Une démonstration trop rapide et sa relecture constructive

Il s'agit d'arithmétique avec les entiers usuels.

Le théorème convoité dit que si a et b sont deux entiers > 1, et si g est leur plus grand commun diviseur, alors tout diviseur de a et b est un diviseur de g.

La démonstration n'est pas simple. On a compris que cela résultait d'un calcul astucieux « l'algorithme d'Euclide ».

Et on a donné le résultat sous une forme plus forte (et plus facile à démontrer) qui s'appelle le **théorème de Bézout**, lequel résulte de l'algorithme d'Euclide.

Théorème. Il existe u et v *dans* **N** tels que $u\,a - v\,b$ *ou* $v\,b - u\,a$ (positif) divise a et b.

Au lieu de prendre u et v dans **N** on les prend dans **Z** et le théorème s'énonce :
Il existe u et v dans **Z** tels que $u\,a + v\,b \geq 1$ divise a et b.

Ainsi, si c divise a et b, il divise $g = u\,a + v\,b$.

Gauss ayant éclairci les choses et démontré correctement le théorème de décomposition unique en facteurs premiers, on aurait pu en rester là.

Mais les adeptes de démonstrations miraculeuses ont voulu « améliorer » la démonstration de Gauss. Plus de calcul ! uniquement un raisonnement abstrait fulgurant ! C'est le suivant.

> *Considérons parmi les entiers naturels > 0 le plus petit qui puisse s'écrire sous la forme $u\,a + v\,b$. Alors on démontre par l'absurde que cet entier g divise a et b.*

Le programme de Hilbert concernant cette démonstration nous dit de la **décrypter**, de trouver un calcul **caché dans la démonstration** pour trouver u et v.

Note : la démonstration éclair a plusieurs défauts. En particulier elle ne nous dit pas comment calculer g.
Simplement, elle a comme conséquence le calcul suivant : parmi les entiers naturels ≤ a et b, cherchons le plus grand qui divise a et b.
Alors il doit exister u et v tels que $u\,a + v\,b = g$.
Quels autres défauts ?

Décryptage de la démonstration fulgurante

Le débat Russel-Poincaré

La lecture des écrits suivants de Poincaré est vivement recommandée

La Science et l'Hypothèse.
Première partie : Chapitre I. Le nombre et la grandeur.
— sur le raisonnement mathématique (la récurrence)
Première partie : Chapitre II. La grandeur mathématique et l'expérience.
— qu'est-ce que le continu ?

Science et Méthode
Livre II le raisonnement mathématique
Chapitre III Les mathématiques et la logique
— critique du formalisme

Dernières Pensées
Chapitre IV La logique de l'infini
— critique de l'infini actuel, que sont les objets mathématiques ?
Chapitre V Les mathématiques et la logique
— les pragmatistes contre les cantoriens

Prédicativité : la nécessité de construire les objets mathématiques dans un ordre naturel raisonnable

https://classiques.uqam.ca/classiques/poincare_henri/science_et_hypothese/science_et_hypothese.pdf

https://classiques.uqam.ca/classiques/poincare_henri/Dernieres_pensees/Dernieres_pensees.pdf

https://classiques.uqam.ca/classiques/poincare_henri/Science_et_methode/Science_et_methode.pdf

https://poincare.univ-lorraine.fr/

Lisons la conclusion de La logique de l'infini dans Dernières Pensées
texte paru la première fois dans
Revue de Métaphysique et de Morale, 1909

§7 Résumé

Les antinomies auxquelles certains logiciens ont été conduits proviennent de ce qu'ils n'ont pas pu éviter certains cercles vicieux. Cela leur est arrivé quand ils considéraient des collections finies, mais cela leur est arrivé bien plus souvent quand ils avaient la prétention de traiter des collections infinies. Dans le premier cas, ils auraient pu éviter aisément le piège où ils sont tombés ; ou plus exactement ils ont eux-mêmes tendu le piège où ils se sont amusés à tomber, et même ils ont été obligés de faire bien attention pour ne pas tomber à côté du piège ; en un mot, dans ce cas les antinomies ne sont que des joujoux. Bien différentes sont celles qu'engendre la notion de l'infini ; il arrive souvent qu'on y tombe sans le faire exprès, et même quand on est averti, on n'est pas encore bien tranquille.

Les tentatives qui ont été faites pour sortir de ces difficultés sont intéressantes à plus d'un titre, mais elles ne sont pas entièrement satisfaisantes. M. Zermelo a voulu construire un système impeccable d'axiomes ; mais ces axiomes ne peuvent être regardés comme des décrets arbitraires, puisqu'il faudrait démontrer que ces décrets ne sont pas contradictoires, et qu'ayant fait entièrement table rase on n'a plus rien sur quoi l'on puisse appuyer une semblable démonstration. Il faut donc que ces axiomes soient évidents par eux-mêmes. Or quel est le mécanisme par lequel on les a construits ? on a pris les axiomes qui sont vrais des collections finies ; on ne pouvait les étendre tous aux collections infinies, on n'a fait cette extension que pour un certain nombre d'entre eux, choisis plus ou moins arbitrairement. À mon sens, d'ailleurs, ainsi que je l'ai dit plus haut, aucune proposition concernant les collections infinies ne peut être évidente par intuition.

M. Russell a mieux compris la nature de la difficulté à vaincre, il ne l'a cependant pas entièrement vaincue, parce que sa hiérarchie des types suppose la théorie des ordinaux déjà faite.

Quant à moi, je proposerais de s'en tenir aux règles suivantes :

> 1° Ne jamais envisager que des objets susceptibles d'être définis en un nombre fini de mots ;
>
> 2° Ne jamais perdre de vue que toute proposition sur l'infini doit être la traduction, l'énoncé abrégé de propositions sur le fini ;
>
> 3° Éviter les classifications et les définitions non prédicatives.

Toutes les recherches dont nous avons parlé ont un caractère commun. On se propose d'enseigner les mathématiques à un élève qui ne sait pas encore la différence qu'il y a entre l'infini et le fini ; on ne se hâte pas de lui apprendre en quoi consiste cette différence ; on commence par lui montrer tout ce qu'on peut savoir de l'infini sans se préoccuper de cette distinction ; puis dans une région écartée du champ qu'on lui a fait parcourir, on lui découvre un petit coin où se cachent les nombres finis.

Cela me paraît psychologiquement faux ; ce n'est pas ainsi que l'esprit humain procède naturellement, et quand même on devrait s'en tirer sans trop de mésaventures antinomiques, cela n'en serait pas moins une méthode contraire à toute saine psychologie.

M. Russell me dira sans doute qu'il ne s'agit pas de psychologie, mais de logique et d'épistémologie ; et moi, je serai conduit à répondre qu'il n'y a pas de logique et d'épistémologie indépendantes de la psychologie ; et cette profession de foi clora probablement la discussion parce qu'elle mettra en évidence une irrémédiable divergence de vues.

Brouwer et la critique du principe du tiers exclu

Un exemple simple.

Théorème Si $\mathbf{k}$ est un corps, tout polynôme $p \in \mathbf{k}[X]$ de degré ≥ 1 possède un facteur irréductible.

Arguments classiques possibles, éventuellement proches d'un algorithme, pour calculer un facteur irréductible ?

Comment **décrypter**, mettre à jour et utiliser le **calcul caché dans la démonstration classique ?**

Une réponse pour le théorème précédent est donnée en calcul formel :

D5 Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In EUROCAL '85. European Conference on Computer Algebra, Linz, Austria, April 1-3, 1985. Proceedings. Vol. 2: Research contributions, edited by Bob F. Caviness, 289–290. Lecture Notes in Computer Science, 204, Springer, Berlin, 1985.

Exemples à priori plus problématiques en analyse

Comment fonder l'analyse sur $\mathbf{R}$ alors qu'on n'a pas de test de signe ?

Une solution se trouve dans le livre de Bishop (1967). Voir plus loin.

Des exemples élémentaires :
— le théorème des valeurs intermédiaires
— une fonction continue sur un intervalle compact atteint ses bornes

Mais aussi, que nous dit Cedric Villani ?

http://hlombardi.free.fr/Villani-ana2.pdf

Analyse II

Cours de deuxième année donné à l'Ecole normale supérieure de Lyon

année universitaire 2003-2004

Cédric Villani

Table des matières

I-2. Résultats de continuité automatique

Dans cette section, nous allons passer en revue quelques théorèmes très utilisés en analyse fonctionnelle, qui ont tous la forme générale : sous certaines hypothèses de complétude, certaines applications (linéaires ou bilinéaires) sont automatiquement continues. Très puissants, ces résultats rendent de grands services dans les démonstrations théoriques, mais il convient de les considérer avec la plus grande méfiance: du fait de leur côté non constructif, ils mèneront presque toujours, dans des situations concrètes, à des résultats désastreux. Ainsi, ils ne donnent aucun ordre de grandeur des constantes mises en jeu (normes d'applications linéaires continues, etc.), et il est en pratique impossible d'adapter leur preuve pour obtenir de telles estimations constructives. En particulier, il est en pratique inutile de connaître leur démonstration, et nous les admettrons tous.

Nous recenserons trois grands principes : le théorème de Banach-Steinhaus, celui du graphe fermé, et celui de l'application ouverte. Leur démonstration est d'habitude subordonnée au théorème de Baire : dans un espace métrique complet, une intersection dénombrable d'ouverts denses est dense. Les preuves qui en résultent ne sont pas très difficiles mais particulièrement opaques à l'intuition (voir [Rudin]). On peut souvent se passer de cet usage du théorème de Baire, mais la complétude est une hypothèse essentielle.

....

I-3. Résultats d'existence et de compacité

...

Théorème I-50 (existence d'une forme linéaire normalisante). Soient E un espace vectoriel normé séparable, et $x0 \neq 0$ un élément de E. Alors il existe une forme linéaire $\Lambda \in E^*$, de norme 1, telle que $\Lambda(x0) = || x0 ||$.

Remarque I-51. La forme forte de l'axiome du choix permet de se passer de l'hypothèse de séparabilité.

Remarque I-52. Encore une fois, ce théorème rend service dans le développement de la théorie générale des espaces vectoriels topologiques, mais ce serait une grave erreur de l'appliquer dans des espaces familiers, tels que $\mathbf{L}_p(\mathbf{R}^n)$. En effet, dans ce cas particulier, non seulement on peut démontrer le résultat de manière très simple, mais en plus on peut construire la forme linéaire Λ explicitement, ce qui est infiniment plus intéressant.

La réponse de Hilbert aux critiques de Poincaré et Brouwer

Arithmétisation des mathématiques !

Plutôt que justifier la « sémantique » des ensembles infinis de Cantor, on peut se contenter de justifier leur « syntaxe », cad démontrer que le discours purement formel qui reprend les intuitions principales de Cantor comme des axiomes ne produit pas de contradiction.

Invention géniale : la **théorie de la démonstration**, la logique mathématique et la métamathématique.

Russel a préparé le terrain avec la nouvelle édition des Principia Mathematicae en 2025 (Russel et Whitehead). La théorie des types (théorie d'une hiérarchie de types) est rendue plus lisible par l'ajout d'axiomes concernant l'égalité. Voir la leçon inaugurale de Thierry Coquand.
https://www.college-de-france.fr/fr/agenda/lecon-inaugurale/la-theorie-des-types-de-russell-aux-assistants-la-demonstration/la-theorie-des-types-de-russell-aux-assistants-la-demonstration

Une réponse humoristique de Brouwer à la découverte d'une démonstration de non contradiction dans une théorie formelle :
« ce n'est pas parce que l'enquête n'a pas déterminé qui était le criminel que le crime n'a pas eu lieu. »

Gödel trouve le criminel

Gentzen plaide que Hilbert n'est pas coupable, car il n'y a pas vraiment de criminel

Conséquence bizarre de l'arithmétisation des mathématiques : peut-on vraiment réduire les mathématiques à l'étude des valeurs d'une fonction simple $\mathbf{N} \to \mathbf{N}$? **.** Celle qui énumère les « numéros » des théorèmes démontrables dans la théorie formelle considérée.

Pas étonnant que cela ait échoué.

Bishop - Foundations of Constructive Analysis - 1967

http://hlombardi.free.fr/Bishop.djvu

Extrait de la préface

This book is a piece of constructivist propaganda, designed to show that there does exist a satisfactory alternative. To this end we develop a large portion of abstract analysis within a constructive framework. This development is carried through with an absolute minimum of philosophical prejudice concerning the nature of constructive mathematics. There are no dogmas to which we must conform.

Our program is simple: to give numerical meaning to as much as possible of classical abstract analysis. Our motivation is the well-known scandal, exposed by Brouwer (and others) in great detail, that classical mathematics is deficient in numerical meaning.

...

The task of making analysis constructive is guided by three basic principles. First, to make every concept affirmative. (Even the concept of inequality is affirmative.) Second, to avoid definitions that are not relevant. (The concept of a pointwise continuous function is not relevant. A continuous function is one that is uniformly continuous on compact intervals.) Third, to avoid pseudogenerality. (Separability hypotheses are freely employed.)

...

We are not contending that idealistic mathematics is worthless from the constructive point of view. This would be as silly as contending that unrigorous mathematics is worthless from the classical point of view. Every theorem proved with idealistic methods presents a challenge: to find a constructive version, and to give it a constructive proof.

Le programme de Hilbert revisité, 1

De manière générale, on remplace les exigences finitistes dans le programme de Hilbert initial par des exigences constructives minimalistes à la Bishop.

Qu'est-ce qu'une version constructive d'un théorème classique ?

La version de Hilbert consistait à examiner des théories formelles du premier ordre, comme **ZF**, et à essayer de prouver leur consistance par des moyens mathématiques élémentaires.

Une contrepartie constructive possible de l'approche formelle de Hilbert est basée sur l'étude de théories formelles particulières, appelées « théories géométriques ».

On peut cependant traduire cet arrière fond logique en termes purement algébriques, sans effrayer les mathématicien.ne.s.

Nous parlerons dans ce qui suit principalement d'Algèbre.

Quelques exemples

— Le lemme de Krull

— Les modules projectifs de type fini (les matrices de projection)

— Le spectre de Zariski et la dimension de Krull

— Le corps de racines d'un polynôme séparable

— La clôture réelle d'un corps ordonné discret

— Qu'est-ce qu'un corps ordonné sans test de signe ?

— Qu'est-ce qu'un corps réel clos sans test de signe ?

Le programme de Hilbert revisité, 2

Le succès de ce programme reste à confirmer, mais il a déjà produit trois livres d'algèbre fondamentale qui n'utilisent pas la négation, et il se confirme par la publication régulière d'articles de recherche qui fournissent des versions constructives de nombreux théorèmes importants de l'algèbre contemporaine.

De manière à priori surprenante, l'algèbre moderne abstraite se prête à des méthodes générales de transformation des concepts abstraits qui en définitive **décryptent** les démonstrations qui utilisent ces concepts et révèlent des **calculs cachés** qui aboutissent à des versions constructives.

Plaidoyer pour l'algèbre constructive : texte écrit avec Thierry Coquand en 2012, sur ma page web, pas mal d'exemples.
http://hlombardi.free.fr/publis/Plaidoyer.pdf

une étude plus théorique
A logical approach to abstract algebra. Coquand T., Lombardi H.
A survey. Math. Struct. in Comput. Science **16**, (2006), 885-900.
http://hlombardi.free.fr/publis/AlgebraLogicCoqLom.pdf

les mathématiciens classiques pensent souvent que les mathématiques constructives étudient uniquement « les objets mathématiques constructifs » alors que les mathématiciens constructifs pensent que les mathématiques constructives et classiques étudient exactement les mêmes objets, mais que les mathématiques classiques ajoutent des axiomes non constructifs sujets à controverses
un exemple paradigmatique est celui des suites d'entiers constructives versus les suites d'entiers « calculables sur ordinateur », voir à ce sujet l'article
Recursive functions and constructive mathematics. Coquand T.
p. 159--167 dans: Bourdeau M., Dubucs J. (Eds.),
Calculability and Constructivity. Historical and Philosophical Aspects.
Logic, Epistemology and the Unity of Science, Vol. 34. Springer (2014)
http://hlombardi.free.fr/coq-rec-2014.pdf

Le Paradis que Cantor a créé pour nous

Personne ne nous chassera du Paradis que Cantor a créé pour nous.
David Hilbert

C'est quoi ce Paradis ?

C'est le Paradis dans lequel on utilise des infinis potentiels comme s'ils étaient des infinis actuels.

Par exemple on a la « construction » $\mathbf{N} \to \mathcal{P}(\mathbf{N})$ déclarée légitime.

Avec Cantor il y a Dedekind, tout aussi important.

Pour Dedekind, le continu, la « droite réelle » est désormais un simple « ensemble de points », chaque point étant une double infinité de points dans **Q.** Ainsi on « construit » **R** en tant qu'un infini actuel du même genre que $\mathcal{P}(\mathbf{N})$.

En théorie des nombres, un « pgcd idéal » de Kummer de deux éléments a et b d'un corps de nombres **K**, devient pour Dedekind un ensemble infini formé par toutes les combinaisons $u\,a + v\,b$ où u et v sont n'importe quels éléments de **K** entiers sur **Z.**

Ces inventions de Dedekind peuvent être contournées de manière constructive. Par exemple la théorie de Kronecker des « pgcds idéaux » est plus générale que celle de Dedekind et donne une version constructive, sans condition noethérienne, de la théorie des diviseurs d'André Weil.

Par contre d'autres résultats importants de la fin du XIX° siècle nécessitent une réécriture constructive importante. Par exemple le fameux théorème de Wedderburn sur la structure des algèbres centrales simples, ou tout ce qui concerne la noethérianité.