$$

$$\forall x_1 ... \forall x_n \forall y \ (y \in f_{x_1,...,x_n,y,A}(x_1, ..., x_n) \Leftrightarrow A)$$

et s'orienter en une règle de calcul

$$y \in f_{x_1,...,x_n,y,A}(x_1, ..., x_n) \longrightarrow A$$

Exercice : un nombre fini d'axiomes (de règles)

Un peu de vocabulaire : la théorie de classes est parfois appelée « logique du second ordre »

Au passage (Leibniz)

Les classes permettent aussi de traiter le cas des axiomes de l'égalité

$$x = y \longrightarrow \forall c \, (x \in c \Rightarrow y \in c)$$

Reste...

L'axiome de récurrence proprement dit

$$\forall c \, (0 \in c \Rightarrow \forall x \, (x \in c \Rightarrow S(x) \in c) \Rightarrow \forall y \; y \in c)$$

Les classes qui contiennent 0 et sont closes par S contiennent tout
Impossible à transformer en une règle de calcul

Peano n'avait pas formulé l'axiome ainsi, mais sous la forme
Les classes qui contiennent 0 et sont closes par S contiennent tous les nombres entiers

Le symbole de Peano

Un symbole de prédicat : N
$N(t)$ exprime que t est un entier
Axiomes 1 et 2

$$N(0)$$

$$\forall x \, (N(x) \Rightarrow N(S(x)))$$

Mais aussi récurrence

$$\forall c \, (0 \in c \Rightarrow \forall x \, (x \in c \Rightarrow S(x) \in c) \Rightarrow \forall y \, (N(y) \Rightarrow y \in c))$$

$$\forall y\ (N(y) \Rightarrow \forall c\ (0 \in c \Rightarrow \forall x\ (x \in c \Rightarrow S(x) \in c) \Rightarrow y \in c))$$

à la place de (1) et (2)

$$\forall y\ (N(y) \Leftrightarrow \forall c\ (0 \in c \Rightarrow \forall x\ (x \in c \Rightarrow S(x) \in c) \Rightarrow y \in c))$$

S'oriente en

$$N(y) \longrightarrow \forall c\ (0 \in c \Rightarrow \forall x\ (x \in c \Rightarrow S(x) \in c) \Rightarrow y \in c)$$

~~Les classes qui contiennent 0 et sont closes par S contiennent tous les nombres entiers~~
Un nombre entier est ce qui appartient à toutes les classes qui contiennent 0 et sont closes par S
Une définition ?

$$0 + y \longrightarrow y$$
$$S(x) + y \longrightarrow S(x + y)$$

$$0 \times y \longrightarrow 0$$
$$S(x) \times y \longrightarrow (x \times y) + y$$

$$Pred(0) \longrightarrow 0$$
$$Pred(S(x)) \longrightarrow x$$

$$Positive(0) \longrightarrow \bot$$
$$Positive(S(x)) \longrightarrow \top$$

$$y \in f_{x_1,\ldots,x_n,y,A}(x_1, \ldots, x_n) \longrightarrow A$$

$$x = y \longrightarrow \forall c \, (x \in c \Rightarrow y \in c)$$

$$N(y) \longrightarrow \forall c \, (0 \in c \Rightarrow \forall x \, (x \in c \Rightarrow S(x) \in c) \Rightarrow y \in c)$$

Sont-ce des définitions ?

- Modularité, mais expressivité ontologique
- Dépend des règles

Mais moins implicites (déguisées) que les axiomes (Poincaré, Hilbert)

IV. Une idée fertile en théorie de la démonstration : l'élimination des coupures pour les théories axiomatiques

La déduction naturelle

Règles d'introduction

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\text{-intro}$$

Règles d'élimination

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\text{-élim} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\text{-élim}$$

La règle axiome

$$\frac{}{\Gamma, A \vdash A} \text{ axiome}$$

~~La règle du tiers exclu~~

Des détours dans les démonstrations

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \quad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ \wedge\text{-intro}}{\Gamma \vdash A}\ \wedge\text{-élim}$$

Une démonstration plus simple : π_1

Une coupure : une règle d'introduction suivie par une règle d'élimination

D'autres exemples

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash \forall x\, A}\ \forall\text{-intro}}{\Gamma \vdash (t/x)A}\ \forall\text{-élim}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow\text{-intro} \qquad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash B}\ \Rightarrow\text{-élim}$$

Le nombre de coupures décroît-il quand on élimine une coupure ?

Pas toujours

$$\dfrac{\dfrac{\dfrac{\dfrac{\dots}{\Gamma \vdash A} \quad \dfrac{\dots}{\Gamma \vdash A'}}{\Gamma \vdash A \wedge A'}\ \wedge\text{-intro} \quad \dfrac{\dots}{\Gamma \vdash B}}{\Gamma \vdash (A \wedge A') \wedge B}\ \wedge\text{-intro}}{\dfrac{\Gamma \vdash A \wedge A'}{\Gamma \vdash A}\ \wedge\text{-élim}}\ \wedge\text{-élim}$$

Coupure créée par l'élimination d'une coupure
La taille de la démonstration ne décroît pas non plus systématiquement (substitution)

Mais l'élimination des coupures termine toujours et produit une démonstration sans coupures

Un lemme

Si une démonstration est

- constructive
- sans coupures
- sans axiomes $\emptyset \vdash A$

elle se termine par une règle d'introduction

Elle ne se termine pas par une règle axiome (sans axiomes)
Elle ne se termine pas par une règle d'élimination, par exemple

$$\dfrac{\dfrac{\pi_1}{\vdash A \Rightarrow B} \quad \dfrac{\pi_2}{\vdash A}}{\vdash B} \Rightarrow\text{-élim}$$

appliquer l'hypothèse de récurrence à π_1

Corollaires I : cohérence et indépendance

$\vdash \bot$ n'a pas de démonstration sans coupures, donc pas de démonstration du tout

$\vdash P$ (P atomique) n'a pas de démonstration sans coupures, donc pas de démonstration du tout

Corollaires II : disjonction et témoin

Si $\vdash \exists x\ A$ a une démonstration, elle a une démonstration sans coupures, se terminant par une règle d'introduction

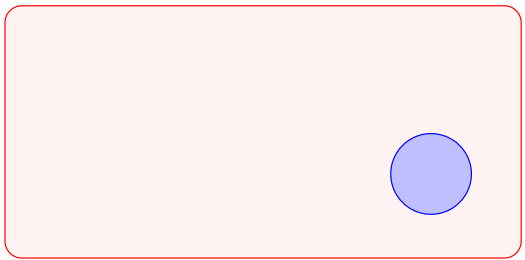
$$\dfrac{\dfrac{}{\vdash (t/x)A}}{\vdash \exists x\ A}$$

donc un témoin t
Le terme t tricoté pendant l'élimination des coupures

Propriété similaire pour la disjonction

Corollaires III : démonstration automatique et décidabilité

Réduction de l'espace de recherche



démonstrations

démonstrations sans coupures

Si par chance l'espace bleu est fini (exemple : la logique propositionnelle) : décidabilité

Un lemme

Si une démonstration est

- constructive
- sans coupures
- sans axiomes $\emptyset \vdash A$

elle se termine par une règle d'introduction

Constructive : une restriction (mais il y a beaucoup de démonstrations constructives en mathématiques)
sans coupures : pas une restriction (théorème d'élimination des coupures)
Sans axiomes : une restriction importante (qui s'intéresse aux démonstrations dans la théorie vide ?)

Quid d'une démonstration sans coupures de $\Gamma \vdash A$?

(I) Pas de propriété de cohérence, ni d'indépendance (et pas d'espoir d'en avoir)

(II) Pas de propriété de la disjonction, ni du témoin (et pas d'espoir d'en avoir)

(III) L'espace de recherche d'une démonstration sans coupures de $\Gamma \vdash A$ est plus petit que l'espace de toutes les démonstrations de $\Gamma \vdash A$
mais l'espace de recherche d'une démonstration sans coupures de $\Gamma \vdash \bot$ n'est pas vide (même si vous savez que la théorie est cohérente, votre système non)

Trois manières d'étendre le th. d'élimination des coupures à une théorie
I : les coupures *ad hoc*

Ajouter des règles de réductions spécifiques à certains axiomes

$$\dfrac{\dfrac{}{\Gamma \vdash I}\ \text{axiome} \quad \dfrac{\dfrac{\pi_1}{\Gamma \vdash P(0)} \quad \dfrac{\pi_2}{\Gamma \vdash \forall x\ (P(x) \Rightarrow P(S(n))}\ \Rightarrow\text{-élim (2)}}{\Gamma \vdash \forall n\ P(n)}\ \forall\text{-élim}}{\Gamma \vdash P(2)}$$

$$I = P(0) \Rightarrow (\forall x\ (P(x) \Rightarrow P(S(x)))) \Rightarrow (\forall n\ P(n))$$

$$\dfrac{\dfrac{\dfrac{\pi_2}{\forall x\,(P(x) \Rightarrow P(S(x)))}}{P(1) \Rightarrow P(2)}\,\forall\text{-élim} \qquad \dfrac{\dfrac{\dfrac{\pi_2}{\forall x\,(P(x) \Rightarrow P(S(x)))}}{P(0) \Rightarrow P(1)}\,\forall\text{-élim} \quad \dfrac{\pi_1}{P(0)}}{P(1)}\,\Rightarrow\text{-élim}}{\Gamma \vdash P(2)}\,\Rightarrow\text{-élim}$$

L'élimination des coupures (incluant les coupures de récurrence) termine

Démonstration sans coupures de $I \vdash \exists x\ A\ (A \vee B, \bot)$ se termine par une règle d'introduction

Pas de démonstration sans coupures of $I \vdash \bot$

Démonstration automatique : comparer la recherche d'une démonstration sans coupures de $I \vdash \bot$, dans l'ancien et nouveau sens

Quelles théories ?

Notion similaire de coupure (et d'élimination des coupures) pour les axiomes de l'égalité
Les autres axiomes de l'arithmétique sont inoffensifs

Mais chaque axiome demande une notion de coupure
Quid de la théorie des ensembles ? De la géométrie ?

Le problème vient de la notion d'axiome en elle-même

Trois manières d'étendre le th. d'élimination des coupures à une théorie
II : exprimer la théorie par des règles de déduction

Plutôt que l'axiome

$$\forall x \forall y \forall z \, (x \in \{y, z\} \Leftrightarrow (x = y \vee x = z))$$

ajouter les règles de conversion

$$\frac{\Gamma \vdash a \in \{b, c\}}{\Gamma \vdash a = b \vee a = c}$$

$$\frac{\Gamma \vdash a = b \vee a = c}{\Gamma \vdash a \in \{b, c\}}$$

Un exemple

$$\dfrac{\dfrac{\dfrac{\dots}{\Gamma \vdash 1 = 1}}{\Gamma \vdash 1 = 1 \vee 1 = 2}\ \vee\text{-intro}}{\Gamma \vdash 1 \in \{1, 2\}}\ \text{conversion}$$

Les règles de conversion peuvent bloquer les coupures

$$\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash P} \quad \dfrac{\pi_2}{\Gamma \vdash Q}}{\Gamma \vdash P \wedge Q}\ \wedge\text{-intro}}{\Gamma \vdash R \wedge S}\ \text{conversion}}{\Gamma \vdash R}\ \wedge\text{-élim}$$

Mais pas

$$\dfrac{\dfrac{\Gamma \vdash a \in \{b, c\}}{\Gamma \vdash a = b \vee a = c}}{\Gamma \vdash a \in \{b, c\}}$$

Atomique

En revanche

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash a = b \vee a = c}}{\Gamma \vdash a \in \{b, c\}}}{\Gamma \vdash a = b \vee a = c}$$

se réduit en π

Prawitz, Crabbé, Hallnäs, Ekman, Plato, Negri...

Trois manières d'étendre le th. d'élimination des coupures à une théorie
III : exprimer la théorie par des règles de calcul

$$\frac{\Gamma \vdash B}{\Gamma \vdash \exists x\, A}\ \exists\text{-intro si } B \equiv (t/x)A$$

Un exemple

$a \in \{b, c\} \longrightarrow a = b \vee a = c$

$$\dfrac{\dfrac{\dots}{\Gamma \vdash 1 = 1}}{\Gamma \vdash 1 \in \{1, 2\}} \vee\text{-intro}$$

Tout dépend de la théorie

L'élimination des coupures ne termine pas toujours (ni avec une règle de conversion, ni avec des règles de calcul)

$A \to (A \Rightarrow \bot)$

$$\dfrac{\dfrac{\dfrac{}{A \vdash A \Rightarrow \bot}\ \text{axiome} \quad \dfrac{}{A \vdash A}\ \text{axiome}}{\dfrac{A \vdash \bot}{\vdash A \Rightarrow \bot}\ \Rightarrow\text{-intro}}\ \Rightarrow\text{-élim} \quad \dfrac{\dfrac{}{A \vdash \neg A}\ \text{axiome} \quad \dfrac{}{A \vdash A}\ \text{axiome}}{\dfrac{A \vdash \bot}{\vdash A}\ \Rightarrow\text{-intro}}\ \Rightarrow\text{-élim}}{\vdash \bot}\ \Rightarrow\text{-élim}$$

$A \to (A \Rightarrow B)$

$A \to C \wedge (A \Rightarrow B)$

Même des contre-exemples confluents et terminants

Mais quand l'élimination des coupures termine

- Cohérence
- Disjonction et témoin
- Réduction de l'espace de recherche

Exemples

Toutes les théories définies par des règles de calcul sur les termes
Toutes les théories définies par des règles de calcul confluentes and terminantes sans quantificateurs
Toutes les théories définies par des règles de calcul positives, confluentes and terminantes
La théorie des types simples
L'arithmétique
(certaines formulation de) la théorie des ensembles

Remettre le calcul au centre des mathématiques

- À la fois un objectif « idéologique » : interface avec l'informatique, et plus généralement avec les utilisations pratiques des mathématiques (comptabilité, arpentage, ingénierie...)
- Mais aussi « philosophique » : aller au delà de la définition implicite (holistique) des concepts mathématiques par des axiomes
- Et « logique » : la théorie de la démonstration butte sur les axiomes : remplaçons les par des règles de calcul