Comment les notions premières sont-elles définies dans les mathématiques anciennes ?

Gilles Dowek

Comment les notions premières sont-elles définies dans les mathématiques anciennes ? *

Gilles Dowek

En progressant dans notre compréhension des mathématiques, nous progressions parfois également dans notre compréhension de leur histoire. Bien entendu, pas en projetant nos préoccupations contemporaines sur le passé, mais en découvrant des vérités nécessaires, qui s'appliquent donc aux mathématiques du passé tout autant qu'aux mathématiques contemporaines.

1 Des démonstrations avant le miracle grec ?

Notre besoin de décrire des algorithmes dans des langages formels pour programmer les ordinateurs et la constatation empirique de notre propension à faire de nombreuses erreurs dans ces descriptions nous ont mené à tenter de démontrer que certains de ces algorithmes sont corrects. Par exemple, démontrer qu'un algorithme qui prend en argument deux nombres entiers et retourne le quotient et le reste de leur division euclidienne est correct consiste à démontrer que le reste calculé par l'algorithme est inférieur au diviseur donné en argument et que la somme de ce reste et du produit du quotient calculé par l'algorithme et du diviseur est égal au dividende donné en argument.

L'apparition de cette notion de démonstration de correction d'algorithmes permet de prendre conscience que nous construisons toujours plus ou moins explicitement de telles démonstrations quand nous construisons un algorithme. Quand nous construisons l'algorithme de tri par sélection, par exemple, nous savons justifier chaque étape. Nous commençons, par exemple, par chercher le plus petit élément du tableau à trier, *parce que c'est le premier élément du tableau trié.*

*Séminaire commun CHSPAM - REHSEIS de SPHERE, Histoire et Philosophie des mathématiques, le 2 février 2010.

Cette prise de conscience nous amène à nous demander comment les Mésopotamiens et les Égyptiens ont pu concevoir des algorithmes avant le miracle grec, avant l'invention de la notion de démonstration. Les *Éléments d'histoire des mathématiques* de Bourbaki notaient déjà le problème : « si on ne rencontre dans les textes [de l'algèbre babylonienne] rien qui ressemble à une "démonstration" au sens formel du mot, on est en droit de penser que 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. » [1]

Si ce texte met en évidence un problème dans l'existence de cette « mathématique préhellénique fort développée » [2] et une possible solution dans l'existence de démonstrations non encore formalisées, avant le miracle grec, il n'insiste pas, en revanche, sur la possibilité de distinguer, au sein des démonstrations mathématiques, une classe particulière : les démonstrations de correction d'algorithmes, et sur la possibilité se poser la question de la place de ces démonstrations dans n'importe quel corpus mathématique, en particulier dans celui des mathématiques grecques.

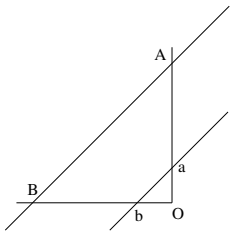
Il n'insiste pas non plus sur le fait que cette hypothèse de l'existence de démonstrations avant le miracle grec résout simultanément un autre problème : celui de la raison pour laquelle les Grecs se sont soudainement mis à faire des démonstrations. Il devient en effet possible d'imaginer une articulation entre les mathématiques mésopotamiennes et égyptiennes et les mathématiques grecques, dans laquelle les démonstrations sont apparues d'abord pour démontrer la correction d'algorithmes, avant de prendre petit à petit une place plus importante dans l'édifice mathématique. Le miracle ne serait donc pas que les Grecs aient inventé la notion de démonstration, mais, d'une part, qu'ils aient consigné leurs démonstrations par écrit et, d'autre part, qu'ils aient étendu leur champ d'application à des propositions qui n'expriment pas toujours la correction d'un algorithme.

Il est bien entendu assez difficile de confronter cette hypothèse à des faits empiriques. Néanmoins, on peut penser que si cette hypothèse est vraie, on devrait trouver parmi les premières démonstrations des mathématiques grecques, quelques démonstrations de correction d'algorithmes.

L'anecdote qui accompagne le théorème de Thalès, selon laquelle la démonstration de ce théorème aurait permis de déterminer la hauteur d'une

1. N. Bourbaki. *Éléments d'histoire des mathématiques*. Hermann, 1969, p. 9.
2. *Ibid.*

pyramide de Gizeh en mesurant l'ombre de la pyramide sur le sol, l'ombre d'un bâton — ou d'une personne — et la taille de ce bâton — dans sa version dans laquelle le rapport des ombres aux hauteurs est 1, telle que la rapportent Diogène Laërce et Pline, ou dans laquelle ce rapport est quelconque, telle que la rapporte Plutarque [3] — semble montrer que ce théorème exprime la correction d'un algorithme de mesure d'un segment.



Le théorème de Thalès nous dit simplement que si les distances Oa et Ob sont égales et les droites ab et AB sont parallèles, alors les distances OA et OB sont égales. Mais l'anecdote nous dit davantage. Elle nous dit que pour déterminer la longueur d'un segment OA, une méthode consiste à prendre un point quelconque a sur le segment OA, puis un point b n'appartenant pas à la droite Oa tel que les distances Oa et Ob soient identiques, à tracer la parallèle à la droite ab qui passe par le point A et à mesurer la distance entre le point O et l'intersection B de cette droite avec la droite Ob. La démonstration que cette distance OB est égale à la distance OA est la démonstration que cet algorithme calcule bien la distance OA.

Le théorème de Pythagore est également le théorème de correction d'un algorithmes ancien [4] qui, pour déterminer la longueur de l'hypoténuse d'un triangle rectangle, consiste à mesurer les deux petits cotés, à élever les nombres obtenus au carré, à ajouter ces deux carrés, à extraire la racine carrée de leur somme.

Cependant, au delà de l'interprétation de ces deux théorèmes, l'argument qui soutient le plus solidement cette thèse est que certains textes mathématiques de la Chine ancienne sont précisément structurés sous la forme d'une suite de descriptions d'algorithmes, chacun accompagné de sa démonstration

3. M. Caveing. *La figure et le nombre. Recherches sur les premières mathématiques des Grecs*. Presses Universitaires du Septentrion, 1997, p. 61.

4. M. Caveing. *Essai sur le savoir mathématique dans la Mésopotamie et l'Égypte anciennes*. Presses Universitaires de Lille, 1994, p. 187, 209-210, 389.

de correction [5]. Les démonstrations dans ces textes semblent avoir comme unique fonction de démontrer la correction de ces algorithmes, ce qui permet de supposer que, en Mésopotamie et en Égypte, comme en Chine, les premières démonstrations ont été des démonstrations de correction d'algorithmes.

Le mystère des mathématiques mésopotamiennes et égyptiennes ne semble donc pas tant être dans le fait que leurs auteurs aient pu concevoir des algorithmes sophistiqués sans disposer de la notion de démonstration, mais dans le fait qu'ils n'aient pas consigné ces démonstrations par écrit, comme l'ont fait, par exemple, leurs homologues chinois.

L'image que cette hypothèse nous donne de la structure des mathématiques anciennes, dans laquelle un problème mathématique « ordinaire » est résolu par l'application d'un algorithme, la recherche d'une démonstration n'étant utilisée que pour la résolution des « problèmes de second niveau », que constituent la correction de ces algorithmes, nous amène à nous demander si nos mathématiques contemporaines ne sont pas, elles aussi, partiellement structurées ainsi. Et, de fait, quand nous devons trouver une solution approchée d'une équation différentielle pour calculer un pont, nous ne cherchons pas de démonstration, nous appliquons un algorithme, par exemple la méthode des éléments finis, et c'est seulement quand cet algorithme est remplacé par un autre — ce qui se produit sur une toute autre échelle de temps que la résolution des équations elle-même — que nous devons trouver une démonstration pour établir la correction du nouvel algorithme. Si cet exemple est délibérément un problème mathématique motivé par un problème concret — construire un pont —, des exemples similaires peuvent être trouvés en mathématiques pures : pour résoudre un système linéaire, dériver une fonction élémentaire, déterminer la primalité d'un nombre entier, nous ne cherchons pas de démonstration, nous appliquons un algorithme et c'est seulement quand ces algorithmes évoluent que nous devons chercher de nouvelles démonstrations.

Nous ne pouvons d'ailleurs expliquer que nous progressions quand nous faisons des mathématiques que parce que l'apprentissage des mathématiques consiste non seulement en l'apprentissage d'axiomes et de théorèmes, mais aussi en l'acquisition d'automatismes, qui sont constamment activés quand nous cherchons à résoudre un problème. Ces automatismes sont des algo-

5. K. Chemla et G. Shuchun. *Les neufs chapitres. Le classique de la Chine ancienne et ses commentaires.* Dunod, 2004.

rithmes, mais bien souvent pas des algorithmes de décision. Par exemple, faire un changement de variable dans une équation différentielle, ne donne pas, en général, une solution de cette équation, mais une autre équation qu'il reste à résoudre.

2 Des axiomes aux règles de calcul

Cette notion de démonstration de correction d'algorithmes n'est cependant pas la seule occurrence de la notion d'algorithme dans la logique contemporaine, où cette notion est également un substitut de celle d'axiome. Et cette autre fonction des algorithmes peut également contribuer à éclairer les mathématiques du passé, en particulier nous aider à relativiser l'idée que les démonstrations anciennes soient des démonstrations axiomatiques.

2.1 Les règles de déduction et les axiomes

La logique des prédicats est formée de règles de déduction qui définissent la signification des connecteurs et des quantificateurs logiques. En revanche, et c'est tout l'intérêt de la logique des prédicats, ces règles ne définissent pas la signification des symboles de fonction et de prédicat qui apparaissent dans les propositions. Ainsi, la proposition $x \leq y \Rightarrow x \leq y + 1$ n'est-elle pas démontrable en utilisant exclusivement les règles de déduction de la logique des prédicats, car, contrairement à celle de la proposition $x \leq y \Rightarrow x \leq y$, sa vérité ne tient pas uniquement à la signification du connecteur logique $\Rightarrow$, mais aussi à celle des symboles $\leq$, $+$ et 1. La signification de ces symboles est donc définie ailleurs : par les axiomes de l'arithmétique.

Les démonstrations de la logique des prédicats sont donc construites en utilisant deux ingrédients : des règles de déduction et des axiomes. Si les règles de déduction sont des objets d'une nature différente des théorèmes, les axiomes, en revanche, comme les théorèmes, sont des propositions. Cette homogénéité entre les axiomes et les théorèmes mène naturellement à la tentation de poser en axiome n'importe quelle proposition que l'on ne parvient pas à démontrer, ou, à l'inverse, à suspecter les autres de l'avoir fait. Par exemple, les tentatives de démontrer l'axiome des parallèles à partir des autres axiomes de la géométrie, repose sur cette suspicion à l'égard de cette proposition, qui semble n'être un axiome qu'en vertu de sa résistance aux tentatives de démonstration.

2.2 Les règles de calcul

Les axiomes de l'arithmétique, en particulier ceux l'addition

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

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

permettent de démontrer la proposition $2 + 2 = 4$. Cependant, comme le remarque Henri Poincaré [6], cette proposition ne semble pas réellement demander de démonstration, car chacun peut la vérifier en effectuant un simple calcul. Cela mène à s'étonner du fait que, en logique des prédicats, les démonstrations soient construites avec des règles de déduction et des axiomes uniquement, et à chercher à construire les démonstrations avec trois ingrédients : des règles de déduction, des axiomes et aussi des règles de calcul. Par exemple, la signification de l'addition semble mieux exprimée par les règles de calcul

$$x + 0 \longrightarrow x$$

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

qui définissent un algorithme pour l'addition, que par les axiomes ci-dessus.

En utilisant ces deux règles la proposition $2 + 2 = 4$ se réduit en $4 = 4$ qui peut simplement être démontrée avec l'axiome de réflexivité de l'égalité, à moins que davantage de règles de calcul, par exemple les règles [7]

$$0 = 0 \longrightarrow \top$$

$$0 = S(y) \longrightarrow \bot$$

$$S(x) = 0 \longrightarrow \bot$$

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

ne la réduisent finalement en $\top$, qui peut être démontrée avec la règle d'introduction du connecteur logique $\top$.

Ces règles de calcul permettent de se passer des axiomes de l'addition, car ceux-ci sont équivalents, modulo les règles de calcul, à des propositions démontrables

$$\forall x\ (x = x)$$

6. H. Poincaré. *La science et l'hypothèse.* Flammarion, 1902.

7. L. Allali. Algorithmic equality in Heyting Arithmetic modulo. *Types for Proofs and Programs.* Lecture Notes in Computer Science 4941, Springer, 2008, p. 1-17.

et

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

Elles permettent également de se passer du troisième et du quatrième axiomes de Peano

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

et

$$\forall x \ (0 = S(x) \Rightarrow \bot)$$

qui sont équivalents, modulo les règles de calcul, aux propositions démontrables

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

et

$$\forall x \ (\bot \Rightarrow \bot)$$

Cette variante de la logique des prédicats dans laquelle les axiomes sont remplacés par des règles de calcul qui peuvent être appliquées à n'importe quel moment dans une démonstration s'appelle la *Déduction modulo* [8], mais cette idée a des origines plus anciennes, en particulier en démonstration automatique et en théorie des types [9]. Remplacer les axiomes par des règles de calcul permet de rendre les démonstrations plus courtes et plus intelligibles. Mais la motivation principale est, en fait, de répondre à des problèmes internes à la théorie de la démonstration, où les axiomes sont à l'origine de nombreuses difficultés [10]. Au delà des axiomes de l'addition et des troisième et quatrième axiomes de Peano, de nombreux axiomes peuvent ainsi être remplacés par des règles de calcul : tous les axiomes de l'arithmétique, ceux de la théorie des types simples, ceux de certaines variantes de la théorie des ensembles, ...

Contrairement aux axiomes, il n'est pas possible de poser n'importe quelle règle de calcul. Par exemple, on ne peut pas poser à la fois la règle

$$x = y \longrightarrow \forall A \ (x \in A \Rightarrow y \in A)$$

et la règle

$$0 = 0 \longrightarrow \top$$

8. G. Dowek, Th. Hardin et C. Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31, 2003, p. 33-72. G. Dowek et B. Werner. Proof normalization modulo. *The Journal of Symbolic Logic*, 68(4), 2003, p. 1289-1316.

9. G. Dowek. *Les métamorphoses du calcul*. Le Pommier, 2007.

10. G. Dowek. From proof theory to theories theory. 2009.

car la proposition $0 = 0$ se réduirait alors à la fois sur la proposition $\forall A\ (0 \in A \Rightarrow 0 \in A)$ et sur la proposition $\top$.

De plus, les règles de calcul, à la différence des axiomes ne sont pas de la même nature que les théorèmes et les conjectures : ce ne sont pas des propositions. Il n'est donc pas possible de se débarrasser de n'importe quelle conjecture en la « posant en règle de calcul », comme c'était le cas avec les axiomes.

2.3 Les définitions explicites

Les *définitions explicites* forment un cas particulier des règles de calcul. Une définition explicite consiste à introduire un symbole pour désigner un objet, autrement désigné par un terme complexe, par exemple le symbole d pour le nombre $1/2$. Traditionnellement, une telle définition peut être comprise de deux manières.

Selon la première, poser la définition « soit d le nombre $1/2$ » consiste à ajouter le symbole d au langage et à poser l'axiome $d = 1/2$. Dans ce cas, les propositions $(1/2) \times 4 = 2$ et $d \times 4 = 2$ sont distinctes, et elles ont des démonstrations distinctes, même si l'axiome $d = 1/2$ permet de transformer toute démonstration de l'une en une démonstration de l'autre.

Selon la seconde, le symbole d n'appartient pas au langage, mais, en lisant la proposition $d \times 4 = 2$, par exemple nous devons mentalement le remplacer par le terme $1/2$. Dans ce cas, les propositions $(1/2) \times 4 = 2$ et $d \times 4 = 2$ sont identiques, et donc toute démonstration de l'une est une démonstration de l'autre.

Une telle définition explicite peut s'exprimer en Déduction modulo par la règle de calcul

$$d \longrightarrow (1/2)$$

qui permet de réduire la proposition $d \times 4 = 2$ en $(1/2) \times 4 = 2$. Ainsi, ces deux propositions sont distinctes mais, étant équivalentes modulo les règles de calcul, elles ont les mêmes démonstrations.

On peut étendre cette notion de définition explicite de manière à inclure les définitions de symboles de fonction, par exemple, la règle

$$f(x) \longrightarrow (2 \times x + 1)$$

qui permet, par exemple, de réduire le terme $f(3)$ sur le terme $2 \times 3 + 1$, et

qui est un peu différente de la définition au sens strict

$$f \longrightarrow (x \mapsto 2 \times x + 1)$$

qui réduirait le terme $f(3)$ sur $(x \mapsto 2 \times x + 1)(3)$, qu'il faudrait encore réduire avec une autre règle, dite de *β-réduction*, pour obtenir le terme $2 \times 3 + 1$.

De même, on peut étendre cette notion de manière à inclure les définitions de symboles de prédicat. La définition de Leibniz de l'égalité, selon laquelle deux objets x et y sont égaux si y appartient à tous les ensembles auxquels x appartient, est un exemple d'une telle définition

$$x = y \longrightarrow \forall A \ (x \in A \Rightarrow y \in A)$$

à partir de cette définition, on peut démontrer la réflexivité de l'égalité puisque la proposition $\forall x \ (x = x)$ se réduit sur la proposition démontrable $\forall x \forall A \ (x \in A \Rightarrow x \in A)$. Et on peut, de même, démontrer ainsi la substitutivité de l'égalité.

De même, on peut définir le prédicat de Peano « être un nombre entier » par le fait que x est un nombre entier s'il appartient à tous les ensembles contenant 0 et clos par successeur

$$N(x) \longrightarrow \forall A \ ((0 \in A \wedge \forall x \ (x \in A \Rightarrow S(x) \in A)) \Rightarrow x \in A)$$

et démontrer le cinquième axiome de Peano — l'axiome de récurrence —, ainsi que les deux premiers axiomes de Peano, selon lesquels 0 est un nombre entier, et le successeur d'un nombre entier est un nombre entier.

2.4 La signification du symbole d'égalité en arithmétique

Nous avons vu deux manières assez différentes d'exprimer la signification du symbole d'égalité en arithmétique. La première est un algorithme qui réduit une proposition de la forme $n = p$ ou bien en $\top$ ou bien en $\bot$ selon que n et p sont égaux ou différents. Cet algorithme est un algorithme de décision car la forme réduite d'une proposition de la forme $n = p$ est ou bien « oui » ($\top$) ou bien « non » ($\bot$). À l'inverse, la définition de Leibniz est un algorithme, mais pas un algorithme de décision, puisqu'il réduit la proposition $n = p$ en $\forall A \ (n \in A \Rightarrow p \in A)$ qu'il faut ensuite démontrer ou réfuter.

Chaque algorithme a ses avantages et ses inconvénients. Le premier permet des démonstrations simples des troisième et quatrième axiomes de Peano, mais la réflexivité et de la substitutivité de l'égalité sont plus difficiles à démontrer. Le second permet des démonstrations simples de la réflexivité et de la substitutivité de l'égalité, mais les troisième et quatrième axiomes de Peano sont plus difficiles à démontrer. Le choix entre l'un et l'autre est une question d'importance relative des propriétés de l'égalité.

Le même problème se pose, mais sous une forme plus aiguë, en théorie des ensembles. Si l'on exprime la signification du symbole d'égalité par sa propriété d'extensionalité, on peut ensuite montrer ses propriétés de réflexivité et de substitutivité. Si l'on exprime la signification de ce symbole par ses propriétés de réflexivité et de substitutivité, il semble que l'on ne puisse pas démontrer sa propriété d'extensionalité [11].

3 Les notions premières dans les mathématiques anciennes

3.1 Les différents types de définitions

En quoi cette possibilité de substituer des règles de calcul aux axiomes peut-elle contribuer à éclairer les mathématiques du passé ?

Nous avons vu que, de manière générale, il y a plusieurs manières d'exprimer la signification des symboles d'une théorie mathématique. La manière la plus simple est d'utiliser une définition explicite : « soit d le nombre $1/2$ », « soit f la fonction $x \mapsto 2 \times x + 1$ », « soit $=$ la relation $\{(x, y) \mid \forall A\ (x \in A \Rightarrow y \in A)\}$ », voire « soit $f(x)$ le nombre $2 \times x + 1$ » et « soit $x = y$ la proposition $\forall A\ (x \in A \Rightarrow y \in A)$ ».

Mais bien des notions, en particulier les notions premières d'une théorie, ne peuvent pas être définies de manière explicite et elles doivent être définies de manière implicite. Une manière de le faire est de poser des axiomes, comme les axiomes de la géométrie, qui définissent implicitement les notions de point, de droite, ... Mais, comme nous l'avons vu, il est aussi possible de d éfinir les notions premières d'une théorie par un algorithme.

Par exemple, l'égalité sur les nombres entiers peut ainsi être définie par un ensemble d'axiomes, qui expriment que l'égalité est réflexive et substitutive,

11. G. Dowek et A. Miquel. Cut elimination for Zermelo set theory. 2007.

par l'algorithme

$$x = y \longrightarrow \forall A\ (x \in A \Rightarrow y \in A)$$

ou encore par l'algorithme de décision

$$0 = 0 \longrightarrow \top$$

$$0 = S(y) \longrightarrow \bot$$

$$S(x) = 0 \longrightarrow \bot$$

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

Cette remarque nous amène à nous interroger sur la manière dont les Anciens définissaient les notions premières qu'ils utilisaient dans leurs démonstrations de correction d'algorithmes. Il ne suffit, en effet, pas qu'ils aient été capables d'« un minimum d'enchaînements logiques » pour construire des démonstrations de correction d'algorithmes, car les règles de déduction expriment la signification des connecteurs et des quantificateurs logiques, mais pas celle des symboles qui expriment les notions premières de la théorie, il faut donc qu'ils aient aussi été capables de définir un minimum les notions premières dont ils avaient besoin dans ces démonstrations.

À coté de la question : quels algorithmes les mathématiciens du passé ont-ils construit ? se pose donc une autre question : comment ces mathématiciens ont-ils défini leurs notions premières ? Avec des axiomes ou des algorithmes ?

Encore une fois, il est difficile de confronter directement cette question à des faits empiriques. Mais deux éléments semblent soutenir l'hypothèse d'une définition algorithmiques de ces notions premières.

Le premier est que, contrairement à leur formulation moderne, la formulation originale des trois premiers axiomes d'Euclide, qui définissent les notion premières de la géométrie grecque : « Conduire une droite d'un point quelconque à un point quelconque. Prolonger indéfiniment, selon sa direction, une droite finie. D'un point quelconque, et avec un intervalle quelconque, décrire une circonférence de cercle. » [12] signale une origine algorithmique de ces axiomes [13].

12. Euclide. *Les éléments.* Traduction F. Peyrard, 1819.
13. M. Serres. *Les origines de la géométrie.* Flammarion, 1993.

3.2 La comparaison

Le second élément est que les définitions algorithmiques sont plus simples que les définitions axiomatiques, car, à la différence d'un algorithme, un axiome ne sert à rien tant qu'il n'est pas inséré dans un système plus vaste de construction de démonstrations, qui comprend, en particulier, des règles de déduction. Ainsi, au lieu de devoir postuler une invention simultanée d'axiomes et de règles de déduction, puisque les uns ne servent à rien sans les autres, nous pouvons postuler une invention séquentielle, d'abord d'algorithmes, puis de règles de déduction.

Nous pouvons illustrer ce point par ce qui semble être un des premiers algorithmes de l'histoire : la comparaison du cardinal de deux ensembles finis. Lorsqu'un troupeau était vendu, il semble que les bergers sortant le troupeau, ajoutaient une unité à un tas de cailloux à chaque fois qu'un animal sortait de la bergerie. À l'arrivée, ils enlevaient un caillou du tas chaque fois qu'un animal entrait dans la bergerie. S'il restait des cailloux à la fin de cette opération, cela signifiait que des animaux manquaient — ces tas de cailloux, enfermés dans des bulles d'argile scellées semblent être les derniers ancêtres non écrits des chiffres.

Pour démontrer la correction de cet algorithme, il faut d'abord définir une notion d'équipotence de deux ensembles. Mais y a-t-il une définition plus simple de l'équipotence de deux ensembles que cet algorithme qui consiste à retirer de manière parallèle les éléments des deux ensembles, jusqu'à épuiser l'un d'eux ?

Ainsi, il est vraisemblable que la première définition de cette notion d'équipotence ait été algorithmique, et non axiomatique.

Si cette hypothèse est exacte, alors cet algorithme de comparaison est correct par définition, et sa correction n'a donc pas besoin d'être démontrée.

3.3 L'addition

On peut, de même, s'interroger sur la manière dont les Anciens définissait l'addition, ce qui demande de définir d'abord les nombres entiers.

La logique contemporaine a donné de nombreuses définitions de cette notion, qui peuvent grossièrement se classer en quatre catégories.

Selon la définition de Peano, les nombres entiers sont définis axiomatiquement, on ne sait pas ce qu'est le nombre n, mais on a un moyen de l'écrire : $S(...S(0)...)$ et on pose des axiomes qui expriment ses propriétés.

Selon une définition de Church, les nombres entiers sont des algorithmes : le nombre n est l'algorithme qui prend en argument un autre algorithme et l'itère n fois.

Selon la définition de Cantor — ou de Frege, ou de Hume, ... —, les nombres entiers sont des ensembles d'ensembles : le nombre n est un ensemble d'ensembles de n éléments — l'ensemble de tous les ensembles de n éléments dans la définition originale, l'ensemble de tous les ensembles de n éléments d'un ensemble infini fixé, selon la définition amendée par Russell et Whitehead, après que l'on a pris conscience de la contradiction des axiomes qui permettaient de montrer l'existence d'un ensemble de tous les ensembles de n éléments.

Selon la définition de Von Neumann, les nombres entiers sont des ensembles héréditairement finis : le nombre n est un ensemble de n éléments particulier, l'ensemble $\{0, ..., n-1\}$.

Dans trois de ces quatre cas, l'addition, peut être définie par un algorithme. Seule la définition de Cantor, faisant des nombres entiers des ensembles infinis, pose un problème. Cela amène à s'interroger sur la conception que les Anciens pouvaient avoir des nombres entiers : il est conceptuellement beaucoup plus simple de définir le nombre 3 comme un ensemble particulier de trois éléments, puis de définir le cardinal d'un ensemble comme l'unique nombre entier auquel il est équipotent que de définir le nombre entier 3 comme l'ensemble de tous les ensembles de trois éléments.

3.4 Des algorithmes aux algorithmes

Si les notions de comparaison, d'addition, ... sont définies de manière algorithmique, il ne semble plus nécessaire démontrer la correction de ces algorithmes, qui sont corrects par définition. De manière plus générale, si les points de départ et l'objectif des mathématiques anciennes sont des algorithmes, quel est leur apport ?

Pour que ces mathématiques apportent quelque chose, il faut que les algorithmes dont elles partent et ceux qu'elles construisent soient différents. Et ils peuvent être différents de plusieurs manières.

Tout d'abord, les algorithmes que ces mathématiques construisent peuvent calculer la même chose que les algorithmes dont elles partent, mais de manière plus efficace. Un exemple typique est l'algorithme de l'addition. La définition algorithmique selon laquelle $n + p$ est le cardinal de l'union disjointe de deux ensembles particuliers de n éléments et de p éléments, par

exemple des ensembles $\{0, ..., n-1\}$ et $\{0, ..., p-1\}$, mène à un algorithme qui comme l'algorithme

$$x + 0 \longrightarrow x$$

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

est linéaire en les nombres ajoutés, donc impraticable. En revanche, n'importe quel algorithme qui utilise la représentation dans un système à base — que cette base soit fixe ou variable, que la signification des chiffres soit indiquée par le chiffre lui-même, par un symbole complémentaire ou par sa position —, est logarithmique donc praticable, mais il demande une démonstration de correction par rapport à la définition algorithmique qui lui sert de spécification.

De même, même si la notion de mesure d'un segment est définie de manière algorithmique : reporter un segment unité dans le segment à mesurer autant de fois de possible, l'algorithme de Thalès permet de mesurer un segment vertical, en se ramenant à la mesure d'un segment horizontal, ce qui est praticable, contrairement à la mesure directe du segment vertical.

Ensuite, même si les notions premières, par exemple l'addition ou la multiplication sont définies de manière algorithmique, les algorithmes construits peuvent calculer d'autres opérations, spécifiées en utilisant ces notions premières.

Les exemples les plus simples sont la soustraction et la division qui peuvent être spécifiées avec l'addition et la multiplication, et plus généralement, tous les algorithmes spécifiés comme l'inverse d'un autre algorithme.

La complexité des algorithmes développés par les Anciens mène à supposer que ceux-ci ont construit des démonstrations avant le miracle grec. Cependant, en faisant cette supposition, nous risquons de projeter la notion de démonstration axiomatique sur la passé et de supposer que les Anciens ont défini leur notions premières par des axiomes. Il semble plus vraisemblable cependant — même s'il ne s'agit que d'une hypothèse — que ces notions premières ait été d'abord définies elles-mêmes de manière algorithmique. Cette hypothèse nous donne à une image différente des mathématiques anciennes, dans laquelle les démonstrations ne relient pas des axiomes à des algorithmes, mais des algorithmes à d'autres algorithmes.