# Nombres: Éléments de mathématiques pour philosophes

Marco Panza

# Nombres : Éléments de mathématiques pour philosophes

Marco Panza

# Table des matières

# Préface

Au cours de l'été 1998 j'avais achevé un livre portant le même titre que celui-ci et je l'avais envoyé à l'éditeur Diderot Multimédia de Paris. J'avais ensuite corrigé plusieurs jeux d'épreuves, donné le bon à imprimer, et attendu que mon livre paraisse. L'imprimeur avait apparemment préparé les clichés, mais il ne les imprimait pas, en attendant que l'éditeur réglât des comptes en suspens. Passèrent ainsi plusieurs mois au cours desquels l'éditeur modifia, je crois, sa raison sociale. Finalement, au cours de l'automne 1999, l'impression fut achevée et le livre apparut affichant le copyright « © 1999 Diderot Multimédia-EDL ». J'en eus quelques copies, d'autres furent envoyées à des collègues, quelques unes parvinrent à quelques libraires parisiens et d'autres encore furent remises à un libraire vendant par *internet*. La grande majorité des copies étaient pourtant encore stockées chez le distributeur, lorsque ce dernier décida d'ouvrir une procédure judiciaire vis-à-vis de l'éditeur et bloqua la distribution. L'éditeur fut mis en administration contrôlée et cessa *de facto* son activité, pendant que ces copies restaient enfermées au fond d'un magasin. Je demandai à plusieurs reprises la résiliation du contrat qui me liait à un éditeur qui n'exerçait plus ses fonctions, et je demandai de même à reprendre les copies restantes de mon livre. Le contrat fut résilié en 2002, mais ces copies sont encore, à ce que je sache, enfermées au fond du même magasin, en attente, sans doute, d'être pilonnées (c'est du moins ce que j'espère et désormais demande au distributeur).

Celle que je présente ici est donc la deuxième édition d'un livre dont la première édition n'est *de facto* jamais parue. C'est un livre écrit il y a six ou sept ans, et que je n'ai pour l'occasion repris que localement, en corrigeant quelques erreurs que j'ai entre temps repérées ou que des amis m'ont signalées, et en ajoutant quelques références bibliographiques à des œuvres récentes.

La partie de la présente préface qui suit ces quelques remarques est tirée de la préface à l'édition de 1998. Je me suis contenté à supprimer certains passages et à en mettre à jour d'autres.

* * *

Lorsque j'ai été nommé à l'université de Nantes, en 1993, en qualité de maître de conférences, au programme de la première année de philosophie, figurait déjà un cours de mathématiques. Pendant des années, Jean-Louis Gardies avait été chargé de ce cours. Il venait alors de prendre sa retraite. On me demandait alors de prendre le relais, et d'enseigner ce cours. Quand, quelques années plus tard, j'eus la chance de connaître personnellement Jean-Louis Gardies, je compris quelle énorme responsabilité on m'avait confiée. Sur le coup, je ne pensai qu'au défit didactique d'une telle entreprise et, il faut l'avouer, au divertissement intellectuel que me procurerait un tel défi. J'acceptai ainsi la proposition et commençai à réfléchir au contenu que j'aurais pu donner à mon cours et à la manière dont il pouvait être enseigné.

## I

Immédiatement, une chose m'apparut claire : ce n'était pas question de tromper mes étudiants. Bien que nombre d'entre eux auraient sans doute préféré se débarrasser de cette corvée — à laquelle ils ne s'attendaient certes pas quand ils avaient décidé de s'inscrire en philosophie —, en se contentat d'écouter quelques-unes de nombreuses anecdotes qu'on raconte au sujet des mathématiques et de leur histoire, ou, tout au plus, en abordant un cours d'introduction à la philosophie des mathématiques, il n'était pas question de leur faire croire qu'on peut faire des mathématiques, même au niveau le plus élémentaire, sans avoir affaire à des contenus techniques. Il s'agissait donc de présenter quelques uns de ces contenu, mais de le faire d'une manière adaptée aux exigences propres à des étudiants de philosophie.

Aucun cours de mathématiques traditionnel, fût-ce d'algèbre, d'analyse ou de géométrie, ne pouvait ainsi faire l'affaire. À l'instar de nombreux textes de vulgarisation, j'aurais pu sélectionner un ensemble significatif de résultats fondamentaux et essayer de les exposer sans entrer nécessairement dans les détails de leurs démonstrations. De cette manière, il m'aurait été possible de donner une image informelle de quelque secteur des mathématiques modernes, en espérant susciter une curiosité qui aurait pu amener quelques-uns de mes étudiants à des études supplémentaires. Deux raisons me convainquirent de l'inopportunité de cette solution. Elle aurait aussi pu générer une idée fausse des mathématiques, en suscitant la croyance qu'on peut extraire de ces dernières des grandes idées directrices, dont la puissance et le charme seraient finalement indépendants de toute possibilité de réduction technique, celle-ci étant, au fond, une tâche secondaire et inessentielle. Cette première raison était, si possible, renforcée par la seconde : en m'interrogeant sur l'utilité, ou plus généralement sur le rôle d'un enseignement des mathématiques dans la formation d'un philosophe, je ne savais assigner aucun rôle essentiel à une information sommaire comme celle que mes étudiants auraient pu tirer d'un cours conçu de cette manière.

Il s'agissait alors, avant de commencer à préparer mon cours, de répondre à la question suivante : quel rôle peut jouer, dans la formation d'un philosophe, un enseignement des mathématiques ? J'avais, et j'ai encore, deux réponses à cette question.

La première tient à ce simple constat : depuis l'antiquité, une grande partie de la réflexion philosophique porte sur la nature de la connaissance. Or, comprendre la nature des mathématiques est une partie essentielle de cet effort, et cela n'est possible qu'à condition de se rapporter aux théories mathématiques et d'en chercher les raisons d'être. Comment comprendre, pour ne donner qu'un exemple parmi les plus faciles, la nature logique d'une construction hypothético-déductive, sans explorer de l'intérieur quelques systèmes axiomatiques, parmi ceux que les mathématiciens ont, en des époques fort différentes, su construire ? Cette recherche à propos de la nature de la connaissance n'est d'ailleurs, à mon sentiment, qu'un aspect d'un effort plus général, qui caractérise la tradition philosophique occidentale, et qui vise l'individuation des catégories à employer pour décrire et expliquer toute réalité à laquelle nous, les hommes, participons d'une manière ou d'une autre. Cette mission essentielle, qui intègre la réflexion philosophique à toute sorte d'entreprise scientifique, rend par ailleurs cette réflexion directement solidaire des buts de toute théorie mathématique. C'est la raison profonde de l'entrelacement, constant dans l'histoire, de problématiques issues respectivement de la tradition philosophique et de l'évolution des mathématiques. La nature de l'espace ou la caractérisation de la continuité ne sont que deux exemples de cet entrelacement que personne ne saurait nier. Il est donc naturel de penser qu'un enseignement de mathématiques doit en premier lieu donner à des philosophes des informations, mais surtout des outils techniques, indispensables aussi bien pour comprendre et évaluer des moments cruciaux de l'histoire de la philosophie, que pour continuer à poursuivre une des missions essentielles de la réflexion philosophique.

La deuxième réponse est plus générale. Aucune forme de raisonnement, quel que soit le contenu auquel ce raisonnement s'applique, ne peut éviter la contrainte de la rigueur dans l'argumentation. On ne peut pas raisonner par images, par métaphores, ou par émotions. Les images, les métaphores et les émotions sont certainement une partie importante de notre vie, mais elles ne sont pas les ingrédients de nos raisonnements. Raisonner signifie associer l'un à l'autre des contenus propositionnels, et le faire selon des contraintes qui ne peuvent pas être arbitraires. Or, la philosophie est essentiellement un exercice de raisonnement, et ne peut pas, comme telle, éviter de se plier à la discipline de la rigueur dans l'argumentation. Un cours de mathématiques peut et doit servir à habituer de jeunes étudiants à cette discipline, dans un contexte où elle manifeste de manière la plus explicite sa nécessité.

Ces deux réponses ont orienté mon choix : il s'agissait de construire un cours qui visait à dévoiler la raison d'être de quelques théories mathématiques élémentaires, à mettre à jour l'organisation interne de ces théories, et à montrer à l' œuvre les modalités argumentatives qui fonctionnent dans ces théories, sans aucun souci d'éviter une technicité nécessaire. Naturellement, pour réaliser ce programme, dans un cours de première année, il était nécessaire de limiter les sujets abordés, visant devantage à l'explication détaillée qu'à l'ampleur de l'information.

Mon livre est une version corrigée et augmentée des notes de cours qui ont guidé mon enseignement pendant toute ma période nantaise, c'est-à-dire de 1993 à 2002.

Le choix des sujets abordés correspond à un programme qui devrait apparaître clairement au vu du titre et de la table des matières : éclairer la manière dont les mathématiques modernes traitent, aux niveaux les plus élémentaires, des nombres. J'ai pourtant exclu de mon programme les nombres complexes, car il m'a semblé qu'un exposé satisfaisant de la théorie de ces nombres, même de ses contenus les plus élémentaires, ne pouvait pas faire l'économie d'un exposé préalable, où j'aurais dû faire entrer au moins des éléments de géométrie analytique et de théorie des équations algébriques, ce qui aurait trop élargi mon sujet. Naturellement, ce n'était pas le seul choix possible, ni le seul qui correspondit aux contraintes que je m'étais données. Il a sans doute été guidé par des goûts et des compétences personnelles, mais aussi par l'espoir de pouvoir aborder, un jour, avec le même esprit et selon la même approche, d'autres sujets dont le traitement pourrait être fondé sur ce premier exposé.

## II

Bien que le but de mon livre soit essentiellement didactique, que les résultats qui y sont exposés soient tous parfaitement connus de tout mathématicien — car ils font partie du contenu disciplinaire le plus fondamental et élémentaire des mathématiques modernes —, et que les arguments qui justifient ces résultats soient, eux aussi, tous assez standard, le choix et l'organisation de mon propos reflètent une conception des mathématiques, une manière de comprendre et de penser ces dernières, qui n'est sans doute pas partagée par la totalité des mathématiciens, des historiens et des philosophes des mathématiques. Il n'est certainement pas question ici de présenter et de justifier mes vues en la matière. Il suffira d'insister sur deux points, en rendant explicites deux convictions qui m'ont guidée tout au long de la rédaction de mon texte, dans le seul espoir que cette explicitation de mes présupposés puisse servir au lecteur pour mieux faire la part des choses entre ce qui, dans mon exposition, relève d'une connaissance acquise, partagée par l'ensemble de la communauté mathématique, et ce qui n'est par contre que l'expression de mes conceptions.

Mon premier point est le suivant : je considère les mathématiques comme une activité humaine qui se déroule au cours du temps. Avant d'avoir une histoire, les mathématiques sont donc, elles-mêmes, une histoire.

Si on peut parler, sans contresens, d'histoire des mathématiques, ce n'est qu'à condition d'utiliser le terme « mathématiques » aussi dans un autre sens : pour indiquer non pas l'activité humaine que je reconnais comme le référant du terme « mathématiques » employé dans le premier sens, mais les traces laissées par cette activité, les constructions auxquelles elle a conduit. Ces deux sens du terme « mathématiques » sont forcement confondus dans mon exposé et ils me semblent aussi qu'ils sont confondus dans la plupart des discours tenus autour de ce que l'on appelle justement « mathématiques ». Il ne s'agit pas ici de fournir un critère pour décider auquel de ces deux sens se réfère chaque occurrence de ce terme. Le lecteur n'aura aucune difficulté à comprendre par lui-même dans quel sens le terme « mathématiques » est, ici ou là, utilisé.

Personne, à ma connaissance, n'a jamais nié que les théories mathématiques dont nous disposons nous ont été léguées par des hommes, grâce à une activité qui s'est déroulée au cours du temps ; et je ne saurais imaginer que quiconque niât jamais cette évidence. Ce n'est donc pas parce que j'affirme ceci que mon approche diffère des autres. Le point sur lequel je veux insister est un autre : les hommes qui, à des époques diverses, nous ont légué les théories mathématiques dont nous disposons, les ont aussi édifiées, en poursuivant des buts, et en obéissant à des raisons ; ils ne se sont pas limités à les lire pour nous dans un livre caché qu'ils ont, de quelque manière que ce soit, su ouvrir ; en d'autres termes, l'activité humaine qui conduit à la donation d'une théorie mathématique n'est pas un dévoilement, elle est une constitution. Une fois constituées, les théories mathématiques obéissent à une logique interne qui, en tant que telle, est indépendante de leurs origines déterminées, qui rend même possibles des découvertes à l'intérieur d'elles, et qu'il est indispensable de saisir si on veut apprendre ces théories et en rechercher les origines, dans un mouvement de reconstruction qui est le travail propre de l'historien des mathématiques. Pourtant, si on veut comprendre ces théories pour le rôle qu'elles acquièrent dans l'édifice de la connaissance pris dans son ensemble, on ne peut pas se limiter à en saisir la logique interne, qui apparaît d'ailleurs souvent plus clairement lorsqu'on la retrouve comme issue d'une constitution répondant à des buts et des raisons. S'il n'est pas toujours nécessaire pour cela d'aller très loin dans une recherche proprement historique, il me semble qu'une telle compréhension d'un système de résultats mathématiques doit intégrer la reconstruction et, pour ainsi dire, la prise de conscience du processus qui a conduit à la constitution de ce système, sous la forme minimale d'une explicitation des buts auxquels cette construction est censée répondre, des problèmes qu'elle est censée résoudre, en un mot, de ses raisons d'être et d'être telle ou telle.

L'exposé qui suit est entièrement issu d'un effort d'éclaircissement de ces buts. Quel que soit le sujet abordé, j'ai tenu à joindre à l'exposition de chaque résultat que j'ai décidé de présenter dans mon texte un éclairage (le lecteur jugera s'il est suffisant ou non) de ses raisons d'être et d'être tel qu'il est. Il me semble d'ailleurs que l'absence de tout effort d'explication de ces raisons est l'obstacle le plus important auquel un lecteur dépourvu d'une culture mathématique suffisante, est confronté lorsqu'il aborde un texte de mathématique courant. Cet effort d'éclairage est ainsi un des aspects par lesquels mon livre diffère des manuels à l'usage des étudiants en mathématiques et/ou des mathématiciens professionnels.

Mon second point est le suivant : je comprends l'activité mathématique essentiellement comme la construction de systèmes d'objets. Certes, un mathématicien énonce des propositions et, dans la plupart des cas, les accompagne de preuves, qui ne sont à leur tour que des enchaînements d'autres propositions. Si on ne reste qu'à la surface des choses, on peut dire que son activité est une performance linguistique. Il me semble pourtant que pour comprendre les raisons d'être et d'être telle qu'elle est de cette performance, il est nécessaire de penser ces propositions soit comme des moyens de fixer la référence d'autres propositions, c'est-à-dire de

définir ou plus généralement d'introduire des objets sur lesquels d'autres propositions porteront ensuite, soit comme des manières de parler de ces objets, d'en énoncer des propriétés. Pour être bref, je dirais simplement que ces objets correspondent à des formes saillantes des phénomènes qui nous entourent. La capacité et le but du mathématicien sont justement d'isoler ces formes de leur contenu et de trouver une manière de les présenter, les manipuler et les étudier comme telles, comme des objets. Pourtant, comme chaque philosophe devrait le savoir, la distinction entre forme et contenu n'est jamais rigide ; elle n'est pas fixée d'elle-même dès qu'est fixé l'objet ou le phénomène duquel on dira plus tard qu'une certaine forme relève. La détermination de cette forme et sa séparation du contenu qu'elle enveloppe est déjà un acte d'interprétation qui fait partie du processus de construction ou, si on préfère, de définition de la forme en tant qu'objet.

Or, la définition d'un objet relève essentiellement (même si je ne crois pas qu'elle ne consiste qu'en ceci, comme on le dit souvent) de la détermination d'un critère d'identité, c'est-à-dire de la fixation des conditions sous lesquelles on peut dire d'un objet qu'il se manifeste d'une certaine manière, qu'il est ou qu'il n'est pas le même objet qui s'était manifesté ou se manifestera à nouveau d'une autre manière. On peut imaginer que pour ce faire, il soit nécessaire de savoir préalablement distinguer entre objets et formes de manifestation de ces objets. Il me semble pourtant que cette distinction n'est pas préalable, mais est plutôt partie du processus de fixation des critères d'identité d'un objet. Ceci est particulièrement évident lorsque la fixation de ce critère d'identité tient à la définition d'une relation d'équivalence entre formes de manifestation, ou si on préfère utiliser un vocabulaire kantien, entre représentations. Les objets mathématiques ne sont pas les seuls qu'on peut caractériser de cette manière et celle-ci n'est pas la seule manière par laquelle on peut parvenir à caractériser ces objets. En mathématiques, les choses vont cependant souvent ainsi : on dispose d'un domaine d'objets préalables, disons de niveau un (qu'on sait distinguer entre eux), et on décide de penser ces objets comme des formes de manifestation, des représentations, d'autres objets, disons de niveau deux ; pour ce faire, ou à la suite de cette décision, on définit une relation d'équivalence sur les objets dont on dispose et on suppose que deux objets distincts, mais équivalents, de niveau un valent comme des formes de manifestation du même objet de niveau deux. Celle qui n'est donc, par rapport aux objets du niveau un, qu'une relation d'équivalence quelconque devient, par rapport aux objets de niveau deux, une relation d'identité, c'est-à-dire une relation d'équivalence fort particulière.

Ce mode de caractérisation sera constamment à l'œuvre dans mon exposé. Cela revient à dire que la définition des objets mathématiques dont il y sera question reposera d'une manière ou d'une autre sur la définition d'une relation d'équivalence propre à un domaine d'objets préalables et sur son emploi pour définir une relation d'identité donnant lieu à un nouveau domaine d'objets.

Lorsqu'on présente une théorie mathématique déjà constituée, on a tendance, pour simplifier les choses et éviter une régression laborieuse, à présenter la relation d'identité comme étant elle-même déjà donnée. C'est alors, en général, cette relation qu'on note par le symbole « = ». Ce symbole intervient alors entre deux autres symboles et indique que ces deux symboles dénotent le même objet. Par ailleurs, l'usage actuel de la communauté mathématique étant de présenter toute théorie mathématique par le truchement de la théorie des ensembles, tout objet mathématique se présente en dernière analyse comme un ensemble particulier et la relation d'identité qui se rapporte à cet objet prend la forme d'une identité ensembliste. Dans la plupart des manuels modernes de mathématiques, le symbole « = » est utilisé pour dénoter cette relation et il indique que les deux symboles entre lesquels il intervient dénotent le même ensemble (où la signification de la notion 'être le même ensemble' est fixée par l'axiomatique de la théorie des ensembles). À côté du symbole « = », on introduit ensuite d'autres symboles, tels

que les symboles « $\equiv$ », « $\approx$ », ou « $\cong$ », pour indiquer d'autres relations d'équivalence distinctes de l'identité.

Cette présentation, sans doute très appropriée à beaucoup d'égards, a le défaut de cacher le processus qui donne origine à une théorie mathématique. Elle ne peut donc pas être adoptée lorsqu'on veut insister sur les raisons d'être et d'être telle qu'elle est d'une théorie mathématique. Pour cela, il faut en effet choisir un ordre d'exposition pour ainsi dire génétique. Comme définir un objet revient, en dernière instance, à en fixer le concept, je qualifierai cet ordre de « génétique des concepts ». Le choix de cet ordre d'exposition m'a conduit à adopter une approche différente de celle que je viens de décrire, qui ne récuse pourtant pas la possibilité d'utiliser de notions ensemblistes au cours de l'exposition (tout en pensant l'axiomatisation de la théorie des ensembles comme la définition d'un domaine d'objets mathématiques parmi les autres). Je traiterai dans la suite la relation d'égalité indiquée par le symbole « $=$ » comme une relation d'équivalence distincte, en général, de l'identité (encore que tout objet sera évidement conçu comme étant égal à lui-même, quelle que soit la manière dont on définisse la relation d'égalité), et qui sera introduite à chaque fois à nouveau, lorsqu'on en viendra à des nouveaux domaines d'objets. Aucun niveau préalable ou universel n'est donc censé supporter la signification du symbole « $=$ » comme un symbole d'identité. Dans certains contextes, et en particulier, après qu'on eut décidé de définir un objet comme une classe d'équivalence sous la relation d'égalité, ce symbole servira à indiquer une identité, car il pourra par exemple exprimer le fait que deux objets de niveau un appartiennent à une même classe d'équivalence, constituant un objet de niveau deux, et sont donc, tout en étant distincts en tant qu' objets du niveau un, des formes de manifestation du même objet de niveau deux. Et comme souvent la logique du raisonnement mathématique intègre une sorte d'oubli nécessaire de l'objectivité originaire, cela reviendra à dire que deux symboles distincts (la distinction des symboles demeurant comme la trace d'une distinction objectale oubliée) dénotent le même objet. Cette identité ne devra pourtant pas être pensée, dans le contexte de mon exposition, comme une identité universelle. Elle ne sera que la conséquence d'une définition d'objets, faite par abstraction, à partir de la donation d'un domaine d'objets préalables.

Une conséquence plus particulière du choix de suivre, dans mon exposition, l'ordre génétique des concepts, est que l'ensemble des nombres réels ne sera défini qu'à l'issu de mon cheminement, alors que la plupart des manuels modernes de mathématiques élémentaires définissent cet ensemble au tout début. Cet usage qui renverse autant l'ordre historique, que l'ordre génétique des concepts, leur permet de disposer d'emblée d'un contexte très confortable pour opérer algébriquement et d'éviter beaucoup des restrictions que caractérisent en revanche mon exposé. Si j'ai choisi de ne traiter des nombres réels qu'à la fin, c'est qu'il m'a semblé que les avantages opératoires de l'ordre d'exposition habituel (qui suppose les théories mathématiques exposées comme étant déjà données) ont souvent pour prix l'incompréhension du processus intellectuel qui conduit à la construction de la théorie mathématique des nombres réels, dont précisément l'exposition est le point culminant de mon discours.

Après avoir défini l'ensemble des nombres réels, la plupart des manuels de mathématiques ne traitent les nombres rationnels et les nombres naturels que comme des nombres réels particuliers, dont la nature est considérée comme étant connue. Il est en particulier assez rare de trouver, dans les nombreux volumes qui occupent une bibliothèque d'un département de mathématiques, une exposition du processus qui conduit à la construction de l'ensemble des nombres naturels et à la définition, sur cet ensemble, des relations et des opérations habituelles. Cette exposition est en revanche le point de départ de mon exposé et occupe les deux premiers chapitres de mon livre. On pourra trouver le chapitre 2, ou au moins certaines de ses parties, assez fastidieux du fait qu'on y utilise des démarches formelles pour démontrer des résultats qui font partie de la

culture mathématique la plus élémentaire. Mon but, dans ce chapitre, est de montrer comment cette culture élémentaire peut être réduite à un système d'axiomes qui exprime une forme universelle. Il ne s'agit pas, par exemple, d'enseigner que l'addition sur les nombres naturels est commutative, mais de montrer comment la commutativité de l'addition sur les nombres entiers se rattache à un système d'axiomes et de définitions dicté par l'effort de fixer la nature logique d'une progression.

## III

Lorsqu'il était question pour moi de décider de m'engager dans la rédaction d'un manuel, un collègue m'invita à réfléchir sur une circonstance que je n'avais pas considérée. Il est possible, me dit-il, que beaucoup d'étudiants, se reposant sur la possibilité de consulter ton texte, ne viennent plus à ton cours. Cette observation, sans doute conforme à la réalité, loin de me dissuader, me convainquit au contraire d'écrire mon livre.

Souvent les étudiants universitaires préparent leurs examens sur les notes de cours et uniquement sur celles-ci, sans se donner la peine d'acquérir et lire des livres. La remarque de mon collègue me fit comprendre soudainement que ce n'était pas seulement de leur faute. C'est que souvent le système universitaire est pensé pour réduire au strict indispensable l'étude individuelle et pour maintenir les étudiants le plus longtemps possible sous l'aile protectrice des enseignants. Il y a de nombreuses raisons, historiques, politiques, sociologiques et même psychologiques pour ceci. Il ne s'agit pas ici de les discuter. Une formule suffira pour résumer la situation : les universités sont souvent conçues comme un lieu d'enseignement plutôt que comme un lieu d'études.

Le livre est le symbole et l'outil principal d'un étude et en particulier de cette forme fondamentale et inévitable d'étude qu'est l'étude individuelle. J'ai toujours accompagné mes cours d'indications de lecture et cherché à éviter de distribuer des photocopies, symbole néfaste d'une lecture remise à jamais. Mais pour mon cours de mathématique pour étudiants de philosophie j'étais en difficulté : quels livres conseiller ? Ce n'est pas qu'il n'y ait pas de livres d'introduction aux mathématiques, plus ou moins spécialement adressés à des philosophes ou à des étudiants de philosophie. Il y en a même plusieurs : des plus classiques — comme ceux de F. Waismann (*Einführung in das mathematische Denken*, Wien, 1936), de R. Courant et H. Robbins (*What is Mathematics*, Oxford 1941 ; deuxième édition révisée par I. Steward, Oxford 1996), de T. Dantzig (*Numbers. The Language of Sciences. A critical Survey Written for the Cultured Non-Mathematicians*, 3rd ed., London, 1947), ou de D. E. Littlewood (*The Skeleton Key of Mathematics*, London, 1949) — aux plus récents — comme ceux de M. Kline (*Mathematics for Liberal Arts*, Reading, Mass., 1967), de I. Steward (*Concepts of Mathematics*, Harmondsworth, Middlesex, 1975), ou de K. Jacobs (*Resultate : Ideen und Entwicklungen in der Mathematik*, Braunschweig und Wiesbaden, 1987 ; ou de D. M. Davis, *The Nature and Power of Mathematics*, Princeton, 1993). Mais aucun de ces livres (envers lesquels je nourris des sentiments fort variés) n'est traduit en français, et, malgré mes incitations à lire, en anglais, le chef d'œuvre de Courant et Robbins — un livre magnifique dont je conseille la lecture à tous —, très peux parmi mes étudiants ont montré d'être en condition de le faire. J'ai ainsi saisi l'occasion et j'ai écrit, à ma manière, mon propre livre.

En principe, il devrait pouvoir être lu par n'importe qui, même si, pour le choix du langage et le style de l'argumentation, il s'adresse prioritairement à des lecteurs qui possèdent une culture et une sensibilité philosophique minimale. Cette visée ne m'a pas poussé, pour autant, à faire l'économie de développements techniques nécessaires.

Norbert Wiener fut un grand mathématicien, mort en 1964. On raconte que son père, Leo Wiener, soutenait que les enfants ne savent pas qu'il sont des enfants mais l'apprennent parce

que les adultes les traitent comme tels. Il suffit de les traiter comme des adultes et de leur parler en conséquence, pour leur éviter de perdre du temps précieux avec l'enfance et l'adolescence. Leo Wiener appliquait cette théorie à son fils : d'abord, il s'occupa personnellement de sa formation, puis l'envoya au lycée à l'âge de neuf ans ; à onze ans Norbert Wiener eu son baccalauréat, et à dix-neuf il obtint son PhD à l'université de Harvard. Le père de Norbert Wiener avait certainement tort, dans l'ensemble, et il fit probablement de son fils un homme malheureux, mais sur un point il avait raison : souvent les ignorants et les idiots ne le sont que parce qu'on les a toujours traités comme tels. Moi, je ne me suis pas permis de traiter mes lecteurs en ignorants ou en idiots : ce n'est pas sous le prétexte de sa difficulté que j'ai évité de présenter un argument, une notion, un résultat qui m'a semblé essentiel dans l'économie de mon exposé.

Cela n'empêche pas que j'ais toujours cherché à expliquer de la manière la plus claire, au prix parfois de quelques longueurs, tout ce qui m'a semblé pouvoir poser problème, sans recourir à des banalisations, ou répéter des simplifications usuelles : je me suis efforcé de ne jamais dire de choses fausses ou imprécises, en m'appuyant sur nécessités de la simplicité ; si je l'ai fait, c'est simplement que je me suis trompé et j'espère alors qu'on me corrigera.

## VI

Ma formation est celle d'un philosophe. Mes compétences mathématiques élémentaires me viennent certes d'une étude individuelle, mais aussi, et surtout, de la fréquentation de plusieurs amis qui ont été, pour des raisons diverses et en des temps différents, des maîtres pour moi. C'est un plaisir pour moi de reconnaître la dette que j'ai envers eux et de les remercier. Je voudrais d'abord rappeler Ernest Coumet : ceux qui ont eu le privilège de le connaître ne peuvent que se sentir plus pauvres après qu'il nous a quitté. Puis : Luis Carlos Arboleda, Michel Blay, Manuel Carpintero, Karine Chemla, José Diaz, Jean Dhombres, Paolo Freguglia, Massimo Galuzzi, Jean-Louis Gardies, Giulio Giorello, Enrico Giusti, Angelo Guerraggio, Niccolò Guicciardini, Giorgio Israel, Carlos Lopez-Beltran, Antoni Malet, Susanna Marietti, Rafael Martinez, Domenico Napoletani, Michael Otte, Jean Petitot, Jean-Claude Pont, Roshdi Rashed et Daniele Struppa. Je dois en outre des remerciements particuliers aux nombreux amis, parmi lesquels beaucoup devraient aussi apparaître dans la liste précédente, avec lesquels j'ai discuté de passages de mon livre, et qui m'ont aidé de manières diverses, au cours de sa rédaction, avec des conseils, des informations, des explications, des critiques et d'autres services variés. C'est, entre autres, le cas de : José Alfredo Amor, Alejandro Bravo, Roberto Casati, Salvador Barberà, Béatrice Daille, Chantal Enguehard, Jean-Louis Fournel, Vincent Jullien, Anila Karadumi, Jan Lacki, Michelle Lemaitre, Sébastien Maronne, Lilliana Morandi, Gloria Origgi, Francesco, Laura et Mario Panza, David Rabouin, Jean-Michel Salanskis, François Schmitz, Farid Si Moussa, Rossana Tazzioli, et Benoît Timmermans. Ma dette est encore plus grande envers Carlos Alvarez, Silvia Annaratone, Brigitte Cicognini, Fernand Doridot, Denis Robin, Loïc Lamy, Sabine Rommevaux et Rodolphe Thévenot, qui ont relu patiemment de grandes parties, ou même la totalité de mon manuscrit, ont avancé des critiques et m'ont conseillé des corrections, aussi bien mathématiques que linguistiques. L'aide de François Loget a été enfin fondamentale : sans lui je n'aurais jamais écrit mon livre.

Je remercie en outre le conseil d'administration de la Société française d'histoire des csiences et des techniques, et en particulier son président Bernard Joly, pour avoir suivi le conseil de Vincent Jullien et avoir accepté de faire paraître mon livre parmi les *Cahiers d'histoire et de philosophie des sciences*.

Mon remerciement s'adresse aussi à tous mes étudiants, dont les réussites aussi bien que les échecs m'ont beaucoup appris. Je remercie en particulier cet étudiant, dont je ne connais

pas le nom, qui dans une copie d'examen a soutenu qu'un ensemble non dénombrable est un ensemble dont les éléments « sont caractérisés plus par leur degré d'absence que par leur degré de présence. » Il a largement contribué à me convaincre de la nécessité d'écrire mon livre.

Mon dernier remerciement est enfin pour ma femme Annalisa Coliva, pour sa présence, son exemple et ses conseils.

Varese, Italie, Août 1998 et Avril 2004.

# Avertissements

Mon exposé comporte trois niveaux, clairement distingués par l'usage de caractères typographiques distincts.

Le premier niveau est constitué par la présentation des théories mathématiques qui font l'objet principal de mon discours. Au deuxième niveau appartiennent des remarques qui ont pour but d'accompagner cette présentation par des commentaires ou des éclairages. Le lecteur qui voudra éviter de lire ces remarques ne devrait pas avoir de peine à suive le fil de mon exposé, tout en étant privé d'un outil qui m'a semblé utile pour aider à parvenir à une compréhension moins superficielle. Le troisième niveau est enfin constitué par des notes historiques qui fournissent à mon discours des supports extérieurs. La lecture de ces notes peut sans doute être évitée. Elle sera néanmoins utile pour donner un cadre plus vivant aux théories considérées.

Chaque note historique est accompagnée d'indications bibliographiques. Certains des textes cités, encore que mentionnés une seule fois, relèvent de sujets traités dans plusieurs parties du livre et, pris dans leurs ensemble, devraient présenter au lecteur qui voudra le consulter un panorama assez large d'où il pourra tirer une compréhension plus profonde des ces sujets et d'autres connectés à ceux-ci.

Dans certains cas, surtout dans les notes historiques, j'ai été obligé à évoquer rapidement des notions que je n'ai éclaircies que plus tard, en suivant le fil de mon exposé. Le lecteur est dans ce cas invité à revenir après coup sur les passages concernés. Cette nécessité d'un aller-retour mise à part, mon livre devrait être autocompréhensif, au moins en ce qui concerne les notions mathématiques sur lesquelles il porte. Comme il a été écrit en premier lieu pour des étudiants de philosophie, je n'ai, en revanche évoqué qu'ici et là des notions philosophiques élémentaires que ces derniers devraient connaître. En particulier, j'ai parfois considéré comme acquises des notions de logique qui devrait constituer le contenu d'un cours propédeutique à cette discipline. En d'autres occasions j'ai pris le temps d'éclaircir d'autres notions analogues, qui m'ont semblé être plus profondément imbriquées à mon exposé. Pourtant je ne l'ai jamais fait en logicien, mais toujours du point de vue, pour ainsi dire concret, du mathématicien.

Parfois, je me suis abstenu de donner la preuve de quelques théorème. Surtout vers la fin du livre, en supposant mes lecteurs plus entraînés, je les ai explicitement invités à rédiger par eux-mêmes ces preuves en guise d'exercices. En d'autres cas, je me suis limité à déclarer ces preuves faciles. Une preuve facile ne doit pourtant pas être confondue avec une preuve non nécessaire. En mathématiques il n'y a pas de preuves non nécessaire : tout théorème en exige une. Si une preuve est négligée dans un exposé, ce n'est pas que le théorème auquel elle devrait se rapporter est évident. C'est simplement que la manière dans laquelle elle pourrait être rédigée est facile à imaginer. Bien que quelques textes de philosophie des mathématiques fassent une distinction entre ces termes, j'ai utilisé toujours les termes « preuve » et « démonstration » comme des synonymes parfaits.

Les guillemets doubles, à la français, indiquent soit une mention — d'un terme, d'une expression, d'un symbole, ou d'un énoncé —, soit une citation. J'ai rarement utilisé des italiques. J'y eu recours pour indiquer un terme ou une expression faisant l'objet d'une définition sans

apparaître sous la forme d'une mention (on dit que *ça et ça* lorsque ceci et ceci). La différence entre usage et mention devrait faire partie du bagage indispensable et même préventif de tout étudiant de philosophie. Pour aider rapidement ceux qui ne la connaissent pas, je dirai simplement qu'on parle de mention, par exemple d'un terme, lorsque ce terme est employé pour référer à lui-même, en tant que terme ; on parle en revanche d'usage d'un terme lorsque ce terme réfère à quelque chose de distinct de lui même et qui constitue sa signification. Voici un exemple de mention : le terme « Paris » est composé par cinq lettres. Ce n'est évidemment pas de la ville de Paris qu'il est ici question, mais du mot employé pour la désigner.

Les guillemets simples, à l'anglaise, servent par contre pour circonscrire des expressions et indiquer qu'elles doivent être prises comme un tout fonctionnant comme un nom propre. Je les ai néanmoins utilisées très rarement.

Bien qu'il soit principalement adressé à des étudiants de philosophie, mon livre devrait pouvoir profiter, lorsqu'ils le lisent à un autre niveau, à des philosophes professionnels, et, du moins pour certaines de ses parties, à des étudiants de sciences. J'espère enfin que, à un troisième niveau de lecture, il puisse être utile pour un public plus général de non-mathématiciens désireux d'acquérir quelques connaissances mathématiques élémentaires.

CHAPITRE 1

# Nombres entiers positifs : une théorie empirique

Ceux que nous appelons aujourd'hui « nombres entiers positifs » ou quelquefois « nombres naturels » ou même « nombres cardinaux », sont désignés par Euclide tout simplement comme « nombres » : Euclide appelle génériquement « nombres » des objets qu'il dénomme en particulier « un », « deux », « trois », etc., et qui se comportent, relativement les uns aux autres et par rapport à la pratique du comptage, comme le font nos nombres naturels. Pourtant, Euclide ne définit ses nombres que très rapidement, comme « multitudes d'unités » : il en parle dans les livres VII à IX des *Éléments* et les emploie dans les autres livres comme s'ils étaient des objets déjà connus, dotés de propriétés également connues. La manière dont il aurait pu les définir peut pourtant être imaginée assez facilement. Je vais l'exposer dans le paragraphe suivant.

NOTE HISTORIQUE 1.1. Les deux premières définitions du livre VII des *Éléments* sont les suivantes : « Est *unité* ce selon quoi chacune des choses existantes est dite une » ; « Et un *nombre* est la multitude composée d'unités ».

Euclide ne se réclame jamais de ces deux définitions dans les démonstrations des propositions qui les suivent. Ceci n'est pas un cas isolé dans les *Éléments*, qui sont au contraire assez riches en définitions qui semblent ne pas participer de la structure déductive de ce même traité ; c'est le cas, par exemple, des définitions du point, de la droite et du plan, au livre I. On a qualifié souvent ces définitions de « métaphysiques », en soulignant qu'elles n'ont d'autre but que d'enraciner les théories mathématiques d'Euclide dans certaines traditions philosophiques. Il faut pourtant observer que si, d'un point de vue moderne, on peut penser que la tâche de fixer les objets sur lesquels portent ces théories est remplie, dans le livre I, par les postulats (qui, en énonçant les règles en accord avec lesquelles on travaille sur les objets de la géométrie bidimensionnelle, définissent implicitement ces objets [sur la notion de définition implicite, cf. la note historique II.5]), l'absence de postulats propres au livre VII, et généralement aux livres arithmétiques des *Éléments*, fait retomber une telle responsabilité sur les seules épaules des définitions. Si Euclide peut donc éviter de se réclamer, lors de ses démonstrations, des définitions de l'unité et du nombre, c'est que ces démonstrations portent sur des objets qu'il peut supposer comme déjà donnés avec leurs propriétés fondamentales. Les définitions précédentes remplissent ainsi, entre autres, sinon la tâche d'exhiber ces objets, du moins celle de préciser de quels objets on parle, et d'indiquer, ne serait-ce que sommairement, le point de vue selon lequel ces objets sont considérés.

On a souvent souligné qu'en définissant l'unité ($\mu o \nu \acute{\alpha} \varsigma$, littéralement : « monade » ) à partir de l'un ($\tau \grave{o}\ \acute{\varepsilon} \nu$), et le nombre ($\alpha \rho \iota \theta \mu \acute{o} \varsigma$), à partir de la multitude ($\pi \lambda \tilde{\eta} \theta o \varsigma$) d'unités, Euclide (qui dans le livre VII semble exposer une théorie due en fait à Théétète) ait voulu mettre au cœur de son arithmétique l'opposition platonicienne de l'intelligible (l'unité et le nombre) et du sensible (l'un, dit d'une chose existante, et la multitude des choses existantes, dont le nombre, en tant que multitude d'unités,

est, en quelque sorte, la forme universelle). Cette interprétation est d'ailleurs à l'origine du choix, désormais canonique, de traduire le neutre pluriel « *τὰ ὀντα* », qui apparaît dans la première définition, par « choses existantes ». Plutôt que d'insister sur les colorations métaphysiques que l'opposition platonicienne assigne ainsi à l'exposé d'Euclide, il me semble intéressant d'observer que les définitions précédentes suggèrent une réduction, au moins opératoire, de l'unité et du nombre aux choses sensibles et à leurs collections. Tout en restant, en tant que tels, des objets abstraits, l'unité et les nombres se font ainsi reconnaître dans des objets empiriques, car ils sont pensés, en dernière instance, non pas comme des principes universels expliquant l'univers par le biais d'une réduction au transcendant, mais comme des formes d'objets d'expérience, qui n'acquièrent leur autonomie que par un processus d'abstraction. Derrière la citation platonicienne se dessine ainsi une rupture forte et féconde avec la tradition pythagoricienne qui restait largement vivante chez Platon.

Tout en définissant les nombres de cette manière, Euclide les représente souvent, dans ses démonstrations, par des segments. Ces derniers servent pourtant plus à représenter des relations parmi les nombres ou des opérations sur ceux-ci, que les nombres eux-mêmes ; ils interviennent dans les arguments d'Euclide lorsqu'il est justement question de relations et opérations entre et sur les nombres analogues aux relations qui se trouvent entre les segments et aux opérations qui s'appliquent à ceux-ci. Cette pratique d'Euclide revient ainsi à souligner que nombres et segments partagent des propriétés relationnelles : ce sont ces propriétés qui font des uns et des autres des quantités.

Il reste à observer que des définitions précédentes, il resulte que l'unité n'est pas un nombre. Le plus petit des nombres euclidiens est donc deux. Même si la terminologie adoptée par Euclide, tout au long de ses livres arithmétiques, est parfaitement conséquente à cette limitation, cela n'empêche pas Euclide de comprendre qu'entre l'unité et les nombres il y a une relation qui fait que ces derniers ne peuvent être étudiés que par rapport à la première. L'exclusion de l'unité du domaine des nombres n'a donc pas, d'un point de vue opératoire, de conséquences majeures. Dans l'exposé qui suit, on se conformera aux usages courants, et on traitera l'unité comme un nombre parmi les autres.

**Lectures possibles** : B. Vitrac, « Notice sur les Livres arithmétiques », *in* Euclide, *Les Éléments*, traduction et commentaires par B. Vitrac, vol. II, PUF, Paris, 1994, pp. 269-289.

* * *

Bien que les *Éléments* soient le livre de mathématiques le plus édité et étudié de l'histoire, on ne connaît à peu près rien de son auteur, Euclide, et, à être précis, on n'est même pas sûrs que les *Éléments* soient l'œuvre d'un seul homme, exposant et organisant à sa manière, dans un seul traité, divisé en plusieurs livres (treize, si on fait confiance aux reconstructions jugées aujourd'hui les plus soignées), différentes théories mathématiques, dont certaines assurément dues à des mathématiciens précédents. En s'appuyant sur les rares témoignages dont on dispose, on conjectur e qu'Euclide enseigna à Alexandrie au début du III$^{\text{ème}}$ siècle av. J.C., où on peut croire qu'il fut attiré par Ptolémée, lors de la fondation du Musée et de la Bibliothèque. On peut penser qu'Euclide écrivit les *Éléments* pour ses étudiants, et qu'il y exposa le contenu de ses cours d'introduction aux mathématiques. D'autres témoignages nous

font penser qu'Euclide ait fait partie de l'Académie, même si rien ne nous assure qu'il fut un disciple direct de Platon, son fondateur.

Les *Éléments* ne sont pas le seul traité mathématique qu'on attribue à Euclide. Parmi les autres, un seul nous est parvenu. Il s'agit des *Données*, une récolte de propositions géométriques où, en partant de l'hypothèse que certains éléments d'une figure géométrique sont connus (donnés), on conclut que d'autres peuvent à leur tour être déterminés (et sont donc à leur tour donnés, même s'ils le sont seulement indirectement). D'autres traités, attribués à Euclide, sont en revanche perdus, et on ne peut qu'en conjecturer le contenu. Parmi ceux-ci : un traité sur les divisions des figures, un autre consacré aux arguments fallacieux, une récolte de *Porismes* (fort probablement un ensemble de problèmes de géométrie non élémentaire), un traité de coniques, précédant celui d'Appollonius, un traité consacré aux lieux géométriques, une œuvre d'astronomie, généralement dénommée « *Les Phénomènes* », une *Optique*, une *Section du Canon*, et même une *Mécanique*.

**Lectures possibles** : M. Caveing, « Introduction générale », Euclide, *Les Éléments*, traduction et commentaires par B. Vitrac, vol. I, PUF, Paris, 1990, pp. 13-148.

## 1. Les nombres entiers positifs en tant que corrélats de l'acte de compter

Imaginons qu'on sache distinguer dans notre univers sensible des collections d'objets, c'est-à-dire qu'on sache distinguer un objet d'un autre, et qu'on sache ordonner les objets (matériellement ou mentalement) de manière à savoir distinguer ceux qui appartiennent à un certain groupe d'objets de ceux qui appartiennent à un autre groupe. Peu importe la raison qui nous amène à faire ces distinctions ; l'important est que nous les fassions.

Qu'on prenne alors une collection d'objets distincts et qu'on l'appelle « $\mathfrak{C}$ ». Considérons lun après lautre les objets de cette collection et déplaons-les (mentalement ou physiquement, peu importe), de sorte á former progressivement une collection nouvelle constituée par les objets qui on a déjá t déplacés. On dira qu'en faisant ceci on compte les objets de $\mathfrak{C}$, ou, pour faire plus simple, qu'on compte $\mathfrak{C}$ elle même. Imaginons maintenant que la collection $\mathfrak{C}$ soit telle que, au bout d'un certain temps, en répétant toujours la même opération, on parvienne à déplacer tous les objets dont elle est composée de sorte que la collection des objets qu'on a déjá déplacés soit identique à la collection qui avait d'abord été donnée. On dira alors que la collection $\mathfrak{C}$ a été épuisée, ou même qu'on l'a complètement compt'ee. Qu'on remarquer la différence entre compter une collection et l'avoir complètement comptée : on peut compter une collection sans jamais parvenir à l'avoir complètement comptée. Une collection qui peut être épuisée, c'est-à-dire qu'au bout d'un certain temps on peut parvenir à l'avoir complètement comptée est dite « finie ». Dorénavant, au cours du présent chapitre, on ne parlera de collections d'objets que pour se référer à des collections finies. L'opération de comptage ainsi définie ne demande pas qu'on sache ce que sont les nombres entiers positifs, ni qu'on connaisse leurs noms. Au contraire, c'est parce qu'on sait accomplir cette opération (repérer/déplacer) qu'on sait reconnaître ce que sont les nombres (entiers positifs).

Prenons maintenant une collection d'objets $\mathfrak{C}_\alpha$ et, avant de commencer à en compter les objets, qu'on en prenne une autre $\mathfrak{C}_\beta$. On peut apprendre facilement à compter ces collections alternativement : d'abord on considère un objet de $\mathfrak{C}_\alpha$ et on le déplace ; ensuite on considère un objet de $\mathfrak{C}_\beta$ et on le déplace à son tour ; on revient ensuite à $\mathfrak{C}_\alpha$ dont on dépalce un autre objet, puis à $\mathfrak{C}_\beta$, et ainsi de suite jusqu'à épuisement de l'une ou l'autre de ces collections. Cette opération (ou procédure) sera dite dans la suite « opération de comptage alterné ».

Imaginons maintenant que $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ soient telles que, lorsqu'on a épuisé $\mathfrak{C}_\alpha$, $\mathfrak{C}_\beta$ n'est pas encore épuisée, mais qu'elle le soit dès qu'on a déplacé l'objet considéré immédiatement

après qu'on a épuisé $\mathfrak{C}_\alpha$. Comme on avait commencé à compter $\mathfrak{C}_\alpha$, on pourra dire que les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ s'épuisent en même temps sous l'opération de comptage alterné. On peut alors introduire une première définition.

DÉFINITION 1.1. *Quand les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont telles qu'elles s'épuisent en même temps, sous l'opération de comptage alterné, on dit qu'elles ont le même nombre d'objets.*

REMARQUE 1.1. Le but de cette définition est de fixer la signification de l'expression « avoir le même nombre d'objets ». Il devrait être clair que cette signification est ainsi fixée avant qu'on ait assigné une quelconque signification au terme « nombre ». Loin de faire dépendre la signification de l'expression « avoir le même nombre d'objets » de la signification du terme « nombre », l'on fera ici dépendre la signification du terme « nombre » de celle de l'expression « avoir le même nombre d'objets ». En général, ceci revient à faire dépendre la définition d'un ou plusieurs objets de celle d'une relation. C'est une procédure courante en mathématiques.

Un univers d'objets préalable étant donné, il s'agit de définir sur ces objets une relation d'équivalence et de définir ensuite de nouveaux objets grâce aux classes d'équivalence associées à cette relation.

On reviendra plusieurs fois par la suite sur la notion de relation d'équivalence et l'on la définira précisément dans le chapitre 2. Ici, il suffira de dire, fort informellement, qu'une relation d'équivalence entre deux objets $a$ et $b$ est une relation qui s'établit entre ces objets lorsqu'ils sont tels que, si on ne les considère que sous un certain aspect, alors ils ne peuvent pas être distingués. La définition d'une telle relation revient ainsi à fixer l'aspect sous lequel ces objets doivent être considérés. Si la définition est suffisamment claire, elle permet, lorsqu'un objet $a$ du domaine préalable est donné, de former la classe de tous les objets de ce domaine qui sont impossibles à distinguer de l'objet donné sous l'aspect considéré — et sont donc équivalents à celui-ci —, et de faire ceci de telle sorte que si on considère un autre objet $\tilde{a}$ de ce même domaine préalable qui n'appartient pas à cette classe, alors la classe des objets du domaine préalable qui sont équivalents à $\tilde{a}$ n'a aucun élément en commun avec la classe des objets de ce domaine qui sont équivalents à $a$. Les classes ainsi construites s'appellent « classes d'équivalence » et sont telles que leur intersection sur le domaine d'objets préalable est nulle et que leur union correspond à ce domaine lui-même. Lorsque la définition d'une relation d'équivalence a permis d'opérer une telle partition du domaine d'objets préalable, on dira qu'on a défini des classes d'équivalence sur ce domaine par cette relation. On pourra alors considérer les différentes classes d'équivalence ainsi définies comme de nouveaux objets, qui pourraient être directement les objets qu'on voulait définir, ou participer à leur définition. Quelques fois on appelle les définitions de cette sorte « définitions par abstraction à la Frege ». La définition des nombres entiers positifs qu'on va donner par la suite est justement une définition par abstraction à la Frege.

NOTE HISTORIQUE 1.2. En 1884 apparaît à Breslau un court essai de G. Frege (Wismar, 1848 ; Bad Kleinen, 1925) dont le titre — *Die Grundlagen der Arithmetik* — énonce, à lui tout seul, un programme fort ambitieux : fournir une réponse précise et exacte à la question : « qu'est-ce qu'un nombre (entier positif) ? ». La réponse avancée par Frege dépend, pour l'essentiel, d'une conception philosophique concernant la nature de l'objectivité mathématique qui est loin d'être généralement partagée. D'après Frege, les nombres sont des objets déterminés, qui existent indépendamment de toute activité humaine, et sont donc préalables à la mise en place de toute théorie mathématique ; le but des *Grundlagen* est de dire de quels objets il s'agit. Cette conception de l'objectivité mathématique n'est pas la mienne. Pourtant, il me semble

que la définition proposée par Frege pour les nombres entiers positifs, une fois libérée des implications ontologiques auxquelles elle se rattache, est riche de suggestions intéressantes, et que rien ne s'oppose à présenter l'arithmétique à partir de définitions proches de celles de Frege. L'exposition des éléments fondamentaux de l'arithmétique que je propose dans le présent chapitre s'apparente d'ailleurs, sous plus d'un aspect, à la construction de Frege.

En particulier, et c'est le point sur lequel il me semble nécessaire d'insister, Frege pense que pour dire ce qu'est un nombre, il faut d'abord fixer une relation d'équinuméricité qui, d'après lui, porte sur des concepts. Pour Frege, savoir répondre à la question « qu'est-ce qu'un nombre ? » signifie savoir assigner une signification aux termes numéraux qui interviennent aussi bien dans notre langage quotidien que dans les propositions de l'arithmétique, et le faire de sorte que cette signification soit la même dans un cas comme dans l'autre. Frege commence donc par se demander : á propos de quoi affirme-t-on quelque chose, lorsqu'on énonce un jugement numérique qui attribue un nombre à quelque chose ? Sa réponse est la suivante : l'attribution d'un nombre contient toujours une affirmation à propos d'un concept. Dire de Vénus qu'elle possède zéro satellites c'est dire quelque chose du concept 'satellite de Venus'. En particulier, ce qu'on dit de ce concept lorsqu'on dit que Venus possède zéro satellites, c'est qu'il n'y a aucun objet qui tombe sous ce concept.

On pourrait penser que cette analyse de la proposition « Venus possède zéro satellites » est circulaire, car elle semble conduire à expliquer le terme « zéro » par le terme « aucun ». Pourtant si on regarde la chose de près, on voit que ce n'est pas le cas. L'analyse de Frege ne vise pas à expliquer le terme « zéro », mais à montrer le rôle que ce terme joue dans la proposition en question. La conclusion à laquelle cette analyse parvient est donc la suivante : une proposition dans laquelle intervient un terme numéral doit être pensée comme l'assignation d'un nombre à un concept. Par exemple, la proposition « le carrosse de l'empereur est tiré par quatre chevaux » doit être analysée ainsi : « au concept 'chevaux qui tirent le carrosse de l'empereur' est attribué le nombre quatre ». De là, il s'ensuit que, dans le langage quotidien, de même que dans les propositions de l'arithmétique, les termes numéraux peuvent être conçus comme noms d'objets. Une proposition dans laquelle intervient un terme numéral doit donc être pensée comme l'association d'un objet (un nombre) à un concept.

Comme on dira qu'une proposition qui assigne le nombre $n$ au concept $F$ est vraie si et seulement si le nombre $n$ s'applique au concept $F$, il s'agit alors de comprendre ce que signifie qu'un nombre $n$ s'applique à un concept $F$. Pour répondre à cette question, Frege s'appuie sur la notion d'extension d'un concept et de la définition d'une relation d'équinuméricité entre concepts. Pour aller vite, on pourra dire d'abord que l'extension d'un concept est l'ensemble des objets qui tombent sous ce concept, ou, si on préfère : l'extension du concept $F$ est l'ensemble des objets qui, mis à la place de $x$, rendent vraie la proposition « $x$ est $F$ ». Deux concepts $F$ et $G$ sont alors équinumériques si et seulement si leurs extensions respectives sont en bijection, c'est-à-dire (comme on le verra ci-dessous) qu'il est possible d'associer à chaque élément de la première extension un et un seul élément de la deuxième extension, de telle sorte que, de cette manière, chaque élément de la deuxième extension se trouve associé à son tour à un et un seul élément de la première extension.

Or, d'après Frege, un nombre est l'extension d'un concept, c'est-à-dire un ensemble. Le nombre qui s'applique au concept $F$ est, en particulier, l'extension du concept 'équinumérique au concept $F$', qui peut être pensé comme un concept de

deuxième niveau construit à partir du concept $F$, de telle sorte que son extension, qui, comme on vient de le dire est justement un nombre, est un ensemble d'extensions et donc un ensemble d'ensembles. Dire ainsi que le carrosse de l'empereur est tiré par quatre chevaux signifie dire que l'extension du concept 'équinumérique au concept 'chevaux qui tirent le carrosse de l'empereur » est le nombre quatre.

Cette dernière définition n'est naturellement pas encore une définition convenable du nombre quatre, et rien dans ce qui précède ne nous fournit de définition convenable des différents nombres. Pour passer de la définition précédente de la relation '$n$ s'applique à $F$', où $n$ est un nombre et $F$ un concept, à la définition des nombres, Frege ne fait que fixer des concepts paradigmatiques fonctionnant comme paramètres définitionnels pour les différents nombres. Il parvient à cela en observant que l'extension d'un concept auto-contradictoire tel que '(être) différent de soi-même' est nécessairement vide. L'extension du concept 'équinumérique au concept '(être) différent de soi-même » est ainsi l'ensemble de tous les ensembles vides. Frege identifie alors le nombre zéro à cet ensemble. Pour continuer, il suffit ensuite d'observer que, d'après cette définition, un objet est le nombre zéro si et seulement s'il est l'extension du concept 'équinumérique au concept '(être) différent de soi-même' ', en sorte que sous le concept '(être) identique à zéro' tombe l'extension du concept 'équinumérique au concept '(être) différent de soi-même' ' et aucun autre objet. Frege identifie alors le nombre à l'extension du concept 'équinumérique au concept '(être) identique à zéro' '.

On pourrait penser que cette définition du nombre un nous fournit un modèle qui peut être appliqué à tout nombre entier positif. On dirait alors que le nombre deux est l'extension du concept 'équinumérique au concept '(être) identique à zéro ou à un' ' ; le nombre trois est l'extension du concept 'équinumérique au concept '(être) identique à zéro, un ou deux' ' ; et ainsi de suite. Cependant cette dernière clause « et ainsi de suite » dénonce que de cette manière la définition de l'ensemble des nombres entiers positifs, conçu comme étant un ensemble infini (cf. la note 2.3 et la remarque qui la précède), dépendrait de l'hypothèse qu'on a la capacité de répéter indéfiniment le même geste définitoire et que cette capacité de répétition indéfinie vaut comme condition suffisante pour admettre qu'il y a une infinité de nombres de la sorte. Frege avait plusieurs raisons pour refuser cette démarche éminemment constructive et pour lui préférer une démarche corrélative (cf. la note 1.4). Une de celles-ci dépendait du fait que par sa définition il visait à montrer que l'arithmétique peut être réduite à la logique et il ne pouvait de ce fait se rendre à la nécessité d'une définition du prédicat '(être) un nombre entier positifs' dépendant d'une supposition extra-logique, telle l'acceptation d'une capacité à répéter un certain geste. C'est la raison pour laquelle, avant de définir le nombre un, il définit la relation de successeur dans la suite des nombres qui s'appliquent à des concepts comme étant la relation qui lie entre eux le nombre qui s'applique à un certain concept $F$ dont l'extension n'est pas vide et comprend un certain objet $x$ et le nombre qui s'applique au concept 'tomber sous $F$, mais être différent de $x$', le second de ces nombres étant le successeur du second. Il montre ensuite que le nombre un, défini comme on l'a dit, est le successeur du nombre zéro dans la suite des nombres qui s'appliquent à des concepts. Puis il définit le relation 'suivre en une succession' comme on définit aujourd'hui l'ancestrale d'une certaine relation (cf. ci-dessous, p. 62) et caractérise enfin, parmi les nombres qui s'appliquent à des concepts, ceux qui suivent zéro dans la succession de ces nombres, en les qualifiant de finis. Ceux-ci sont justement les nombres qu'on qualifie habituellement de nombres entiers positifs.

**Lectures possibles** : G. Frege, *Les fondements de l'arithmétique*, Seuil, Paris, 1970.

* * *

La définition des nombres entiers positifs proposée par Frege est fort ingénieuse, mais elle tombe sous une difficulté cruciale. Si $G$ est un concept dont l'extension n'est pas vide, alors l'extension du concept 'équinumérique au concept $G$' est, pour ainsi dire, trop grande pour pouvoir être traitée comme un ensemble. En particulier, il est aisée de montrer qu'il est possible d'associer à tout ensemble donné un ensemble différent qui soit équinumérique au concept $G$ et tombe ainsi sous cette extension. Imaginons par exemple que $G$ soit le concept '(être) identique à zéro' de sorte que son extension ne contienne que l'objet 'zéro'. Si $F$ est un ensemble quelconque, pour lui associer un ensemble qui soit équinumérique au concept $G$, il suffit de lui associer l'ensemble dont cet même ensemble $F$ est le seul élément. Il y aura donc au moins autant d'ensembles équinumériques au concept $G$ qu'il y a d'ensembles. Admettre ainsi que l'extension du concept 'équinumérique au concept $G$' puisse être traitée comme un ensemble équivaut à rendre possible le surgissement de paradoxes similaires à celui de Russell (cf. la note 1.6). Mais dans sa définition, Frege traite justement une telle extension comme un ensemble. Donc cette définition est inacceptable.

Récemment il a été cependant montré qu'il est possible d'obtenir une définition parfaitement acceptable des nombres entiers positifs en se limitant à postuler un principe que Frege avait employé dans son entreprise en l'attribuant à Hume et qui est aujourd'hui généralement appelé « principe de Hume ». Ce principe affirme que le nombre qui s'applique à un concept $F$ est le même que le nombre qui s'applique au concept $G$ si et seulement si $F$ et $G$ sont équinumériques. Une fois ce principe admis (et à condition d'admettre que les concepts peuvent être traités à leur tour comme des objets, ce qui revient, en termes techniques, à faire usage de celle qu'on qualifie habituellement de logique du deuxième ordre : une logique où l'on admet qu'un énoncé du type « pour toute propriété $P$, il est le cas que... » ait un sens), il est ensuite possible de définir l'ensemble des nombres entiers positifs (finis) sans dire explicitement ce que chaque nombre est (avec la seul exception du nombre zéro défini comme le nombre qui s'applique au concept '(être) différent de soi même'), ou, si l'on préfère, en traitant chaque nombre entier positifs (fini) comme une classe d'équivalence définie sur le domaine des concepts par la relation 'équinumérique avec' définie à son tour sur ce domaine. Cette définition constitue la pierre de touche d'un programme philosophique, dit « néo-logicisme », qui cherche aujourd'hui de réaffirmer, en les amendant convenablement, les conceptions de Frege.

**Lectures possibles** : C. Wright, *Frege's Conception of Numbers as Objects*, Aberdeen University Press, Aberdeen 1983 ; G. Boolos(1987), « The consistency of Frege's *Foundations of arithmetic* », *On being and Saying : Essays in Honor of Richard Cartwright*, J. Thomson éd., MIT Press, Cambridge (Mass.), 1987, pp. 3-20 ; C. Wright, B. Hale, ' *Reasons's Proper Study. Essays Towards a Néo-Fregean Philosophy of Mathematics*, Oxford University Press, Oxford 2001.

Il est facile de voir que l'opération de comptage alterné associe à chaque objet de la collection $\mathfrak{C}_\alpha$ un objet (et un seul) de la collection $\mathfrak{C}_\beta$. En particulier, elle associe à tout objet $x$ appartenant à $\mathfrak{C}_\alpha$ l'objet $y$ appartenant à $\mathfrak{C}_\beta$ qu'on déplace, en suivant la procédure de comptage alterné, tout de suite après avoir déplacé l'objet $x$. Il est alors facile de démontrer le théorème suivant :

THÉORÈME 1.1. *Si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont le même nombre d'objets, alors on peut associer à chaque objet de $\mathfrak{C}_\alpha$ un et un seul objet de $\mathfrak{C}_\beta$, de sorte que tout objet de $\mathfrak{C}_\beta$ soit de cette manière associé à un et un seul objet de $\mathfrak{C}_\alpha$.*

**Preuve** La manière la plus simple de réaliser une telle association entre les objets de $\mathfrak{C}_\alpha$ et de $\mathfrak{C}_\beta$ est justement d'exploiter l'association fournie par l'opération de comptage alterné. Comme pour prouver le théorème il suffit de montrer qu'une telle association est possible, cette réalisation est une preuve du théorème 1.1. □

REMARQUE 1.2. Comme on le voit, cette preuve ne fait référence qu'à la définition 1.1 et ne dépend en aucune manière de nos idées préalables sur ce que sont les nombres, ou sur ce que signifie que des collections ont le même nombre d'objets. Ceci est un trait distinctif des preuves mathématiques : elles ne se réclament de rien qui n'ait été explicitement posé dans le cadre de la théorie à laquelle elles appartiennent. Ainsi, si quelqu'un parmi les lecteurs pense que le théorème 1.1 est évident à lui tout seul et qu'il ne nécessite pas d'être démontré, qu'il réfléchisse sur ceci : cette évidence ne viendrait-elle pas de la présupposition de quelques connaissances préalables sur les nombres et l'égalité ? Comme l'objectif de ma démarche est justement de parvenir à justifier ces croyances, cette évidence ne pourrait alors être acceptée qu'au prix de tomber dans un cercle vicieux.

Une définition nous permettra d'être plus brefs par la suite :

DÉFINITION 1.2. *Si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont telles que tout objet de $\mathfrak{C}_\alpha$ peut être associé à un et un seul objet de $\mathfrak{C}_\beta$, de sorte que tout objet de $\mathfrak{C}_\beta$ soit de cette manière associé à un et un seul objet de $\mathfrak{C}_\alpha$, alors on dit que les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont entre elles en bijection. L'association en question est appelée à son tour « bijection ».*

Le théorème 1.1 pourra alors se formuler ainsi :

THÉORÈME 1.2. *Si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont le même nombre d'objets, alors elles sont en bijection entre elles.*

Imaginons maintenant qu'on ne sache pas si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont ou non le même nombre d'objets, mais que l'on sache par contre qu'elles sont entre elles en bijection. On pourra alors appliquer à ces collections la procédure du comptage alterné en passant de chaque objet de $\mathfrak{C}_\alpha$ à l'objet de $\mathfrak{C}_\beta$ qui lui est associé par la bijection. Il est alors clair qu'en comptant alternativement de cette manière, on ne pourra qu'épuiser ces collections en même temps. Cela démontre la réciproque du théorème 1.2. On aura donc le théorème suivant :

THÉORÈME 1.3. *Les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont le même nombre d'objets si et seulement si elles sont entre elles en bijection.*

REMARQUE 1.3. Avant de continuer, les lecteurs sont invités à réfléchir sur la différence entre le théorème 1.2 et le théorème 1.3. Affirmer que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi ce n'est pas la même chose que d'affirmer que si la condition $B$ est satisfaite, alors la condition $A$ l'est aussi, ou que la condition $A$ est satisfaite si et seulement si la condition $B$ l'est aussi. Il n'y a pas de doute, par exemple, que si je parle en français, alors je parle, mais rien ne m'assure que si je parle, alors je parle en français. D'autre part, si les conditions $A$ et $B$ sont telles que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi, il s'ensuit que si la condition $B$ n'est pas satisfaite, alors la condition $A$ ne peut pas l'être non plus, car si elle l'était, alors la condition $B$ devrait l'être aussi. Donc, pour que la condition $A$ soit satisfaite, il faut que la condition $B$ le soit aussi, ou bien : la condition $A$ est satisfaite seulement si la condition $B$ l'est aussi. Dire que si la

condition $A$ est satisfaite, alors la condition $B$ l'est aussi, est alors la même chose que de dire que la condition $A$ est satisfaite, seulement si la condition $B$ l'est aussi. Dire que la condition $A$ est satisfaite si la condition $B$ l'est aussi est d'autre part la même chose que de dire que si la condition $B$ est satisfaite, alors la condition $A$ l'est aussi. Ainsi dire que la condition $A$ est satisfaite si et seulement si la condition $B$ l'est aussi équivaut à dire en même temps : *i*) que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi ; et *ii*) que si la condition $B$ est satisfaite, alors la condition $A$ l'est aussi. Il sera alors facile de comprendre que pour prouver qu'une condition $A$ est satisfaite si et seulement si une autre condition $B$ l'est aussi, il faut démontrer séparément et successivement deux choses : d'une part que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi, et, d'autre part, que si la condition $B$ est satisfaite, alors la condition $A$ l'est aussi. Pour ce faire, on suppose d'abord que la condition $A$ est satisfaite et on cherche à démontrer, à partir de cette supposition, que la condition $B$ est satisfaite. Ensuite, on suppose que la condition $B$ est satisfaite et on cherche à démontrer, encore à partir de cette supposition, que la condition $A$ est satisfaite. Si les deux preuves sont établies, alors on aura justement démontré que la condition $A$ est satisfaite si et seulement si la condition $B$ l'est aussi.

Souvent en mathématiques, pour indiquer les mêmes circonstances, on utilise un langage différent de celui que je viens d'employer. Si les conditions $A$ et $B$ sont telles que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi, on dit que $A$ est une *condition suffisante* de $B$, ou que $B$ est une *condition nécessaire* de $A$. Ainsi, si les conditions $A$ et $B$ sont telles que la condition $A$ est satisfaite si et seulement si la condition $B$ l'est aussi, on dira que $A$ est une *condition nécessaire et suffisante* de $B$, ou, ce qui est évidemment la même chose d'un point de vue logique, que $B$ est une *condition nécessaire et suffisante* de $A$. Les considérations précédentes devraient suffire pour justifier aux yeux des lecteurs ces conventions terminologiques.

Finalement, il est aussi fréquent de dire, lorsque la condition $A$ est satisfaite si et seulement si la condition $B$ l'est aussi, que ces deux conditions sont *équivalentes*. Évidemment, il s'agit là d'une équivalence de nature purement logique, qui peut revêtir une asymétrie épistémologique fondamentale, car il est bien possible que, même si les conditions $A$ et $B$ sont équivalentes, elles soient telles que, lorsqu'on les considère séparément, il est bien plus facile de prouver, ou de se rendre compte, qu'une de ces conditions, disons $A$, est satisfaite, plutôt que de prouver ou de se rendre compte que l'autre l'est. Si on se trouve dans un cas comme celui-ci, et qu'on sait de surcroît prouver que les conditions $A$ et $B$ sont équivalentes, alors, on peut ajouter l'une à l'autre les deux preuves, celle qui nous assure que la condition $A$ est satisfaite et celle qui nous assure que les conditions $A$ et $B$ sont équivalentes, et produire ainsi une preuve qui nous assure que la condition $B$ est aussi satisfaite, chose qu'il aurait été par contre bien plus difficile de prouver séparément. On dira alors que la condition $A$ est un *critère* de satisfaction de la condition $B$, car pour savoir si la condition $B$ est satisfaite ou non, il suffit de s'assurer que la condition $A$ l'est ou ne l'est pas. En revanche si la condition $A$ et la condition $B$ ne sont pas équivalentes, mais sont seulement telles que si la condition $A$ est satisfaite, alors la condition $B$ l'est aussi, alors, pour s'assurer que la condition $B$ est satisfaite, il suffit de s'assurer que la condition $A$ l'est aussi, mais il ne suffit pas, évidemment, de s'assurer que la condition $A$ n'est pas satisfaite pour s'assurer que la condition $B$ ne l'est pas non plus. On n'a donc pas là un critère, mais seulement, comme on l'a dit, une condition suffisante.

Si, en considérant les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$, nous ne sommes intéressés qu'à savoir si elles sont ou non en bijection, il n'est pas nécessaire de faire attention à la nature particulière des objets qui composent ces collections. La seule chose qui importe est de savoir distinguer

leurs objets les uns des autres. Chacun de ces objets peut alors être représenté par un symbole conventionnel, par exemple un trait vertical : « | ». Il est facile de comprendre que cette opération de représentation conduit à construire, lorsqu'une collection $\mathfrak{C}$ est donnée, une autre collection $\mathfrak{C}'$ de traits verticaux, qui est en bijection avec la collection $\mathfrak{C}$ donnée. Or, comme toutes les collections qui sont en bijection entre elles ont le même nombre d'objets, il en résulte que si nous ne sommes intéressés qu'à savoir si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont ou non le même nombre d'objets, nous pouvons nous borner à considérer, non pas les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ comme telles, mais les collections de traits verticaux $\mathfrak{C}'_\alpha$ et $\mathfrak{C}'_\beta$ qui sont en bijection avec celles-ci : le fondement de cette possibilité est donné par le théorème suivant :

THÉORÈME 1.4. *Les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont le même nombre d'objets (c'est-à-dire qu'elles sont en bijection) si et seulement si elles sont en bijection avec la même collection de traits verticaux.*

Il est facile de comprendre comment un tel théorème peut être démontré. En employant un langage plus libre, on dira donc que cette même collection de traits verticaux représente, ou pourrait représenter autant la collection $\mathfrak{C}_\alpha$ que la collection $\mathfrak{C}_\beta$ (lorsqu'il ne s'agit que de compter leurs éléments). Selon qu'on veuille insister sur le fait qu'elle représente la collection $\mathfrak{C}_\alpha$, ou qu'elle est en bijection avec celle-ci, ou qu'elle représente la collection $\mathfrak{C}_\beta$, ou qu'elle est en bijection avec celle-ci, on appelle cette collection « $\mathfrak{C}'_\alpha$ » ou « $\mathfrak{C}'_\beta$ ».

Considérons maintenant des collections distinctes de traits verticaux, $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$. On peut introduire la définition suivante :

DÉFINITION 1.3. *Les collections $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ de traits verticaux sont dites « égales » entre elles (en symboles : $\mathfrak{C}' = \widetilde{\mathfrak{C}'}$) si et seulement si elles sont en bijection.*

Le théorème 1.4 pourra alors être formulé ainsi :

THÉORÈME 1.5. *Les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ ont le même nombre d'objets (c'est-à-dire qu'elles sont en bijection), si et seulement si :*

$$\mathfrak{C}'_\alpha = \mathfrak{C}'_\beta$$

Telle qu'elle vient d'être définie dans la définition 1.3, la relation d'égalité qui a lieu entre deux collections de traits verticaux est naturellement une relation d'équivalence, définie sur le domaine préalable des collections de traits verticaux. Ainsi, grâce à la définition 1.3 et au théorème 1.4, l'écriture « $\mathfrak{C}'_\alpha = \mathfrak{C}'_\beta$ » peut s'interpréter de deux manières : soit elle indique que les collections désignées par « $\mathfrak{C}'_\alpha$ » et « $\mathfrak{C}'_\beta$ » sont distinctes tout en étant en bijection ; soit elle indique que « $\mathfrak{C}'_\alpha$ » et « $\mathfrak{C}'_\beta$ » sont des noms distincts de la même collection de traits verticaux. Lorsqu'on ne considère pas comme ses objets les diverses collections distinctes de traits verticaux qu'on peut tracer sur un bout de papier, un tableau noir ou une plage, à Nantes, à Washington ou en Nouvelle-Zélande, mais plutôt les classes d'équivalence de ces collections sous la relation d'égalité (ce qui signifie qu'on décide de prendre deux collections distinctes, mais égales, de traits verticaux comme la même collection), la différence entre ces deux interprétations de l'écriture « $\mathfrak{C}'_\alpha = \mathfrak{C}'_\beta$ » devient fortuite : il n'y aura plus d'intérêt à distinguer entre le cas où les noms « $\mathfrak{C}'_\alpha$ » et « $\mathfrak{C}'_\beta$ » réfèrent à la même collection de traits verticaux et le cas où ils réfèrent à deux collections distinctes (mais égales) de traits verticaux. Cette situation est typique en mathématique et on aura souvent du mal à comprendre un raisonnement mathématique si on ne s'y conforme pas.

NOTE HISTORIQUE 1.3. En commençant un de ses articles les plus connus, *Über Sinn und Bedeutung*, publié en 1892, G. Frege s'interroge sur la nature logique de

la relation d'égalité. Le terme « égalité » apparaît dès la première ligne de cet article et il est d'entrée accompagné d'une note, où Frege précise que ce terme est utilisé pour indiquer une identité, de sorte que le contenu d'une proposition telle que « $a = b$ » pourrait aussi être exprimé en disant que $a$ est le même que $b$ ou que $a$ et $b$ coïncident. Frege veut donc distinguer d'emblée entre l'égalité entendue de cette manière, et identifiée de ce fait avec l'identité, et une relation d'équivalence quelconque qui pourrait être exprimée en utilisant le même symbole. Dans l'introduction au présent livre, j'ai déjà indiqué mes vues à propos des rapports entre identité, égalité et équivalence. Ici je vais résumer l'argument que Frege avance en faveur d'une interprétation de la relation d'identité qui me semble être parfaitement correcte et qui est en général acceptée dans les discussions philosophiques contemporaines.

Frege considère d'abord la possibilité d'interpréter la relation d'identité comme une relation entre noms (ou signes) d'objets. L'argument qui semble suggérer cette interprétation est le suivant : si on considérait la relation indiquée par la proposition « $a = b$ » comme une relation entre les objets indiqués par les symboles « $a$ » et « $b$ », il n'y aurait plus aucune manière d'expliquer la différence essentielle entre les contenus des deux propositions « $a = b$ » et « $a = a$ » ; autant la première que la deuxième de ces propositions exprimeraient en effet le même rapport entre un objet et lui-même.

Pourtant, à cet argument, purement négatif, on pourrait en opposer un autre : si on considérait la relation indiquée par la proposition « $a = b$ » comme une relation entre les symboles « $a$ » et « $b$ », et précisément comme la relation qui s'instaure entre ces deux symboles lorsqu'ils désignent le même objet, alors le rapport d'identité serait totalement arbitraire, car il est possible de prendre n'importe quel symbole comme une désignation de n'importe quel objet. Le contenu de la proposition « $a = b$ » ne concernerait alors que la manière avec laquelle nous choisissons et utilisons nos symboles et, ajoute Frege, cette proposition n'exprimerait ainsi aucune connaissance. Naturellement, l'efficacité de cet argument dépend de la disponibilité à voir, derrière une proposition, une réalité non linguistique dont cette proposition nous parlerait. En l'absence de cette disponibilité, cet argument ne serait pas valable et l'interprétation précédente de l'identité pourrait être maintenue. De mon point de vue, cette disponibilité est pourtant hors discussion et le consensus assez large qui, depuis plus d'un siècle, est accordé à l'analyse de Frege suggère qu'elle est largement admise.

Si on accepte le contre-argument précédent, on doit donc conclure que la seule manière pour assurer à la proposition « $a = b$ » un contenu de connaissance et distinguer ce contenu de celui de la proposition « $a = a$ » est de penser que, tout en désignant le même objet, les deux symboles distincts « $a$ » et « $b$ » désignent cet objet de manière différente et qu'il sont justement distincts, ou, pour être plus précis, qu'ils interviennent comme distincts dans la proposition « $a = b$ », car ils désignent cet objet de deux manières distinctes.

Cette observation est à l'origine d'une distinction que Frege introduit quelques lignes plus loin et qui est aujourd'hui un présupposé habituel des discussions philosophiques : celle entre *Sinn*, c'est-à-dire sens, ou intension, et *Bedeutung*, c'est-à-dire signification ou extension. La signification d'un terme est ce que ce terme désigne ; si ce terme est un nom d'objet, sa signification est l'objet désigné par ce terme. Le sens d'un terme est par contre la manière avec laquelle ce terme désigne ce qu'il désigne. Pour exprimer la même idée d'une façon un peu différente de celle choisie par Frege,

on pourrait dire que le sens d'un nom est le mode par lequel ce nom nous permet de parvenir à l'individuation de l'objet dont il est le nom.

Faisons un exemple. Considérons la proposition « Paris est la capitale de la France ». Selon l'analyse de Frege, cette proposition exprime le contenu suivant : la ville qui a été baptisée du nom « Paris » est la même ville que celle qui a été choisie comme capitale de la France ; ou si on veut dire les choses différemment : le nom « Paris » a été assigné à la ville qu'on pourrait aussi caractériser en disant qu'elle est la capitale de la France. On voit d'emblée que, lue de cette manière, la proposition précédente nous dit quelque chose d'essentiellement distinct des propositions « Paris est Paris » ou « La capitale de la France est la capitale de la France ».

Naturellement, pour pouvoir accepter comme légitime la distinction de Frege et l'interprétation de l'identité qu'elle comporte, il faut accepter l'idée qu'un nom désigne un objet d'une certaine manière. Dans un langage qui est le mien, plutôt que celui de Frege, cela signifie qu'un nom désigne un objet en caractérisant cet objet au moyen d'une certaine structure de concepts qui permet de l'identifier comme tel.

Une fois qu'on a compris ceci, revenons aux deux symboles « $\mathfrak{C}'_\alpha$ » et « $\mathfrak{C}'_\beta$ » dont on a parlé auparavant. Si Frege a raison et si on interprète le symbole « = » comme indiquant une identité, alors la proposition « $\mathfrak{C}'_\alpha = \mathfrak{C}'_\beta$ » pourrait s'interpréter ainsi : la collection de traits verticaux qui est en bijection avec la collection $\mathfrak{C}_\alpha$ est la même collection de traits verticaux que celle qui est en bijection avec la collection $\mathfrak{C}_\beta$ ; c'est-à-dire que les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont en bijection avec la même collection de traits verticaux. Cette interprétation de la proposition « $\mathfrak{C}'_\alpha = \mathfrak{C}'_\beta$ » n'est pourtant possible qu'une fois qu'on a accepté d'employer la relation d'équivalence 'être en bijection' définie sur les collections empiriquement (c'est-à-dire spatio-temporellement) distinctes comme la base pour une définition d'une collection de traits verticaux en tant qu'objet non empirique, conçu justement comme une classe d'équivalence de collections empiriques de traits verticaux (cf. le numéro II de la préface).

**Lectures possibles** : G. Frege, *Écrits logiques et philosophiques*, Paris, Seuil, 1971.

Arrivé à ce point, on peut définir les nombres entiers positifs comme corrélats de l'acte de compter. Qu'on considère, pour ce faire, une collection d'objets $\mathfrak{C}_\alpha$ quelconque. On appellera « nombre de $\mathfrak{C}_\alpha$ » la forme commune à $\mathfrak{C}_\alpha$ et à toute collection d'objets $\mathfrak{C}_\beta$ qui est en bijection avec $\mathfrak{C}_\alpha$. Si on appelle ce nombre « $n$ », on dira alors que la collection $\mathfrak{C}_\alpha$, ainsi que toute autre collection d'objets $\mathfrak{C}_\beta$ qui est en bijection avec $\mathfrak{C}_\alpha$, « est composée de $n$ objets » ou bien « contient $n$ objets ».

On pourra penser que cette définition est vague, car elle repose sur la notion imprécise de « forme commune ». C'est la raison pour laquelle je ne l'ai pas numérotée. À cette objection je réponds en disant que c'est justement pour la rendre moins vague que je me suis réclamé ci-dessus des collections de traits verticaux.

Remarque 1.4. Ce qui importe en mathématiques (mais aussi souvent dans la vie quotidienne), ce n'est pas de savoir ce que les nombres sont vraiment, mais plutôt comment ils sont représentés ou exprimés dans tel ou tel système opérationnel, et comment ils se comportent les uns par rapport aux autres. On peut même être plus radical : l'attitude du mathématicien revient à affirmer que la question de la nature des nombres est dénuée de sens précis, et que le seul problème consiste à définir une famille d'objets qui se comportent les uns par rapport aux autres comme nous pensons que les nombres doivent se comporter. Le mathématicien appellera alors « nombres » les éléments de cette famille d'objets et laissera

au (mauvais) philosophe le soin de se demander si ces objets sont *vraiment* des nombres ou non. Ceci fait, le mathématicien pourra dire avoir « objectivé » la notion pré-mathématique de nombre et avoir construit, à partir de cette notion, un « objet mathématique ». Naturellement, il y a beaucoup de manières d'objectiver une notion pré-mathématique et dans le présent chapitre on n'en considérera qu'une seule parmi les nombreuses manières d'objectiver la notion pré-mathématique de nombre. Une autre manière, radicalement différente, sera présentée dans le chapitre 2.

Si on accepte de se réclamer des collections de traits verticaux, alors on peut substituer à la vague définition précédente la définition suivante : on appellera « nombre de $\mathfrak{C}_\alpha$ » ($\mathfrak{C}_\alpha$ étant une collection quelconque d'objets) la forme commune à $\mathfrak{C}_\alpha$ et à toute collection d'objets $\mathfrak{C}_\beta$ qui est en bijection avec $\mathfrak{C}_\alpha$, à condition que cette forme soit représentée par la collection $\mathfrak{C}'_\alpha$ de traits verticaux qui est en bijection avec $\mathfrak{C}_\alpha$ (et par conséquent avec toute collection $\mathfrak{C}_\beta$ qui est bijection avec $\mathfrak{C}_\alpha$).

On peut supposer que cette définition est, elle-aussi, trop vague, et en effet je ne l'ai pas numérotée non plus. Pour l'éclaircir, il faudrait indiquer les propriétés des nombres des collections d'objets qui sont aussi les propriétés d'une collection de traits verticaux, c'est-à-dire qu'il faudrait éclairer les modalités selon lesquelles une collection de traits verticaux représente la forme d'une collection quelconque. Mais il est plus facile de fixer une famille d'opérations possibles sur les collections de traits verticaux et de dire que la propriété d'une collection de traits verticaux est la propriété d'un nombre si et seulement si elle résulte d'une ou de plusieurs de ces opérations. Et on pourra même aller plus vite et identifier carrément les nombres des collections d'objets avec les collections de traits verticaux. Évidemment, cette identification ne devra pas être pensée comme une réponse à la question métaphysique générale « qu'est-ce que le nombre ? » (pour peu que cette question ait un sens), mais simplement comme la détermination d'une famille d'objets qui se comportent comme les nombres devraient se comporter, pourvu qu'on ne considère que le comportement de ces objets par rapport à une certaine classe bien déterminée d'opérations. Les définitions précédentes pourraient alors être reformulées ainsi :

Définition 1.4. *On appellera « nombre de $\mathfrak{C}_\alpha$ » ($\mathfrak{C}_\alpha$ étant une collection quelconque d'objets) la collection $\mathfrak{C}'_\alpha$ de traits verticaux qui est en bijection avec $\mathfrak{C}_\alpha$ (et par conséquent avec toute collection $\mathfrak{C}_\beta$ qui est bijection avec $\mathfrak{C}_\alpha$).*

Grâce à cette définition, on sait enfin ce qu'on doit entendre par nombre d'une collection d'objets : ce n'est qu'une autre collection d'objets choisie convenablement. Il sera alors facile de dire, à partir de là, ce qu'on doit entendre par nombre entier positif :

Définition 1.5. *$n$ est un nombre entier positif si et seulement s'il est le nombre d'une collection quelconque $\mathfrak{C}_\alpha$ d'objets.*

Pour aller plus vite, on parlera dorénavant, et tout au long de ce chapitre, de « nombres » pour désigner seulement les nombres entiers positifs, dans le sens fixé par la définition 1.5. Voici alors un nombre :

$$\Big\{|, |, |, |, |, |\Big\}$$

Il ne reste qu'à préciser (s'il y en avait encore besoin) que l'identification entre nombres et collections de traits verticaux ne vaut que dans le contexte opérationnel fixé dans les paragraphes qui suivent, ce qui nous empêche de conclure, du fait que la collection de traits verticaux qu'on vient d'exhiber est imprimée en noir, que le nombre qu'on exhibe ainsi est aussi noir.

## 2. Ordre des nombres

Selon les définitions précédentes, si les collections $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ de traits verticaux sont en bijection entre elles, alors elles sont des représentations du même nombre, ou, pour être plus clairs, elles sont le même nombre. Ainsi, pour conclure que $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ sont des représentations du même nombre, ou mieux qu'elles sont le même nombre, il suffit de vérifier qu'elles sont en bijection, c'est-à-dire que $\mathfrak{C}' = \widetilde{\mathfrak{C}'}$. Plus généralement, on dira que les noms de nombres « $n$ » et « $m$ » sont des noms du même nombre lorsqu'ils indiquent soit la même collection de traits verticaux, soit des collections égales de traits verticaux. Comme on l'a déjà dit, cela revient à considérer toutes les collections de traits verticaux qui sont entre elles en bijection comme le même nombre. On n'aura donc des collections distinctes de traits verticaux qu'à condition que ces collections ne soient pas en bijection.

Soient alors $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ des collections (non vides) de traits verticaux qui ne sont pas en bijection ($\mathfrak{C}' \neq \widetilde{\mathfrak{C}'}$). En comptant alternativement ces collections, on parvient facilement à associer des objets (des traits verticaux) de l'une à des objets (encore des traits verticaux) de l'autre. Comme ces collections ne sont pas en bijection, on ne pourra pas les épuiser en même temps au moyen de cette opération. Imaginons alors qu'on parvienne d'abord à épuiser la collection $\mathfrak{C}'$. Cela signifie qu'après avoir déplacé un certain objet de la collection $\widetilde{\mathfrak{C}'}$ (en admettant que l'on ait commencé par la collection $\mathfrak{C}'$), on ne trouvera plus d'objet de $\mathfrak{C}'$ à déplacer, lorsqu'il restera encore des objets de $\widetilde{\mathfrak{C}'}$ à déplacer. L'opération de comptage alterné aura alors associé à tout objet distinct de $\mathfrak{C}'$ un et un seul objet distinct de $\widetilde{\mathfrak{C}'}$ , mais cette association ne sera pas telle que tout objet de $\widetilde{\mathfrak{C}'}$ soit par là-même associé à un et un seul objet de $\mathfrak{C}'$.

Il est alors facile de comprendre que les collections $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ satisfont à une des conditions qui permettent de dire qu'elles sont en bijection, mais qu'elles ne satisfont pas à l'autre. Elles ne sont donc pas en bijection. La condition satisfaite est pourtant remarquable et mérite une définition :

Définition 2.1. *Si les collections $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont telles que tout objet de $\mathfrak{C}_\alpha$ peut être associé à un et un seul objet de $\mathfrak{C}_\beta$ de manière qu'il n'y ait pas d'objets distincts de $\mathfrak{C}_\alpha$ qui soient associées au même objet de $\mathfrak{C}_\beta$ (sans que cela entraîne nécessairement que tout objet de $\mathfrak{C}_\beta$ soit associé à un et un seul objet de $\mathfrak{C}_\alpha$), alors on dira que $\mathfrak{C}_\alpha$ est en injection sur $\mathfrak{C}_\beta$ et que l'association en question est une injection.*

Remarque 1.5. Bien que la notion d'injection soit une des notions fondamentales des mathématiques modernes, les textes de mathématiques n'utilisent pas, à ce que je sache, l'expression « être en injection sur », et se limitent à qualifier d'injectives (ou carrément d'injections) certaines relations, associations ou fonctions. Il m'a semblé pourtant utile d'introduire ici cette expression désuète pour pouvoir disposer d'un correspondant de l'expression « être en bijection avec » que j'ai employée ci-dessus.

Le théorème suivant est alors immédiat, et il pourrait être démontré comme exercice :

Théorème 2.1. *Si $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont en bijection, alors $\mathfrak{C}_\alpha$ est en injection sur $\mathfrak{C}_\beta$ et $\mathfrak{C}_\beta$ est en injection sur $\mathfrak{C}_\alpha$ .*

Il est pourtant clair que, du fait que $\mathfrak{C}_\alpha$ est en injection sur $\mathfrak{C}_\beta$, on ne peut pas conclure que $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ sont en bijection. Le cas évoqué ci-dessus des collections $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ est justement un cas où une injection ne s'accompagne pas d'une bijection. Il est clair qu'il y a un sens à dire que, dans ce cas, $\widetilde{\mathfrak{C}'}$ contient plus d'objets (de traits verticaux) que $\mathfrak{C}'$. Cela nous permet de définir un ordre sur les nombres.

Définition 2.2. *On dira que le nombre $n$ précède le nombre $m$ (ou bien que $n$ est plus petit que $m$ ; en symboles : $n < m$), lorsque $n$ est en injection sur $m$, $n$ et $m$ n'étant pas en bijection.*

En indiquant l'association par une flèche, le diagramme

$$\begin{array}{llllllllllllllllll} \{ & | & , & | & , & | & , & | & , & | & \} & = n \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \{ & | & , & | & , & | & , & | & , & | & , & | & , & | & , & | & \} & = m \end{array}$$

indique alors que $n < m$.

Imaginons maintenant que le nombre $n$ précède le nombre $m$ et qu'il n'y ait aucun nombre $p$ tel qu'on ait à la fois $n < p$ et $p < m$. Il est facile de voir quand cette condition est vérifiée. Considérons deux collections $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$, et comptons-les alternativement ; que la collection $\mathfrak{C}'$ soit telle que, après avoir déplacé un certain objet de $\widetilde{\mathfrak{C}'}$, être revenu à $\mathfrak{C}'$ et avoir constaté qu'il n'y a plus d'objets de $\mathfrak{C}'$ à déplacer, on trouve un nouvel objet de $\widetilde{\mathfrak{C}'}$ dont le déplacement entraîne *ipso facto* l'épuisement de $\widetilde{\mathfrak{C}'}$ par l'opération de comptage alterné. Le schéma suivant illustre cette situation :

$$\begin{array}{llllllllllll} \{ & | & , & | & , & | & , & | & , & | & \} & = n \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \{ & | & , & | & , & | & , & | & , & | & , & | & \} & = m \end{array}$$

Il s'agit d'une situation remarquable qui mérite une définition :

Définition 2.3. *Si $n$ et $m$ sont des nombres et $n < m$ et qu'il n'y a pas de nombre $p$ tel que $n < p$ et $p < m$, alors on appelle $m$ « successeur de $n$ » et on le note par le symbole « $\sigma(n)$ ».*

Ainsi formulée, cette définition peut gêner, car elle repose sur un fait qu'il pourrait être difficile de vérifier : l'« inexistence » du nombre $p$ (ou même, tout simplement, parce qu'elle s'appuie sur la notion d'inexistence, qui peut apparaître ardue). Pour éviter cette objection, on peut chercher une nouvelle formulation apte à remplacer la définition 2.3. Pour cela, observons que si $\mathfrak{C}_\alpha$ est en injection sur $\mathfrak{C}_\beta$ ($\mathfrak{C}_\alpha$ n'étant pas vide), alors il y aura dans $\mathfrak{C}_\beta$ des objets qui, pris ensemble, formeront une sous-collection de $\mathfrak{C}_\beta$ (notons-la « $\overline{\mathfrak{C}_\beta \setminus \mathfrak{C}_\alpha}$ » ), qui sera en bijection avec $\mathfrak{C}_\alpha$. On peut le vérifier en comptant alternativement $\mathfrak{C}_\alpha$ et $\mathfrak{C}_\beta$ jusqu'à épuisement de $\mathfrak{C}_\alpha$, et en ne considérant que les objets de $\mathfrak{C}_\beta$ ainsi déplacés (naturellement, on devra aussi considérer l'objet de $\mathfrak{C}_\beta$ qui est déplacé tout de suite après avoir déplacé le dernier objet de $\mathfrak{C}_\alpha$ ). Le théorème suivant est alors facile à démontrer :

Théorème 2.2. *Si $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ sont des nombres tels que $\mathfrak{C}' < \widetilde{\mathfrak{C}'}$, alors $\overline{\widetilde{\mathfrak{C}'} \setminus \mathfrak{C}'} = \mathfrak{C}'$.*

Imaginons alors que $\mathfrak{C}'$ et $\widetilde{\mathfrak{C}'}$ soient des nombres tels que $\mathfrak{C}' < \widetilde{\mathfrak{C}'}$. Considérons la sous-collection $\overline{\widetilde{\mathfrak{C}'} \setminus \mathfrak{C}'}$ de $\widetilde{\mathfrak{C}'}$ définie comme ci-dessus et éliminons-la de $\widetilde{\mathfrak{C}'}$. Il en restera une collection de traits verticaux, c'est-à-dire un nombre qu'on pourra noter par le symbole « $\widetilde{\mathfrak{C}'} \setminus \mathfrak{C}'$ ». La définition qui remplacera la définition 2.3 sera alors la suivante :

Définition 2.4. *Si $n$ et $m$ sont des nombres tels que*

***(i)*** : $n < m$ ;

***(ii)*** : $n \setminus m = \{|\}$ ;

*alors on appelle $m$ « successeur de $n$ » et on le note par le symbole « $\sigma(n)$ ».*

Or, il est clair, d'après la définition 2.2, qu'aucune collection (non vide) de traits verticaux ne peut précéder la collection $\{|\}$. Étant donnée cette collection, il est en revanche facile de construire une collection de traits verticaux qui soit le nombre successeur de $\{|\}$. Ce nombre est $\{|,|\}$. En continuant, il est facile d'exhiber, dans leur ordre de succession, des nombres qui précèdent tous les autres nombres. Comme l'opération qui permet de passer d'un nombre à son successeur n'est pas seulement facile, mais peut aussi être réalisée en toutes circonstances, on ne saurait imaginer un nombre qui n'ait pas de successeur, et il suffit ainsi d'ajouter des points de suspension, indiquant une suite indéfinie, pour obtenir une représentation de tous les nombres, dans leur ordre de succession :

$$
\begin{array}{ll}
 & \{|\} \\
 & \{|,|\} = \sigma(\{|\}) \\
(1) & \{|,|,|\} = \sigma(\{|,|\}) = \sigma(\sigma\{|\})) \\
 & \{|,|,|,|\} = \sigma(\{|,|,|\}) = \sigma(\sigma(\{|,|\})) = \sigma(\sigma(\sigma(\{|\})))) \\
 & \dots
\end{array}
$$

Pourtant, on n'a là qu'une représentation, et non pas une exhibition, car ce schéma ne fait que nous suggérer les nombres qui suivent $\{|,|,|,|\}$ ; il nous pousse tout au plus à les imaginer. Et il ne servirait à rien de rajouter d'autres collections de traits verticaux avant les points de suspension : il y aura toujours des nombres qu'on ne pourra qu'imaginer. De surcroît, nous ne pouvons imaginer qu'un nombre manquant à la fois, jamais tous les nombres manquants ensemble. Nous devrons donc, après un certain temps, nous arrêter d'imaginer de nouvelles collections, et laisser la place à l'imagination (ou à la conviction) de pouvoir toujours continuer la construction.

C'est une caractéristique typique et essentielle de toute définition constructive, telle que la définition 1.5 : elle permet d'exhiber les nombres un par un seulement ; donc elle ne permet pas d'exhiber ensemble tous les nombres.

Note Historique 1.4. Jean-Michel Salanskis a attiré l'attention, dans plusieurs de ses travaux, sur la distinction entre deux modalités distinctes de définition, ou plus généralement de donation, des objets mathématiques, la modalité constructive et la corrélative. En accord avec cette distinction, on dit qu'un objet mathématique est donné constructivement s'il est défini singulièrement, grâce à une construction explicite finie et reproductible. On dit, en revanche, qu'il est donné corrélativement s'il est défini à l'aide d'un ensemble de conditions qu'il doit respecter, soit singulièrement soit en tant qu'élément d'un certain ensemble ; l'objet, ou l'ensemble auquel il appartient, n'est alors caractérisé que comme ce qui respecte ces conditions. Si, constructivement, on ne peut que définir les objets mathématiques les uns après les autres, ou, tout au plus, les reconnaître collectivement comme des objets d'une certaine nature, qu'on suppose pouvoir exhiber singulièrement, lorsque les circonstances l'exigent, la modalité corrélative permet de définir d'un seul coup une infinité d'objets, dont certains pourront ensuite être dénotés par des noms ou des symboles particuliers. La définition des nombres entiers positifs qui fait l'objet du présent chapitre est un exemple typique de définition constructive, la définition de ces mêmes nombres (qu'à l'occasion on appellera plutôt « nombres naturels » ) qui fera l'objet du prochain chapitre est en revanche un exemple typique de définition corrélative.

Un objet ne peut évidemment être donné constructivement qu'à condition qu'on dispose d'un point de départ pour la construction qui l'exhibe. Ce point de départ peut être un objet mathématique primitif, propre à la théorie à laquelle participent les objets qui seront ensuite construits à partir de ce même objet (comme c'est le cas

de la collection $\{|\}$, si on suppose qu'un nombre, défini comme une collection de traits verticaux, est construit par adjonction successive de traits verticaux à cette collection de départ) ; un tel objet primitif devra alors être supposé comme étant donné avant toute construction, grâce à une clause constructive fort particulière, qui apparaît, en dernière instance, comme assez proche d'une donation corrélative. Mais il pourrait aussi être un objet étranger à la théorie de laquelle participent les objets qui seront ensuite construits à partir de ce même objet (comme c'est le cas d'une collection quelconque d'objets, si on suppose qu'un nombre, défini comme une collection de traits verticaux, est construit en construisant la collection de traits verticaux qui est en bijection avec une collection d'objets donnés) ; l'objet primitif sera alors un objet dont on dispose préalablement, et l'acte de naissance de la théorie portant sur les objets qui seront ensuite construits sera justement la détermination de la procédure qui permet de passer des objets préalables à cette théorie aux objets mathématiques dont cette théorie va traiter.

Historiquement, la modalité corrélative de donation des objets mathématiques ne s'est imposée comme habituelle parmi les mathématiciens qu'à partir de la deuxième partie du XIX$^{\text{ème}}$ siècle. Avant cette date, les mathématiciens ne semblent caractériser corrélativement que des objets considérés comme inconnus, dont la détermination constructive constitue la solution d'un problème. Il me semble que ce changement d'attitude marque un tournant décisif dans l'histoire des mathématiques.

**Lectures possibles** : J.-M. Salanskis, « Platonisme et philosophie des mathématiques », in *L'objectivité mathématique. Platonisme et structures formelles*, M. Panza et J.-M. Salanskis éds., Masson, Paris, 1995, pp. 179-212 ; M. Panza, « Quelques distinctions à l'usage de l'historiographie des mathématiques », *in* F. Rastier, J.-M. Salanskis et R. Scheps (éds.), *Herméneutique : textes, Sciences*, P.U.F, Paris, 1997, pp. 357-388.

## 3. Quelques propriétés des nombres

Les définitions précédentes permettent de conclure que les nombres ont, entre autres, les propriétés qu'on va présenter ci-après et qui jouent, comme on le verra dans le chapitre 2, un rôle particulier dans la construction d'une axiomatique pour les nombresdits « naturels ».

On aura d'abord le théorème suivant, qu'on peut considérer comme ayant été déjà démontré :

THÉORÈME 3.1. $\{|\}$ *est un nombre.*

Si on considère aussi, parmi les différentes collections possibles, la collection vide, notée « $\emptyset$ », et qu'on l'imagine, pour ainsi dire, comme vide de traits verticaux, rien ne nous empêche d'ajouter cette collection à la succession (1). Naturellement, cette collection précédera alors la collection $\{|\}$ qui sera son successeur, de sorte qu'on aura la succession de nombres :

$$\begin{array}{l}\emptyset\\ \{|\} = \sigma(\emptyset)\\ \{|,|\} = \sigma(\sigma(\emptyset))\\ \{|,|,|\} = \sigma(\sigma(\sigma(\emptyset)))\\ \{|,|,|,|\} = \sigma(\sigma(\sigma(\sigma(\emptyset))))\\ \ldots\end{array}$$

Par extension, on pourra alors énoncer le théorème suivant :

THÉORÈME 3.2. $\emptyset$ *est un nombre.*

La définition 2.4 et l'argument qui la suit, à propos de la possibilité de construire le successeur de tout nombre, nous conduisent ensuite au théorème suivant :

THÉORÈME 3.3. *Si $n$ est un nombre, alors il a un successeur $\sigma(n)$ qui est un nombre et, quel que soit le nombre $n$, si $p = \sigma(n)$ et $q = \sigma(n)$, alors $p = q$ ; tout nombre $n$ a donc un et un seul successeur.*

Ensuite, il est clair que si on ne considère pas $\emptyset$ comme une collection, alors le nombre $\{|\}$ précédera tout autre nombre. On aura donc le théorème suivant :

THÉORÈME 3.4. *Il n'y a pas de nombre $n$ tel que : $\{|\} = \sigma(n)$*

En revanche, si on admet que $\emptyset$ est une collection, ce théorème doit être remplacé par le suivant :

THÉORÈME 3.5. *Il n'y a pas de nombre $n$ tel que : $\emptyset = \sigma(n)$.*

La définition 2.4 et celles qui la précèdent permettent ensuite de s'assurer que chaque nombre ne peut être le successeur que d'un seul nombre. On pourra alors énoncer le théorème suivant :

THÉORÈME 3.6. *Si $n$ et $m$ sont des nombres et $\sigma(n) = \sigma(m)$, alors $n = m$.*

Imaginons maintenant que $S$ soit une collection de nombres, que le nombre $\{|\}$ appartienne à $S$ et que la collection vide ne soit pas considérée comme une collection. Imaginons aussi qu'on possède une preuve — ou plus généralement un argument considéré comme correct — qui nous assure, quel que soit le nombre $n$, que si $n$ appartient à $S$, alors $\sigma(n)$ appartient aussi à $S$. Alors, comme $\{|\}$ appartient à $S$, on pourra conclure que $\{|,|\} = \sigma(\{|\})$ appartient aussi à $S$. En raisonnant de la même manière, on admettra aussi que $\{|,|,|\} = \sigma(\{|,|\}) = \sigma(\sigma(\{|\}))$ appartient à $S$. En continuant, on pourra conclure que si $n$ est un nombre, alors il appartient à $S$, c'est-à-dire que tout nombre appartient à $S$.

Ce raisonnement prouve que les nombres possèdent la propriété énoncée par le théorème suivant, dite « propriété de récurrence » :

THÉORÈME 3.7. *Si $S$ est une collection de nombres telle que :*

- **(*i*):** *$\{|\}$ appartient à $S$ ;*
- **(*ii*):** *du fait qu'un nombre quelconque $n$ appartient à $S$, il suit que le nombre $\sigma(n)$ appartient à $S$ ;*

*alors tout nombre appartient à $S$.*

Si en revanche, on considère $\emptyset$ comme une collection, des prémisses (*i*) et (*ii*) on pourra conclure seulement que tout nombre $m$ tel que $\emptyset < m$ appartient à $S$, c'est-à-dire que tout nombre appartient à $S$, à l'exclusion éventuelle de $\emptyset$. Pour savoir si $\emptyset$ appartient à $S$, il faut un argument supplémentaire. Imaginons que l'on possède cet argument (et donc qu'on sait que $\emptyset$ appartient à $S$). Du coup on n'a pas besoin d'un autre argument pour s'assurer que $\{|\}$ appartient à $S$, car la prémisse (*ii*) permet de s'en assurer par le seul fait que $\emptyset$ appartient à $S$. Ainsi, à la place du théorème 3.7, on aura le théorème suivant :

THÉORÈME 3.8. *Si $S$ est une collection de nombres telles que :*

- **(*i*):** *$\emptyset$ appartient à $S$ ;*
- **(*ii*):** *du fait qu'un nombre quelconque $n$ appartient à $S$, il suit que le nombre $\sigma(n)$ appartient à $S$ ;*

*alors tout nombre appartient à $S$.*

NOTE HISTORIQUE 1.5. Dans un article très célèbre, paru dans le deuxième volume (1894) de la *Revue de métaphysique et de morale*, sous le titre « Sur la nature du raisonnement mathématique », Henri Poincaré se proposait de résoudre ce qui lui apparaît comme un paradoxe : si les mathématiques ne procèdent pas par déduction, alors elles ne peuvent pas être rigoureuses ; par contre si elles procèdent par déduction, alors elles ne peuvent consister en rien d'autre que dans une formulation, sous les formes les plus diverses, du contenu de leurs axiomes (qui constituent le point de départ de la déduction). Si on suppose que les mathématiques avancent par déduction et si on pense que leurs axiomes expriment des vérités empiriques, il s'ensuit que les mathématiques ne font que redire ces vérités ; en revanche, si on pense que les axiomes des mathématiques se réduisent, en dernière instance, au principe de non-contradiction, il s'ensuit que les mathématiques se réduisent, elles-aussi, dans leur totalité, à ce principe. Pour sortir des difficultés, nous dit Poincaré, il faut donc, ou bien reconnaître dans les axiomes autre chose que l'affirmation de vérités empiriques ou l'expression du principe de non-contradiction, ou bien reconnaître dans le raisonnement mathématique « une sorte de vertu créatrice » qui le « distingue du syllogisme ». On sait que, pour ce qui est de la géométrie, Poincaré pensait que le paradoxe pouvait être résolu de la première manière (c'est la thèse du conventionnalisme géométrique de Poincaré, sur laquelle on a tant écrit). Dans l'article dont il est question, il argumente en revanche en faveur de la deuxième possibilité, pour ce qui est de l'arithmétique. Cette dernière se fonderait en fait sur un mode de raisonnement qui, d'après Poincaré, est « irréductible » aux règles de la déduction. Ce mode de raisonnement serait justement celui qui nous a conduits aux deux derniers théorèmes énoncés ci-dessus : on prouve que le nombre 0 possède une certaine propriété ; on prouve ensuite que lorsqu'un nombre quelconque possède cette propriété, alors son successeur la possède aussi ; on en conclut que tous les nombres possèdent cette propriété. Cet argument se fonde sur un principe, dit « de récurrence ». D'après Poincaré, le caractère essentiel de cet argument est qu'il contient, condensée dans une seule formule, une infinité de syllogismes, qu'on ne pourra donc jamais vérifier un par un. Ce principe est donc un véritable jugement synthétique *a priori*. Bien que, comme on le verra dans le prochain chapitre, on puisse fixer ce principe par le biais d'un axiome, il intervient au cours de l'argumentation mathématique comme un principe d'inférence, qui n'est donc pas, d'après Poincaré, strictement déductif. Voici une citation qui illustre fort bien le point de vue de ce dernier : « Pourquoi [...] ce jugement s'impose-t-il à nous avec une irrésistible évidence ? C'est qu'il n'est que l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible. L'esprit a de cette puissance une intuition directe et l'expérience ne peut être pour lui qu'une occasion de s'en servir et par là d'en prendre conscience ». On se rendra compte dans la suite du rôle absolument central du principe de récurrence dans l'édification de l'arithmétique.

**Lectures possibles** : H. Poincaré, *La science et l'hypothèse*, Flammarion, Paris, 1902 (nombreuses rééditions successives).

* * *

Né à Nancy, le 29 avril 1854 et mort à Paris, le 17 juillet 1912, Henri Poincaré fut un mathématicien total : ses contributions fondamentales concernent à peu près tous les domaines de recherche en mathématiques et en physique mathématique : de la théorie des fonctions réelles et complexes, à la mécanique céleste, en passant, entre

autres, par la théorie des nombres, la topologie algébrique, l'algèbre et la théorie des groupes, les géométries non euclidiennes, la géométrie différentielle et algébrique, la théorie des équations différentielles et aux dérivées partielles, la théorie de la lumière, celle de la propagation électromagnétique, et celle de la stabilité de l'univers. Il fut capable de surcroît de saisir des liens profonds entre théories mathématiques différentes ; le cas de l'emploi des fonctions fuchsiennes (une sorte particulière de fonctions à variable complexe) pour fournir un fondement aux géométries non euclidiennes est souvent cité comme paradigmatique.

Provenant d'une famille appartenant à la bourgeoisie lorraine, cousin de Raymond Poincaré, qui fut président de la République Française pendant la première guerre mondiale, Henri Poincaré fut un élève de l'École Polytechnique, puis de l'École des Mines ; professeur aux universités de Caen et de Paris, il entra à trente-trois ans à l'Académie des Sciences et fut élu plus tard à l'Académie Française. Parmi ses innombrables intérêts intellectuels, il réserva une place non négligeable à la philosophie des mathématiques et en particulier aux réflexions sur la nature de l'espace et sur les processus cognitifs qui nous amènent à la construction d'une géométrie à partir des données sensibles.

**Lectures possibles** : A.-F. Schmid, *Une philosophie de savant. Henri Poincaré et la logique mathématique*, Maspero, Paris, 1978 ; T. Dantzig, *Henri Poincaré Critic of Crisis*, Greenwood Press Pub., New York, 1954.

### 4. Opérer sur les nombres : l'addition et la multiplication

Ayant défini les nombres comme des collections de traits verticaux, il sera facile de définir l'opération fondamentale qui porte sur eux et qu'il est d'usage d'appeler « addition ».

REMARQUE 1.6. Ici on entend par « opération sur $\mathfrak{D}$ » ($\mathfrak{D}$ étant un certain domaine d'objets) une association qui associe à certains couples d'objets de $\mathfrak{D}$, éventuellement à tout couple d'objets de $\mathfrak{D}$, un objet du même domaine $\mathfrak{D}$. À proprement parler, celle-ci est une « opération binaire » (car elle porte sur un couple d'objets de $\mathfrak{D}$) mais, comme on ne traitera dans la suite que d'opérations binaires, on peut l'appeler « opération » tout-court.

Voici la définition de l'addition :

DÉFINITION 4.1. *On appelle « addition » (sur les nombres ci-avant définis comme collections de traits verticaux) l'opération qui associe aux collections de traits verticaux $n$ et $m$ (quelles que soient ces collections) la collection de traits verticaux contenus dans ces collections. Si $n$ et $m$ sont donc des nombres, on note leur addition par le symbole « $n + m$ ».*

À cette définition il faut en ajouter une autre :

DÉFINITION 4.2. *Si $n$ et $m$ sont des nombres, on appelle « somme de $n$ et $m$ » la collection de traits verticaux contenus dans ces collections, ce qu'on pourrait aussi qualifiar de résultat de l'addition $n + m$.*

REMARQUE 1.7. Bien que les concepts d'addition de deux nombres et de somme de ces nombres soient distincts entre eux, ainsi que les concepts plus généraux de l'opération $*$ appliquée à un couple d'objets $x$ et $y$ d'un certain domaine $\mathfrak{D}$ d'objets, et de l'objet de $\mathfrak{D}$, associé à de couple d'objets de $\mathfrak{D}$, ou résultat de cette opération, les mathématiciens sont habitués à noter les objets correspondants à ces concepts de la même manière, en employant le symbole « $x * y$ » dans un cas comme dans l'autre. Le lecteur n'aura pas de difficultés, par la suite, à distinguer les différents usages de ce symbole.

De la définition 4.1, il est clair que l'addition est une opération sur les nombres qui associe un nombre à tout couple de nombres. Il sera alors naturel de chercher un critère pour savoir si un nombre $p$ est ou non la somme de deux nombres quelconques donnés, $n$ et $m$. Compte-tenu des remarques faites au début du paragraphe 2, ce critère peut être donné sous forme d'un théorème déduit des définitions 4.1 et 4.2 :

THÉORÈME 4.1. *Si $n$, $m$ et $p$ sont des nombres, alors*

$$n + m = p$$

*si et seulement si $p$ est en bijection avec la collection des traits verticaux contenus dans les collections $n$ et $m$.*

Parmi les illustrations de ce théorème, il y a par exemple la suivante :

$$\{|,|,|\} + \{|,|\} = \{|,|,|,|,|\}$$

car

$$\begin{array}{ccc} \{|,|,|\} & ; & \{|,|\} \\ \downarrow\downarrow\downarrow & & \downarrow\downarrow \\ \{|,|,| & , & |,|\} \end{array}$$

Le théorème suivant est aussi facile à démontrer :

THÉORÈME 4.2. *Si $n$, $m$ et $p$ sont des nombres, alors :*

***(i)*:** *$n + m = p$ si et seulement si $p \setminus n = m$ ;*

***(ii)*:** *$n + m = p$ si et seulement si $p \setminus m = n$.*

REMARQUE 1.8. Ce théorème pourrait suggérer des définitions de l'addition et de la somme, différentes de celles données dans les définitions 4.1 et 4.2, et qui se réclameraient de l'opération sur les collections d'objets qu'on a notée « $\setminus$ ». Ces définitions auraient pourtant un défaut majeur : elles permettraient bien sûr de savoir si $p$ est ou non la somme de $n$ et $m$, mais ne permettraient pas de calculer directement $p$ à partir de $n$ et $m$. C'est la raison pour laquelle on ne les adoptera pas.

Une conséquence remarquable du théorème 4.1, dont la preuve serait également facile à obtenir, est la suivante :

THÉORÈME 4.3. *Si $n$ est un nombre, alors :*

$$n + \{|\} = \sigma(n) \qquad \text{et} \qquad n + \emptyset = n$$

Et de là, il suit :

THÉORÈME 4.4. *Si $n$ et $m$ sont des nombres, alors :*

$$m = \sigma(n) \text{ si et seulement si } n + \{|\} = m$$

Il sera aussi facile de prouver le théorème suivant :

THÉORÈME 4.5. *Si $n$, $m$ et $p$ sont des nombres et $n$ et $m$ ne sont pas $\emptyset$, alors :*

*si $n + m = p$, alors* $\begin{cases} n < p \\ m < p \end{cases}$

De la définition 4.1, il suit de surcroît que l'addition sur les nombres possède deux propriétés remarquables : la commutativité et l'associativité. C'est ce que nous disent les deux théorèmes suivants :

THÉORÈME 4.6. **[Commutativité de l'addition]** *Si $n$ et $m$ sont des nombres, alors :*

$$n + m = m + n$$

THÉORÈME 4.7. **[Associativité de l'addition]** *Si $n$, $m$ et $p$ sont des nombres, alors :*

$$n + (m + p) = (n + m) + p$$

REMARQUE 1.9. L'énoncé de ce dernier théorème fait un usage des parenthèses qui, bien qu'il soit courant et facile à comprendre et à justifier, n'a pas encore été précisé ici. Si le symbole « $*$ » indique une opération portant sur des couples d'objets d'un domaine $\mathfrak{D}$, et si $x$, $y$ et $z$ sont des objets convenables de ce domaine, alors les symboles « $z * (x * y)$ » et « $(z * x) * y$ » intervenant dans l'énoncé de ce théorème dénotent respectivement : le résultat de l'opération $*$ appliquée au couple formé par l'objet $z$ et par le résultat de l'opération $*$ appliquée aux objets $x$ et $y$ ; et le résultat de l'opération $*$ appliquée au couple formé par le résultat de l'opération $*$ appliquée aux objets $z$ et $x$ et par l'objet $y$. Il est alors clair que l'associativité d'une opération $*$ est une condition nécessaire et suffisante pour que la réitération de l'application de cette opération ne comporte aucune ambiguïté quant au résultat obtenu, c'est-à-dire que l'écriture « $x * y * z * ...$ », où $x$, $y$ , $z$, ... sont des objets convenables d'un domaine $\mathfrak{D}$, dénote un et un seul objet de ce même domaine. Ceci explique le rôle central que la propriété d'associativité d'une opération prendra au cours des paragraphes et des chapitres qui suivent.

Bien que les théorèmes 4.6 et 4.7 soient très faciles à prouver, je vais en exposer ici des démonstrations possibles (le lecteur pourra facilement en trouver d'autres par lui-même).

**Preuve du théorème 4.6** Selon le théorème 4.2, pour démontrer ce théorème, il suffit de vérifier que

$$(m + n) \setminus n = m$$

Or, $(m + n) \setminus n$ n'est rien d'autre que le résultat de l'addition des collections $m$ et $n$, puis de l'élimination de la collection $\overline{(m + n) \setminus n}$. Mais, si $m$ n'est pas $\emptyset$, du théorème 4.5, il suit que $n$ est plus petit que $m + n$, et donc, selon le théorème 2.2, $\overline{(m + n) \setminus n} = n$ et donc $(m + n) \setminus n$ est le résultat de l'élimination de $n$ de la somme de $m$ et $n$, ce qui nous ramène au nombre $m$, et le théorème est donc prouvé. En revanche, si $n$ est $\emptyset$, alors, $(m + n) \setminus n = m + n = m$, et le théorème est également prouvé. □

**Preuve du théorème 4.7** La preuve est analogue, car il est facile de vérifier que

$$[(n + m) + p] \setminus n = m + p$$

ce qui conclut la preuve. □

Bien qu'on ait choisi de considérer toutes les collections de traits verticaux qui sont en bijection comme la même collection, et que donc on ne peut pas avoir de nombres à la fois distincts et égaux (ce qui signifie que l'écriture « $n + m = p$ » doit être comprise comme signifiant que « $n + m$ » et « $p$ » sont des noms distincts du même nombre), rien n'empêche de considérer le même nombre plusieurs fois et de l'additionner à lui-même autant de fois que l'on veut. On a alors une addition d'un type particulier qu'on appelle « multiplication ». Voici sa définition :

DÉFINITION 4.3. *On appelle « multiplication » (sur les nombres définis comme ci-avant) l'opération qui associe à des collections de traits verticaux $n$ et $m$ la collection des traits verticaux contenus dans les collections de traits verticaux qui appartiennent à la collection de collections de traits verticaux dont les éléments sont des collections de traits verticaux, toutes égales à $n$ (c'est-à-dire des répétitions de la collection $n$), et qui est en bijection avec $m$. Si $n$ et $m$ sont des nombres, on note leur multiplication par le symbole « $n \cdot m$ ».*

Remarque 1.10. Pour bien comprendre cette définition, on doit observer qu'une collection de traits verticaux est un objet comme un autre. Une collection $\mathfrak{C}$ de collections de traits verticaux est donc une collection d'objets et elle peut bien être en bijection avec une collection $\mathfrak{C}'$ de traits verticaux, chaque collection de traits verticaux de la collection $\mathfrak{C}$ étant de cette manière associée à un et un seul trait vertical de la collection $\mathfrak{C}'$, de sorte que tout trait vertical de $\mathfrak{C}'$ soit de cette manière associé à une et une seule collection de traits verticaux appartenant à $\mathfrak{C}$. En parlant un langage un peu plus technique, ceci revient à dire que les collections d'objets, et en particulier les collections de traits verticaux et les collections de collections de traits verticaux, doivent être traitées comme des ensembles et non pas comme n'importe quels agrégats d'objets. Pour caractériser un agrégat d'objets, il peut suffire d'en fixer les limites, sans préjuger au préalable de la nature de ses éléments, ceux-ci peuvant varier selon notre capacité d'analyse et nos modalités de classifications. Les éléments d'une bibliothèque pouvant être, par exemple, soit les volumes qui y sont conservés, soit les tomes qui composent ces volumes, ou les pages de ces tomes. Pour définir un ensemble, il faut, en revanche : ou bien fixer la nature de ses éléments, déterminer *a priori* la condition à laquelle un objet doit satisfaire pour pouvoir être considéré comme un élément de cet ensemble ; ou bien indiquer de manière explicite ces éléments. Ainsi, une bibliothèque n'est un ensemble que lorsque l'on a déterminé si elle est composée par des volumes, des tomes ou des pages. Dans notre cas, si les éléments d'une collection de traits verticaux sont bien des traits verticaux, les éléments d'une collection de collections de traits verticaux ne peuvent guère être des traits verticaux ; ils sont forcément, et de manière univoque, des collections de traits verticaux, de sorte qu'aucun trait vertical n'appartient à cette collection. Dit d'une autre manière, la collection $\{|,|,|,|,|\}$ est essentiellement distincte de la collection $\{\{|,|\},\{|,|,|\}\}$, et ces deux collections ne sont même pas en bijection, bien que la collection des traits verticaux contenus dans les collections qui appartiennent à la deuxième de ces collections soit en bijection avec la première, et soit de ce fait la même collection.

Note Historique 1.6. Bien que la notion d'ensemble puisse apparaître comme parfaitement simple, et que de nombreux philosophes des mathématiques, en commençant par Frege et Russell, aient soutenu que la réduction de toutes les mathématiques à la théorie des ensembles corresponde à une fondation des mathématiques sur des principes « purement logiques », l'histoire nous enseigne que l'état actuel de la théorie des ensembles est le résultat d'acquisitions difficiles qui ne concernent pas seulement les aspects les plus sophistiqués de cette théorie, portant sur des ensembles infinis, mais aussi ses fondements les plus élémentaires.

Lorsque, vers la fin du XIX$^{\text{ème}}$ siècle, Frege et Cantor commencèrent, entre autres, à parler d'ensembles, ils le firent d'abord dans des contextes bien distincts. Pour Cantor, la notion d'ensemble émergeait d'un effort de généralisation visant la compréhension de certains phénomènes propres à une branche de l'analyse. En effet, Cantor n'avait d'abord d'autres buts que de résoudre des problèmes connus et difficiles à propos des séries de Fourier (des sommes infinies, dont les termes sont des fonctions trigonométriques d'arcs multiples ; les notions de fonction et de série seront éclairées par la suite, quant aux notions de fonction trigonométrique et d'arcs multiples, le lecteur pourra se rapporter à n'importe quel manuel d'analyse), des problèmes qu'il commença à formuler en parlant justement de certains ensembles de points ou de nombres. Bientôt, Cantor comprit que ses ensembles de points ou de nombres pouvaient être pensés comme des exemplifications particulières d'une notion plus générale, et se rendit compte des avantages dérivant d'une étude de cette notion générale, prise en tant que telle. Ses réflexions le portèrent ainsi d'emblée à étudier

des ensembles infinis, à considérer ces ensembles du point de vue de leur cardinalité (cf. les chapitres 4 et 6), et à les regarder comme des domaines d'objets sur lesquels on avait défini, ou on pouvait définir, des relations, des fonctions ou des opérations (cf. le chapitre 2). Pour Frege, la notion d'ensemble participait en revanche d'un effort d'éclaircissement de la nature logique et du fonctionnement du langage. Bien que la visée de Frege, fût en dernière instance de fournir un fondement ultime pour les mathématiques, son approche n'était pas celle d'un mathématicien engagé, comme Cantor, dans des recherches de pointe, mais celle d'un observateur en quelque sorte extérieur, qui cherchait à comprendre les mécanismes logiques et/ou linguistiques qui opèrent à l'intérieur des théories mathématiques élémentaires.

Autant Cantor que Frege comprirent rapidement la différence entre un ensemble et un simple agrégat d'objets, c'est-à-dire qu'ils comprirent qu'un ensemble n'est déterminé comme tel que lorsqu'on a caractérisé de manière précise ses éléments. Il ressort qu'un certain ensemble peut être défini en donnant la liste complète de ces éléments, mais il peut aussi être défini en fixant une propriété, disons $P$, et en supposant qu'un objet est un élément de cet ensemble si et seulement s'il jouit de cette propriété. On aura alors l'ensemble de tous les $x$ tels que $P(x)$. De cette manière on ne décide pas *a priori* quels sont les éléments de l'ensemble en question, mais on fournit un critère univoque pour établir, pour chaque objet donné, s'il est ou pas un élément de cet ensemble.

Cela ne revient pas à dire, pourtant, que, quelle que soit la propriété $P$, on peut définir l'ensemble de tous les objets qui jouissent de cette même propriété. C'était la conviction de Frege, qui l'avait traduite dans un axiome célèbre (généralement dit « axiome de compréhension » ) affirmant que, pour toute propriété $P$, il existe l'ensemble de tous les objets qui jouissent de $P$. Si on accepte cet axiome, il n'est pourtant pas difficile d'en dériver des paradoxes. Le plus célèbre fut communiqué à Frege par Russell, dans une lettre datée du 16 juin 1902. Pour l'obtenir, il suffit de considérer la propriété 'ne pas appartenir à soi-même' et d'étudier les propriétés de l'ensemble présumé de tous les ensembles qui n'appartiennent pas à eux-mêmes. Si cet ensemble présumé appartenait à lui-même, alors il n'appartiendrait pas à lui-même, et s'il n'appartenait pas à lui-même, alors il appartiendrait à lui-même. Donc, un tel ensemble devrait en même temps appartenir et ne pas appartenir à lui-même.

On dit souvent que la cause de ce paradoxe réside dans l'autoréférencialité de la propriété 'ne pas appartenir à soi-même'. Ceci était aussi la conviction de Russell qui élabora une théorie assez complexe (la théorie des types) pour indiquer les conditions auxquelles l'application de l'axiome de compréhension ne portait pas à des paradoxes. On peut pourtant penser, à mon avis bien plus correctement, que la cause du paradoxe de Russell est en même temps plus profonde et plus simple : c'est que la notion d'ensemble ne peut pas être identifiée en général avec l'idée informelle de collection d'objets qui jouissent d'une certaine propriété. La manière la plus simple d'éviter tout paradoxe, et de fournir en même temps une base convenable pour la théorie des ensembles, est alors de caractériser en général la notion d'ensemble, grâce à un système d'axiomes qui fixent le contexte opérationnel de cette théorie. Ceci fut l'objet, dans les années 1920, de nombreuses recherches qui aboutirent à la détermination de l'axiomatique dite « de Zermelo-Fraenkel », qui est aujourd'hui généralement acceptée comme le contexte minimal à l'intérieur duquel il est possible de parler d'ensembles de manière correcte et précise.

**Lectures possibles** : C. Mangione et S. Bozzi, *Storia della logica : da Boole ai nostri giorni*, Garzanti, Milano, 1993.

* * *

Né le 19 février 1845 à St. Petesbourg, G. Cantor (sur lequel cf. aussi la note historique 6.16) vécut son adolescence à Francfort et étudia les mathématiques, la physique et la philosophie à l'université de Berlin, où il fut l'élève de Weierstrass, Kummer et Kronecker. Ce fut justement Weierstrass qui suggéra au jeune Cantor de se consacrer au problème de la représentativité des fonctions par des séries trigonométriques, problème qui le conduira plus tard à la création de la théorie des ensembles. À partir de 1872, il fut professeur à l'université de Halle, où il resta jusqu'à sa mort, survenue en 1918. Ses efforts pour rentrer à Berlin furent toujours contrés par son ancien maître Kronecker, duquel il fut séparé par une longue et célèbre dispute.

**Lectures possibles** : W. Purkert und H. J. Ilgauds, *Georg Cantor,* 1845-1918, Birkhaüser Verlag, Basel, Boston, Stuttgart, 1987 ; A. Kertész, *Georg Cantor,* 1845-1918*, Schöpfer der Mengenlehre*, numéro 15 (1983) de *Acta Historica Leopoldina.*

Comme dans le cas de l'addition, à la définition 4.3, il faut en adjoindre une autre :

Définition 4.4. *Si $n$ et $m$ sont des nombres, on appelle « produit de $n$ et $m$ » la collection des traits verticaux contenus dans les collections de traits verticaux qui appartiennent à la collection de collections de traits verticaux dont les éléments sont des collections de traits verticaux, toutes égales à $n$, et qui est en bijection avec $m$, ce qu'on pourrait aussi qualifiar de résultat de la multiplication $n \cdot m$.*

De la définition 4.3, apparaît clairemment que la multiplication est une opération sur les nombres qui associe un nombre à tout couple de nombres. Suivant cette définition, l'exécution d'une multiplication entre des nombres donnés, $n$ et $m$, demande une étape intermédiaire. Si les collections de traits verticaux $n$ et $m$ sont données : d'abord, on construit la collection $\{n, n, ..., n\}$ qui est en bijection avec la collection $m$ ; ensuite on additionne les éléments de cette collection ; le produit de la multiplication $n \cdot m$ est justement le résultat de cette addition. Ainsi le critère pour savoir si un nombre $p$ est ou non le produit des nombres donnés $n$ et $m$ est celui qui est énoncé par le théorème suivant :

Théorème 4.8. *Si $n$, $m$ et $p$ sont des nombres, alors*

$$n \cdot m = p$$

*si et seulement si $p$ est est en bijection avec la collection de traits verticaux contenus dans les différents éléments d'une collection de collections des traits verticaux toutes égales à $n$, qui soit en bijection avec $m$.*

Il est clair que ce théorème, ainsi que la définition 4.3, ne sont intelligibles que parce qu'on vient de prouver que l'addition sur les nombres est associative, ce qui, comme on l'a déjà remarqué, permet de comprendre, sans aucune ambiguïté, et à partir de la seule définition 4.1, ce qui est la somme d'autant de nombres $n, m, p, q, ...$ qu'on veut :

$$n + m + p = (n + m) + p = n + (m + p)$$
$$n + m + p + q = (n + m + p) + q = n + (m + p + q)$$
*etc.*

Ce point éclairé, il est ensuite aisé de déduire du théorème 4.8 une foule de théorèmes portant sur des nombres particuliers. Un de ces théorèmes est par exemple illustré par le diagramme suivant :

$$\{|,|,|\} \cdot \{ \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \}$$

$$= \{ \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \} + \{ \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \} + \{ \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \} + \{ \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \begin{array}{c}|\\ \downarrow\end{array} \}$$

$$= \{ \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \} + \{ \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \} + \{ \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \} + \{ \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \}$$

$$= \{ \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \begin{array}{c}|\\ |\end{array} \}$$

ou bien

$$\{|,|,|\} \cdot \{|,|,|,|\} = \left\{ \begin{array}{l} |,|,|, \\ |,|,|, \\ |,|,|, \\ |,|,| \end{array} \right\}$$

Pour passer à des théorèmes généraux, on voit d'abord que de la définition 4.4, suivent les théorèmes suivants, que le lecteur pourra démontrer aisément :

THÉORÈME 4.9. *Si $n$ est un nombre, alors :*

$$n \cdot \{|\} = n \qquad et \qquad n \cdot \emptyset = \emptyset$$

*et, si $m$ est également un nombre et $n$ n'est pas $\emptyset$, alors :*

$$n \cdot m = n \text{ si et seulement si } m = \{|\}$$

THÉORÈME 4.10. *Si $n$, $m$ et $p$ sont des nombres, et $n$ et $m$ ne sont pas $\emptyset$, alors :*

$$\text{si } n \cdot m = p, \text{ alors } \left\{ \begin{array}{l} n < p \text{ ou } n = p \text{ (lorsque } m = \{|\}\text{)} \\ m < p \text{ ou } m = p \text{ (lorsque } n = \{|\}\text{)} \end{array} \right.$$

Comme l'addition, la multiplication sur les nombres est commutative et associative. Il est en fait facile de démontrer les théorèmes suivants :

THÉORÈME 4.11. [**Commutativité de la multiplication**] *Si $n$ et $m$ sont des nombres, alors :*

$$n \cdot m = m \cdot n$$

THÉORÈME 4.12. [**Associativité de la multiplication**] *Si $n$ et $m$ sont des nombres, alors :*

$$n \cdot (m \cdot p) = (n \cdot m) \cdot p$$

Voici des preuves possibles de ces théorèmes.

**Preuve du théorème 4.11** Si $n$ et $m$ sont des nombres, alors ils sont des collections de traits verticaux, disons, respectivement, les suivantes :

$$\{|\,,|\,,|\,,\ldots|\} \text{ et } \{|\,,|\,,\ldots|\}$$

En vertu de la définition de la multiplication, on aura alors

$$n \cdot m = \left\{ \begin{array}{l} |\,,|\,,|\,,\cdots|, \\ |\,,|\,,|\,,\cdots|, \\ \vdots \\ |\,,|\,,|\,,\cdots| \end{array} \right\}$$

$$m \cdot n = \left\{ \begin{array}{l} |\,,|\,,\cdots|, \\ |\,,|\,,\cdots|, \\ |\,,|\,,\cdots|, \\ \vdots \\ |\,,|\,,\cdots| \end{array} \right\}$$

Considérons ces collections. Il est facile de vérifier que, en accord avec la définition 4.3, chaque ligne de la collection $n \cdot m$ est en bijection avec chaque colonne de la collection $m \cdot n$, tandis que chaque colonne de la collection $n \cdot m$ est en bijection avec chaque ligne de la collection $m \cdot n$. Les deux collections sont donc en bijection. □

**Preuve du théorème 4.12** Conformément au théorème précédent, on aura

$$\begin{aligned} n \cdot (m \cdot p) &= (m \cdot p) \cdot n \\ (n \cdot m) \cdot p &= (m \cdot n) \cdot p \end{aligned}$$

donc, si

$$\begin{aligned} n &= \{|\ ,\ \dots\ |\} \\ m &= \{|\ ,|\ ,\ \dots\ |\} \\ p &= \{|\ ,|\ ,|\ ,\ \dots\ |\} \end{aligned}$$

de la définition de la multiplication il suivra :

$$n \cdot (m \cdot p) = (m \cdot p) \cdot n = \left\{ \begin{array}{cccc} |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, \\ |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, \\ |\ ,|\ ,\ \dots\ |, & ,...,\ & |\ ,|\ ,\ \dots\ |, \\ \vdots & & \vdots \\ |\ ,|\ ,\ \dots\ | & & |\ ,|\ ,\ \dots\ | \end{array} \right\}$$

$$(n \cdot m) \cdot p = (m \cdot n) \cdot p = \left\{ \begin{array}{cccccc} |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, \\ \vdots & , & \vdots & , & \vdots & ,...,\ & \vdots \\ |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, & & |\ ,|\ ,\ \dots\ |, \end{array} \right\}$$

On peut alors raisonner sur ces collections comme précédemment, en considérant les lignes et les colonnes qui ont la collection $m$ comme élément. Il est facile de voir que ce raisonnement vérifie le théorème et clôture la preuve. □

Prises ensemble, l'addition et la multiplication bénéficient d'une autre propriété remarquable : la distributivité de la multiplication sur l » addition. C'est le contenu du théorème suivant :

THÉORÈME 4.13. [**Distributivité de la multiplication sur l'addition**] *Si $n$, $m$ et $p$ sont des nombres, alors :*

$$n \cdot (m + p) = (n \cdot m) + (n \cdot p)$$

**Preuve** Si $n$, $m$ et $p$ sont comme dans la preuve précédente, alors

$$n \cdot (m + p) = (m + p) \cdot n = \left\{ \begin{array}{c} |\ ,|\ ,\ \dots\ |\ ;|\ ,|\ ,|\ ,\ \dots\ |\ , \\ \vdots \\ |\ ,|\ ,\ \dots\ |\ ;|\ ,|\ ,|\ ,\ \dots\ | \end{array} \right\}$$

et

$$(n \cdot m) + (n \cdot p) = \left\{ \begin{array}{c} |\ ,\ \dots\ |\ , \\ |\ ,\ \dots\ |\ , \\ \vdots \\ |\ ,\ \dots\ | \end{array} \right\} + \left\{ \begin{array}{c} |\ ,\ \dots\ |\ , \\ |\ ,\ \dots\ |\ , \\ |\ ,\ \dots\ |\ , \\ \vdots \\ |\ ,\ \dots\ | \end{array} \right\}$$

et le théorème découle donc immédiatement de la définition de l'addition, en observant que

$$\left\{\begin{array}{l} |\,,\ldots|\,, \\ |\,,\ldots|\,, \\ \vdots \\ |\,,\ldots| \end{array}\right\} = \left\{\begin{array}{l} |\,,|\,,\ldots| \\ \vdots \\ |\,,|\,,\ldots| \end{array}\right\}$$

et

$$\left\{\begin{array}{l} |\,,\ldots|\,, \\ |\,,\ldots|\,, \\ |\,,\ldots|\,, \\ \vdots \\ |\,,\ldots| \end{array}\right\} = \left\{\begin{array}{l} |\,,|\,,|\,,\ldots|\,, \\ \vdots \\ |\,,|\,,|\,,\ldots| \end{array}\right\}$$

à cause de la bijection entre lignes et colonnes. □

REMARQUE 1.11. Bien qu'on puisse résumer le contenu des théorèmes 4.6, 4.7, 4.11, 4.12 et 4.13 en disant que l'addition et la multiplication sur les nombres sont des opérations commutatives et associatives, et que la première est distributivesur la deuxième, il est important de rendre explicite ce que j'ai déjà implicitement dit dans la remarque qui a suivi le théorème 4.7 : ces propriétés de l'addition et de la multiplication sur les nombres dépendent de l'identification de certaines sommes et produits plutôt que de l'identification de certaines applications de l'addition ou de la multiplication. Si nous utilisons les termes « addition de $x$ et $y$ » et « multiplication de $x$ et $y$ » pour nous référer à des applications particulières des opérations définies dans les définitions 4.1 et 4.3, alors nous pouvons nous exprimer ainsi : en disant que la multiplication sur les nombres est commutative, nous ne disons nullement — pour ne faire qu'un seul exemple — que la multiplication de n'importe quels nombres $n$ et $m$ s'identifie à la multiplication des nombres $m$ et $n$, tout ce que nous disons est que ces multiplications (qui restent, quant à elles, distinctes, car multiplier le nombre $n$ au nombre $m$ n'est nullement la même chose que de multiplier le nombre $m$ au nombre $n$) donnent le même résultat.

## 5. Opérations inverses : la soustraction et la division

Considérons un domaine $\mathfrak{D}$ d'objets et supposons que $*$ soit une opération commutative sur $\mathfrak{D}$, et $x$ et $y$ deux objets de $\mathfrak{D}$, tels qu'il y ait en $\mathfrak{D}$ un et un seul objet $z$ tel que $x*y = y*x = z$ et que si $\tilde{x}$ est différent de $x$ et qu'il y a en $\mathfrak{D}$ un et un seul objet $\tilde{z}$ tel que $\tilde{x}*y = y*\tilde{x} = \tilde{z}$, alors $\tilde{z}$ est différent de $z$. On pourra alors associer aux objets $z$ et $x$ l'objet $y$ et aux objets $z$ et $y$ l'objet $x$. Cette association correspondra à une nouvelle opération sur $\mathfrak{D}$, disons $\circledast$, qui sera alors définie en termes de l'opération $*$ préalablement donnée. On dira que l'opération $\circledast$ ainsi définie est l'opération inverse de $*$ sur $\mathfrak{D}$.

Si les objets $x$ et $y$ sont donnés, et qu'on sait déterminer un et un seul objet $z$ de $\mathfrak{D}$, tel que $x*y = y*x = z$, alors cette définition nous conduira sur le champ aux égalités

$$\begin{aligned} z \circledast x &= y \\ z \circledast y &= x \end{aligned}$$

Mais si les objets donnés sont $y$ et $z$ ou les objets $x$ et $z$, alors rien ne nous assure qu'il y ait en $\mathfrak{D}$ respectivement un et un seul objet $x$, et un et un seul objet $y$ tels que $x*y = y*x = z$, même si $*$ est une opération qui associe un objet de $\mathfrak{D}$ à tout couple d'objets de $\mathfrak{D}$. Ainsi, s'il suffit qu'il y ait en $\mathfrak{D}$ des objets $x$, $y$ et $z$ tels que $x*y = y*x = z$ pour que l'on puisse définir sur $\mathfrak{D}$ l'opération inverse de $*$, il ne suffit pas que l'opération $*$ associe un objet de $\mathfrak{D}$ à tout couple

d'objets de $\mathfrak{D}$ pour que son opération inverse associe un objet de $\mathfrak{D}$ à tout couple d'objets de $\mathfrak{D}$. Cela n'est justement pas le cas de l'addition et de la multiplication sur les nombres. La définition de leurs opérations inverses doit ainsi tenir compte de cette situation. Voici d'abord une définition de la soustraction :

DÉFINITION 5.1. *On appelle « soustraction » (sur les nombres définis comme ci-avant) l'opération qui consiste à passer des nombres $n$ et $m$ (pris dans cet ordre) au nombre $p$, tel que :*

$$p + m = m + p = n$$

*chaque fois que $m$ et $n$ sont tels qu'il y a un et un seul nombre $p$ qui satisfasse à cette condition. Si $n$ et $m$ sont donc des nombres de telle sorte, on note leur soustraction par le symbole « $n - m$ », et on appelle « différence » le résultat $p$ de cette opération.*

DÉFINITION 5.2. *On appelle « division » (sur les nombres définis comme ci-avant) l'opération qui consiste à passer des nombres $n$ et $m$ (pris dans cet ordre) au nombre $p$, tel que :*

$$p \cdot m = m \cdot p = n$$

*chaque fois que $m$ et $n$ soient tels qu'il y ait un et un seul nombre $p$ qui satisfait à cette condition. Si $n$ et $m$ sont donc des nombres, on note leur division par le symbole « $n : m$ », et on appelle « quotient » le résultat $p$ de cette opération.*

Il est alors facile de voir que ni la soustraction, ni la division ne sont commutatives. En revanche, la commutativité de l'addition et de la multiplication permet de démontrer immédiatement le théorème suivant :

THÉORÈME 5.1. *Si $n$, $m$ et $p$ sont des nombres, alors :*

***(i)*:** *$n + m = p$ si et seulement si $p - n = m$ ;*

***(ii)*:** *$n + m = p$ si et seulement si $p - m = n$ ;*

***(iii)*:** *$n \cdot m = p$ si et seulement si $p : n = m$, pourvu que $n \neq \emptyset$ ;*

***(iv)*:** *$n \cdot m = p$ si et seulement si $p : m = n$, pourvu que $m \neq \emptyset$.*

De cela on peut ensuite conclure aisément que :

$$p - n = m \text{ si et seulement si } p - m = n$$

et

$$p : n = m \text{ si et seulement si } p : m = n, \text{ pourvu que } n, m \neq \emptyset$$

Une conséquence immédiate des théorèmes 4.5 et 5.1 est le théorème suivant, que le lecteur démontrera à titre d'exercice :

THÉORÈME 5.2. *Si $n$, $m$ et $p$ sont des nombres et $m$ n'est pas $\oslash$, alors :*

***(i)*:** *si $n - m = p$, alors $p < n$ ;*

***(ii)*:** *si $n : m = p$, alors $p < n$ ou $p = n$ ;*

La confrontation des théorèmes 4.5 4.10 et 5.1 permet de démontrer un autre théorème :

THÉORÈME 5.3. *Si $n$, $m$ sont des nombres, alors :*

***(i)*:** *il y a un nombre $p$ tel que $n - m = p$ seulement si $m < n$ ou $m = n$ (et dans ce dernier cas, $p = \emptyset$) ;*

***(ii)*:** *il y a un nombre $p$ tel que $n : m = p$ seulement si $\emptyset < m < n$ ou $m = n \neq \emptyset$ ou $m \neq n = \emptyset$ ; et si $m = n \neq \emptyset$, alors $p = \{|\}$, tandis que si $m \neq n = \emptyset$, alors $p = \emptyset$.*

Demandons-nous maintenant si ces conditions nécessaires sont aussi suffisantes. La réponse diffère dans les deux cas ; pour la soustraction vaut le théorème suivant :

THÉORÈME 5.4. *Si $n$ et $m$ sont des nombres, alors il y a un nombre $p$ tel que $n - m = p$ si et seulement si $m < n$ ou $m = n$.*

**Preuve** Une fois démontré le théorème 5.3($i$), il suffit de démontrer que

$$\text{Si } m < n \text{ ou } m = n, \text{ alors il existe un nombre } p \text{ tel que } n - m = p$$

Pour cela il faut raisonner de la manière suivante : conformément à la définition 2.2, si $m < n$, alors $m$ est en injection sur $n$, et $m$ et $n$ ne sont pas en bijection. Donc il y a une collection, qu'on pourra appeler « $p$ », telle que $p + m = n$, ce qui en vertu de la définition 5.1 entraîne que $n - m = p$. En revanche, si $m = n$, alors $n$ et $m$ sont en bijection, mais alors il suffit que $p = \emptyset$ pour que $p + m = m = n$. □

L'argument utilisé pour cette preuve ne s'applique pas au cas de la division. On peut au contraire démontrer le théorème suivant :

THÉORÈME 5.5. *Si $n$ et $m$ sont des nombres tels que $m < n$, alors (même lorsque $m \neq \emptyset$) il se peut qu'il n'y ait pas un nombre $p$ tel que $n : m = p$.*

**Preuve** Si $m = \emptyset$, alors on est dans le cas du théorème 5.3 (*ii*). En revanche, si $m \neq \emptyset$ et si un nombre $p$ tel que $n : m = p$ existait, alors on aurait, en vertu du théorème 5.1 (*iii* et *iv*), $n = p \cdot m = m \cdot p$. On pose :

$$m = \{| \, , | \, , \ldots \, |\}$$

Si pour tout couple de nombres $n$ et $m$, tels que $m < n$, il y avait un nombre $p$, tel que $n : m = p$, alors il devrait y avoir une collection $p = \{| \, , | \, , | \, , \ldots \, |\}$ telle que

$$n = \left\{ \begin{array}{c} | \, , | \, , | \, , \ldots \, |, \\ | \, , | \, , | \, , \ldots \, |, \\ \vdots \\ | \, , | \, , | \, , \ldots \, | \end{array} \right\}$$

Mais si on prend par exemple $m \neq \{|\}$ et $n = m + \{|\}$, il est facile de vérifier que cela n'est pas possible. □

REMARQUE 1.12. Cette dernière preuve suit un schéma typique : pour démontrer qu'une certaine condition $A$ n'est pas toujours satisfaite, il suffit d'exhiber une situation particulière (une seule, et construite comme l'on veut) dans laquelle cette condition n'est pas satisfaite. Il s'agit d'une preuve négative par construction d'un contre-exemple. Les preuves de cette sorte sont courantes en mathématiques.

Pour résumer les résultats auxquels on est parvenu, on posera la définition suivante :

DÉFINITION 5.3. *Si $\mathfrak{D}$ est un domaine d'objets et $*$ une opération définie sur les objets de $\mathfrak{D}$, alors on dira que $\mathfrak{D}$ est fermé relativement à $*$ lorsque : si $x$ et $y$ sont des objets de $\mathfrak{D}$, alors il y a en $\mathfrak{D}$ un et un seul objet $z$ tel que $x * y = z$, c'est-à-dire que l'opération $*$ sur $\mathfrak{D}$ associe un élément de $\mathfrak{D}$ à tout couple d'éléments de $\mathfrak{D}$. En revanche, s'il y a en $\mathfrak{D}$ des objets $x$ et $y$ tels qu'il n'y ait pas en $\mathfrak{D}$ d'objet $z$, tel que $x * y = z$, alors on dira que $\mathfrak{D}$ est ouvert relativement à $*$.*

En employant cette définition, on aura le théorème suivant :

THÉORÈME 5.6. *Le domaine des nombres est fermé par rapport à l'addition et à la multiplication, mais il est ouvert par rapport à la soustraction et à la division.*

## 6. Noms et symboles des nombres

Jusqu'ici on n'a pas éprouvé le besoin d'assigner aux différents nombres des noms spécifiques et on ne les a indiqués que par des symboles génériques, sauf quand on a fait référence au nombre $\{|\}$ ou au nombre $\emptyset$ et à leurs successeurs immédiats. En principe, on n'a besoin de rien d'autre pour construire une théorie des nombres, une « arithmétique » comme disent les mathématiciens. Mais si on n'assigne pas un nom à chaque nombre et qu'on se contente (comme on l'a fait jusqu'à présent) de caractériser tout nombre autre que $\{|\}$ ou $\emptyset$ comme le successeur du successeur... du successeur de $\{|\}$ ou de $\emptyset$, il sera difficile de formuler des théorèmes particuliers portant sur les propriétés des différents nombres par rapport aux opérations qu'on a définies sur eux. De surcroît, il sera difficile de se référer aux nombres en parlant des collections d'objets que nous rencontrons dans la vie quotidienne et dont nous avons envie de parler.

L'assignation de noms aux nombres répond essentiellement à ces exigences : elle doit donc se faire de manière à faciliter l'énoncé (et la preuve) de théorèmes portant sur des nombres particuliers et la référence aux nombres dans la vie quotidienne. Ainsi, si en principe rien ne nous empêche de désigner les nombres par des noms quelconques (comme le fait Funes dans la nouvelle de Borges, *Funes el memorioso*), cela ne répond pas aux exigences qui nous poussent à assigner des noms aux nombres. Certes, quel que soit notre choix, les noms des nombres resteront des conventions terminologiques, mais on peut songer à relier ces conventions par d'autres conventions relationnelles, de manière à soulager notre mémoire et du même coup à rendre aisée l'identification de tout nombre une fois que l'on connaît son nom.

Une façon de procéder est d'assigner des noms élémentaires et indépendants à un petit groupe de nombres et de construire tous les autres noms de nombres en combinant ces noms. Ceci fait, on pourra dire qu'on a construit un *système de dénomination* des nombres basé sur les nombres auxquels on a assigné un nom particulier. Naturellement, pour que ce système réponde à des exigences pratiques, il faut choisir la quantité des noms élémentaires en fonction de l'usage qu'on veut faire de ce même système. En laissant de côté pour l'instant les emplois spéciaux (comme ceux qui tiennent à l'informatique), supposons que notre système de dénomination doive être conçu pour les usages de la vie quotidienne. Il faut alors que les noms élémentaires ne soient pas en grande quantité (pour éviter des efforts de mémoire trop importants), mais aussi qu'ils ne soient pas trop peu nombreux (pour ne pas devoir recourir trop tôt à des noms trop composés). De surcroît, en associant à chaque nom un symbole convenable (c'est-à-dire un autre nom, sans contenu phonétique particulier, consistant en un signe), on pourra espérer faciliter les opérations sur ces noms : elles pourraient en effet se faire directement sur ces symboles et conduire à des preuves faciles pour les théorèmes portant sur des nombres particuliers. On dira que le système de ces symboles, associés en même temps aux nombres et à leurs noms, est un *système de numérotation*.

Dans l'histoire de l'humanité, différents systèmes de dénomination des nombres et de numérotation ont été adoptés, répondant plus ou moins bien à ces exigences et à ces principes. Dans la plupart d'entre eux, la composition des noms et des symboles élémentaires suit des conventions positionnelles, c'est-à-dire que chaque nom ou symbole élémentaire prend une signification différente selon la position qu'il occupe dans les noms composés. Ce principe est aussi largement adopté dans les systèmes de numérotation. Par exemple, dans la notation latine, le symbole « I » indique des choses différentes dans les symboles composés « VI » et « IV ». Dans le premier il indique qu'il faut additionner $\{|\}$ au nombre noté « V », dans le deuxième cas, qu'il faut le soustraire.

Cet exemple montre toutefois une convention positionnelle qui s'est révélée peu satisfaisante. Une convention plus satisfaisante a été découverte en Inde et importée en Europe par

les Arabes. Elle consiste à construire les symboles composés à partir du seul principe de l'addition et à assigner à chaque symbole élémentaire, non seulement une signification différente, mais aussi une valeur différente, selon sa position dans un symbole composé. En outre, les Indiens comprirent la facilité de notation dérivant de l'introduction d'un symbole indiquant une absence, renvoyant à une addition avec la collection vide.

NOTE HISTORIQUE 1.7. Bien qu'aujourd'hui on distingue soigneusement entre les nombres, les noms qui les désignent et les symboles qui les indiquent, l'histoire de l'acquisition de la notion de nombre est en même temps l'histoire de la mise au point des systèmes de représentation, puis de dénomination et expression symbolique des différentes étapes d'un comptage. C'est en partie grâce à la disponibilité des formes archaïques de représentation, puis de dénomination que l'homme est progressivement passé de la capacité de compter à la conception des nombres comme objets abstraits et séparables de l'acte de compter.

Il semble qu'on commença par représenter les invariants qu'on reconnaîtra plus tard comme des nombres par des collections d'objets particuliers, en les désignant par le biais des noms de ces collections : le soleil pour un, les yeux pour deux, le trèfle pour trois, pour ne considérer que des exemples possibles. Probablement, vint ensuite le tour de descriptions de genres, indiquant des gestes qui pouvaient donner origine à des collections d'objets dans lesquelles on reconnaissait l'invariante qu'on voulait indiquer, ou de la référence à des parties du corps aptes à évoquer ou représenter des collections convenables, par exemple la main, ou les différents doigts. Avec le temps, les noms de ces objets ou collections d'objets commencèrent à désigner directement les nombres, sans la nécessité d'aucun intermédiaire matériel ; ils commencèrent à former des successions de termes indiquant la suite des nombres.

Un tournant décisif dans ce processus fut la découverte de la possibilité d'utiliser des bases pour se référer aux différents nombres, des groupements privilégiés servant comme des sortes d'échelles permettant une répartition hiérarchisée des nombres. Cette possibilité apparut d'abord comme une aide précieuse dans la formation des noms des nombres et fut ensuite appliquée à la construction des systèmes aptes à fournir une expression symbolique écrite des nombres, permettant des calculs. Différentes bases et différents systèmes de dénomination et d'expression symbolique furent choisis par des civilisations différentes. Les Sumériens adoptèrent la base 60 (même si les noms sumériens pour des nombres inférieurs à soixante sont souvent composés) ; les Égyptiens la base 10 ; les Mayas la base 20. Les Grecs et les Romains employèrent des lettres de leurs alphabets pour exprimer des nombres. Les Indiens, qui adoptèrent la base 10, introduisirent les premiers les symboles qui, par transformations successives, et après avoir été importés en Occident par les Arabes, donnèrent origine aux chiffres modernes. Ils introduisirent aussi un symbole pour indiquer le zéro. Bien qu'ils ne fussent probablement pas les premiers à concevoir le nombre zéro et à l'exprimer symboliquement, ils surent l'employer comme un opérateur arithmétique, ce qui leur permit de construire un système de numérotation positionnel particulièrement puissant et agile qui est, au fond, celui que nous utilisons aujourd'hui.

**Lectures possibles** : G. Ifrah, *Histoire universelle des Chiffres*, Laffont, Paris, 1994 ; E. Cousquer, *La fabuleuse histoire des nombres*, Diderot éditeur, Paris, 1998.

Voici le principe général du système de numérotation indien, qui est celui qui est aujourd'hui adopté (presque) universellement. Pour en faire comprendre le fonctionnement profond, au-delà des conventions notationnelles auxquelles nous sommes habitués, je choisirai d'abord des

symboles non usuels. En choisissant les nombres $\emptyset$, $\{|\}$, $\{|,|\}$ $\{|,|,|\}$ comme les seuls auxquels on va assigner de symboles élémentaires, mon exemple portera sur les conventions notationnelles suivantes (le symbole à droite servira comme une notation du nombre à gauche) :

$$\begin{array}{llll} \emptyset & \longrightarrow & \heartsuit & \qquad\qquad \{|,|\} \longrightarrow \clubsuit \\ \{|\} & \longrightarrow & \diamondsuit & \qquad\qquad \{|,|,|\} \longrightarrow \spadesuit \end{array}$$

Pour assigner un symbole aux autres nombres, on suppose ce qui suit. Le successeur du nombre qui a reçu le dernier nom élémentaire est choisi comme base. Cela signifie que, dans un symbole numérique composé, construit comme une suite, allant de la droite vers la gauche, des symboles élémentaires, chacun des symboles « $\heartsuit$ », « $\diamondsuit$ », « $\clubsuit$ », « $\spadesuit$ » indique respectivement :

— les produits

$$\begin{array}{l} \{|\} \cdot \emptyset \\ \{|\} \cdot \{|\} \\ \{|\} \cdot \{|,|\} \\ \{|\} \cdot \{|,|,|\} \end{array}$$

si ces symboles sont positionnés à l'extrême droite de la suite ;

— les produits

$$\begin{array}{l} \{|,|,|,|\} \cdot \emptyset \\ \{|,|,|,|\} \cdot \{|\} \\ \{|,|,|,|\} \cdot \{|,|\} \\ \{|,|,|,|\} \cdot \{|,|,|\} \end{array}$$

s'ils sont positionnés immédiatement à gauche du symbole qui commence la suite, en partant de la droite ;

— les produits

$$\begin{array}{l} \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \emptyset \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|\} \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|\} \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|\} \end{array}$$

s'ils sont positionnés immédiatement à gauche du symbole qui est positionné immédiatement à gauche du symbole qui commence la suite, en partant de la droite ;

— les produits

$$\begin{array}{l} \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \emptyset \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|\} \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|\} \\ \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|,|\} \cdot \{|,|,|\} \end{array}$$

s'ils sont positionnés immédiatement à gauche du symbole qui est positionné immédiatement à gauche du symbole qui est positionné immédiatement à gauche du symbole qui commence la suite, en partant de la droite ;

— et ainsi de suite.

Cela établi, il suffit d'ajouter que la suite ainsi construite indique le nombre qui résulte de l'addition de tous les produits indiqués par les symboles élémentaires qui la composent. Il

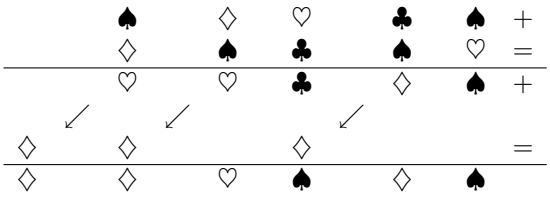
sera alors aisé de démontrer qu'après les associations élémentaires données ci-dessus, on aura les suivantes :

$$
\begin{array}{lll}
\diamondsuit\heartsuit & \longrightarrow & \{|,|,|,|\} = \{|,|,|,|\} \cdot \{|\} + \{|\} \cdot \emptyset \\
\diamondsuit\diamondsuit & \longrightarrow & \{|,|,|,|,|\} = \{|,|,|,|\} \cdot \{|\} + \{|\} \cdot \{|\} \\
\diamondsuit\clubsuit & \longrightarrow & \{|,|,|,|,|,|\} = \{|,|,|,|\} \cdot \{|\} + \{|\} \cdot \{|,|\} \\
\diamondsuit\spadesuit & \longrightarrow & \{|,|,|,|,|,|,|\} = \{|,|,|,|\} \cdot \{|\} + \{|\}\,\{|,|,|\} \\
\clubsuit\heartsuit & \longrightarrow & \{|,|,|,|,|,|,|,|\} = \{|,|,|,|\} \cdot \{|,|\} + \{|\} \cdot \emptyset \\
\clubsuit\diamondsuit & \longrightarrow & \{|,|,|,|,|,|,|,|,|\} = \{|,|,|,|\} \cdot \{|,|\} + \{|\} \cdot \{|\} \\
\ldots & \ldots & \qquad\qquad\qquad \ldots
\end{array}
$$

Un tel système de numérotation permet de réduire toute addition et toute multiplication entre nombres à des additions et des multiplications entre les nombres auxquels sont associés les symboles élémentaires. Le principe de base de cette réduction est celui de l'opération en colonne. Il s'agit d'opérer des additions sur des colonnes en reportant sur la colonne immédiatement à gauche de la colonne considérée un symbole indiquant le nombre de fois qu'on atteint le nombre choisi comme base, et en recommençant à partir de $\emptyset$, à chaque fois qu'on atteint ce nombre. Grâce à cette pratique, toute addition entre les nombres indiqués par des symboles composés appartenant au système symbolique de base $\{|,|,|,|\}$, qu'on a choisi pour notre exemple, peut être réduite à des additions sur les nombres $\emptyset$, $\{|\}$, $\{|,|\}$, $\{|,|,|\}$. Celles-ci seront des additions élémentaires, dont le résultat peut être calculé en opérant sur des collections de traits verticaux. Les résultats de ces additions élémentaires sont donnés par la table suivante (qui est évidemment symétrique, à cause de la commutativité de l'addition) :

| + | ♡ | ♢ | ♣ | ♠ |
|---|---|---|---|---|
| ♡ | ♡ | ♢ | ♣ | ♠ |
| ♢ | ♢ | ♣ | ♠ | ♢♡ |
| ♣ | ♣ | ♠ | ♢♡ | ♢♢ |
| ♠ | ♠ | ♢♡ | ♢♢ | ♢♣ |

Cette table étant posée, voici comment on calcule par exemple la somme de ♠♢♡♣♠ et de ♢♠♣♠♡, en utilisant, évidemment, l'associativité de l'addition :




Pour ce qui est de la multiplication, il est facile, en se souvenant de la distributivité de la multiplication sur l'addition, de trouver une procédure analogue. Dans notre exemple, la table de multiplication élémentaire (établie en opérant sur des collections de traits verticaux) est la suivante :

| · | ♡ | ♢ | ♣ | ♠ |
|---|---|---|---|---|
| ♡ | ♡ | ♡ | ♡ | ♡ |
| ♢ | ♡ | ♢ | ♣ | ♠ |
| ♣ | ♡ | ♣ | ♢♡ | ♢♣ |
| ♠ | ♡ | ♠ | ♢♣ | ♣♢ |

(qui, en vertu de la commutativité de la multiplication, est elle-aussi, symétrique). Cette table étant donnée, si on veut par exemple multiplier ♣♠♢ par ♢♣♠, on peut raisonner comme suit.

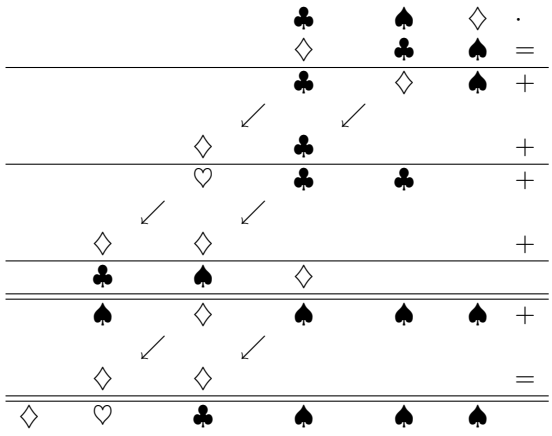
On note d'abord que, à cause des conventions constituant notre système de numérotation, on a

$$\begin{aligned} \clubsuit\spadesuit\diamondsuit &= \clubsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)]+\spadesuit\cdot[\diamondsuit\heartsuit]+\diamondsuit\cdot[\diamondsuit] \\ \diamondsuit\clubsuit\spadesuit &= \diamondsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)]+\clubsuit\cdot[\diamondsuit\heartsuit]+\spadesuit\cdot[\diamondsuit] \end{aligned}$$

et donc, à cause de la distribution de la multiplication sur l'addition :

$$(\clubsuit\spadesuit\diamondsuit)\cdot(\diamondsuit\clubsuit\spadesuit) = \left\{\begin{array}{l} (\clubsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)])\cdot[\diamondsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)]+\clubsuit\cdot[\diamondsuit\heartsuit]+\spadesuit\cdot[\diamondsuit]] \\ +(\spadesuit\cdot[\diamondsuit\heartsuit])\cdot[\diamondsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)]+\clubsuit\cdot[\diamondsuit\heartsuit]+\spadesuit\cdot[\diamondsuit]] \\ +(\diamondsuit\cdot[\diamondsuit])\cdot[\diamondsuit\cdot[(\diamondsuit\heartsuit)\cdot(\diamondsuit\heartsuit)]+\clubsuit\cdot[\diamondsuit\heartsuit]+\spadesuit\cdot[\diamondsuit]] \end{array}\right.$$

De là il est facile d'aboutir à la règle suivante : pour multiplier entre eux deux nombres $n$ et $m$, indiqués respectivement par deux suites de symboles élémentaires, on multiplie d'abord le nombre indiqué par le premier symbole élémentaire à droite, dans la suite qui indique un des nombres à multiplier, disons $m$, successivement par tous les nombres indiqués par les symboles élémentaires de l'autre nombre, disons $n$, en formant des colonnes et en reportant à gauche de celle qu'on est en train de former des symboles indiquant le nombre de fois qu'on a atteint, au cours de cette opération, le nombre choisi comme base, et en recommençant à partir de $\emptyset$, à chaque fois qu'on atteint ce nombre ; on décale d'une colonne à gauche et on fait la même chose, sur une autre ligne, relativement au nombre indiqué par le symbole élémentaire suivant à gauche le premier, dans le symbole donné qui indique le nombre $m$ ; on continue de cette manière jusqu'à épuiser les symboles élémentaires intervenant dans le symbole composé qui indique le nombre $m$ ; on additionne enfin les lignes ainsi obtenues selon la procédure par colonnes exposée auparavant. Dans le cas de notre exemple, on a ainsi :



Le passage de cet exemple à la notation habituelle à base $\{|,|,|,|,|,|,|,|,|\}$ est facile. Les symboles et les noms élémentaires seront, comme chacun sait :

$$\begin{aligned} \emptyset &\longrightarrow 0 \longrightarrow \text{zéro} \\ \{|\} &\longrightarrow 1 \longrightarrow \text{un} \\ \{|,|\} &\longrightarrow 2 \longrightarrow \text{deux} \\ \{|,|,|\} &\longrightarrow 3 \longrightarrow \text{trois} \\ &\ldots \\ \{|,|,|,|,|,|,|,|,|\} &\longrightarrow 9 \longrightarrow \text{neuf} \end{aligned}$$

Donc en reprenant les mêmes exemples, on aura

$$\begin{aligned}
\spadesuit\diamondsuit\heartsuit\clubsuit\spadesuit &= 3\cdot\left(4^4\right)+1\cdot\left(4^3\right)+0\cdot\left(4^2\right)+2\cdot(4)+3\cdot(1)\\
\diamondsuit\spadesuit\clubsuit\spadesuit\heartsuit &= 1\cdot\left(4^4\right)+3\cdot\left(4^3\right)+2\cdot\left(4^2\right)+3\cdot(4)+0\cdot(1)\\
\clubsuit\spadesuit\diamondsuit &= 2\cdot\left(4^2\right)+3\cdot(4)+1\cdot(1)\\
\diamondsuit\clubsuit\spadesuit &= 1\cdot\left(4^2\right)+2\cdot(4)+3\cdot(1)
\end{aligned}$$

où, si $n$ et $m$ sont des nombres, le symbole « $n^m$ » indique le produit

$$\underbrace{n\cdot n\cdot n\cdot\ldots\cdot n}_{m \text{ fois}}$$

ce qui entraîne

$$\begin{aligned}
4^4 &= 4\cdot4\cdot4\cdot4=(16)\cdot4\cdot4=(64)\cdot4=256\\
4^3 &= 4\cdot4\cdot4=(16)\cdot4=64\\
4^2 &= 4\cdot4=16
\end{aligned}$$

Et de là, il est facile de tirer :

$$\begin{aligned}
\spadesuit\diamondsuit\heartsuit\clubsuit\spadesuit &= 3\cdot(256)+1\cdot(64)+0\cdot(16)+2\cdot(4)+3\cdot(1)=843\\
\diamondsuit\spadesuit\clubsuit\spadesuit\heartsuit &= 1\cdot(256)+3\cdot(64)+2\cdot(16)+3\cdot(4)+0\cdot(1)=492\\
\clubsuit\spadesuit\diamondsuit &= 2\cdot(16)+3\cdot(4)+1\cdot(1)=45\\
\diamondsuit\clubsuit\spadesuit &= 1\cdot(16)+2\cdot(4)+3\cdot(1)=27
\end{aligned}$$

Et les précédentes opérations en colonnes peuvent être nottées ainsi de la manière suivante :

| | | | | | |
|---|---|---|---|---|---|
| | 8 | 4 | 3 | + | |
| | 4 | 9 | 2 | = | |
| | 2 | 3 | 5 | + | |
| | ↙ | ↙ | | | |
| 1 | 1 | | | = | |
| 1 | 3 | 3 | 5 | = | $1\cdot(10^3)+3\cdot(10^2)+3\cdot(10)+5\cdot(1)$ |
| | | | | = | $1.000+300+30+5$ |

et

| | | | | | |
|---|---|---|---|---|---|
| | | 4 | 5 | · | |
| | | 2 | 7 | = | |
| | | 8 | 5 | + | |
| | ↙ | ↙ | | | |
| | 2 | 3 | | + | |
| | 8 | 0 | − | + | |
| | ↙ | | | | |
| | 1 | | | + | |
| | 1 | 1 | 5 | + | |
| | ↙ | ↙ | | | |
| 1 | 1 | | | = | |
| 1 | 2 | 1 | 5 | = | $1\cdot\left(10^3\right)+2\cdot\left(10^2\right)+1\cdot(10)+5\cdot(1)$ |
| | | | | = | $1000+200+10+5$ |

Après ces exemples, il n'est pas nécessaire d'insister davantage sur la signification des symboles numéraux dans notre système de numération à base 10, ni de fournir l'exemple d'autres

systèmes. Il sera clair que si les symboles élémentaires sont « $\alpha_0$ », « $\alpha_1$ », « $\alpha_2$ », « $\alpha_3$ » ..., « $\alpha_n$ » avec $n \geq 5$, le symbole composé

$$\alpha_m \alpha_n \alpha_p \alpha_q \alpha_r \alpha_s$$

indiquera par exemple le nombre

$$\alpha_m \left(\alpha_1 \alpha_0\right)^{\alpha_5} + \alpha_n \left(\alpha_1 \alpha_0\right)^{\alpha_4} + \alpha_p \left(\alpha_1 \alpha_0\right)^{\alpha_3} + \alpha_q \left(\alpha_1 \alpha_0\right)^{\alpha_2} + \alpha_r \left(\alpha_1 \alpha_0\right)^{\alpha_1} + \alpha_s \left(\alpha_1\right)$$

qu'il sera facile d'additionner et de multiplier à d'autres nombres, notés dans le même système de numérotation, avec les algorithmes précédents.

REMARQUE 1.13. Quels que soient les nombres $n$ et $m$ l'écriture « $n^m$ » indique, comme on l'a dit auparavant, le produit de la multiplication $\underbrace{n \cdot n \cdot n \cdot \ldots \cdot n}_{m \text{ fois}}$, qui est dite « puissance $m$-ième de $n$ ».

Il reste à comprendre ce que signifient, dans le langage quotidien, des propositions telles que : « il y a 5 pommes dans mon panier », « il y a trois femmes dans ma vie » ou « il y a 3 jours de plus dans le mois de janvier que dans le mois de février ». Rapportées à l'exposé précédent du système des nombres, ces propositions signifient respectivement que :

— la collection des pommes qui sont dans mon panier est en bijection avec la collection de traits verticaux qui constitue le nombre indiqué par le symbole « 5 » ;

— la collection de femmes qui sont dans ma vie est en bijection avec la collection de traits verticaux qui constitue le nombre indiqué par le nom « trois » ;

— la collection de jours du mois de février est en bijection avec une collection de traits verticaux qui, soustraite à la collection de traits verticaux avec laquelle est en bijection la collection des jours du mois de janvier, produit la collection de traits verticaux indiquée par le symbole « 3 » ;

Sur la base de ces exemples, il sera facile de comprendre quelle signification il faut donner à toute proposition du langage quotidien contenant des termes numéraux. Ceux qui ont lu les *Grundlagen der Arithmetik* (1884) de Frege pourraient observer que la première des affirmations ci-dessus pourrait aussi s'énoncer ainsi :

— la collection de traits verticaux qui est en bijection avec la collection de pommes qui sont dans mon panier est celle qui constitue le nombre indiqué par le symbole « 5 » ;

ou si l'on préfère ains :

— la collection de traits verticaux qui est en bijection avec la collection de pommes qui sont dans mon panier est le nombre 5.

NOTE HISTORIQUE 1.8. Comme on l'a déjà remarqué dans la note historique I.2, Frege suggéra, dans les *Grundlagen der Arithmetik*, d'entendre une proposition dans laquelle intervient un terme numéral comme l'association d'un objet, identifié avec un nombre, à un concept. L'analyse qu'on vient de donner de la proposition « il y a 5 pommes dans mon panier » concorde avec la suggestion de Frege : selon cette analyse, une telle proposition dit du concept 'pommes qui sont dans mon panier' qu'il est associé au nombre 5. Cela signifie que, dans cette proposition, le symbole « 5 » (mais on aurait pu dire la même chose du terme « cinq » s'il était apparu dans une telle proposition) se réfère à un objet, est le nom d'un objet.

Comme on l'a aussi remarqué dans la note I.3, cette conclusion permet, d'après Frege, d'assigner aux termes (et aux symboles) numéraux la même signification, qu'ils interviennent dans des propositions arithmétiques ou qu'ils interviennent dans des

propositions du langage quotidien : ces termes sont dans les deux cas des noms d'objets. Frege pense que la possibilité de garantir cette identité de signification est une condition à laquelle toute philosophie plausible de l'arithmétique doit satisfaire : si cela n'était pas le cas, on comprendrait mal comment l'arithmétique peut prétendre à une application dans la vie quotidienne. Je crois que Frege a, à ce propos, parfaitement raison.

Dire qu'un terme numéral est un nom d'objet n'est pas exactement la même chose que de dire qu'un nombre est un objet. Pour passer de la première à la deuxième thèse, il faut disposer d'une explication plausible de l'identification entre nombres et objets qui ne renvoie pas, tout simplement, au fonctionnement logique du langage. Bien qu'il n'y ait aucun doute que Frege ait soutenu dans les *Grundlagen* la première de ces thèses, certains doutent qu'il ait aussi soutenu la deuxième. Bien que la distinction entre les deux thèses soit parfaitement claire, il me semble pourtant que la manière avec laquelle Frege soutient la première rend sa philosophie totalement redevable non seulement de la deuxième thèse, mais aussi d'une thèse bien plus forte : les nombres sont des objets qui existent indépendamment de nos constructions théoriques et de notre langage ; les propositions portant sur les nombres sont vraies ou fausses de ces objets, et leur valeur de vérité est donc indépendante de toute preuve (dire d'une proposition arithmétique qu'elle a été prouvée ou qu'elle est prouvable ce n'est pas la même chose que de dire qu'elle est vraie). Cette thèse plus forte est généralement connue sous le nom de « platonisme arithmétique », et Frege est généralement présenté comme le champion du platonisme arithmétique.

Naturellement, l'arithmétique n'est pas la seule branche des mathématiques par rapport à laquelle il est possible d'énoncer la thèse platoniste. Ce qu'on vient de dire des nombres peut bien être dit de tout autre entité mathématique. Le platonisme mathématique serait alors la thèse qui affirme l'existence préalable d'un domaine d'objets mathématiques, que nos théories mathématiques ne font que décrire, tant bien que mal. Cette thèse est acceptée par un bon nombre de philosophes des mathématiques contemporains et elle est tout naturellement acceptée par la majorité des mathématiciens. Elle comporte pourtant de graves problèmes et des ambiguïtés non secondaires. Le débat autour des avantages et des difficultés du platonisme mathématique a été très vif depuis la fin du XIX$^{\text{ème}}$ siècle et il est loin d'être terminé. Il me semble pourtant que ce débat pourrait être bien plus productif si on savait distinguer la thèse radicale, ou ontologique, que je viens de présenter, d'autres thèses qui, tout en concordant avec celle-ci quant à l'interprétation des théories mathématiques comme des théories d'objets, sauraient éviter les dérives ontologiques et métaphysiques de cette position. Pour ce faire, il me semble possible et souhaitable de se tourner du côté d'une conception phénoménologique de l'objectivité.

**Lectures possibles** : M. Dummet, *Frege. Philosophy of Mathematics*, Duckworth, London 1991 ; M. Panza et J.-M, Salanskis (éds.), *L'objectivité mathématique. Platonisme et structures formelles*, Masson, Paris, 1995.

CHAPITRE 2

# Nombres entiers positifs : une théorie axiomatique

Dans l'exposé précédent, on n'a eu aucun besoin de se référer à des axiomes, c'est-à-dire à des propositions non démontrées qui fournissent un point de départ pour une théorie. La raison en est que la théorie des nombres (entiers positifs) qui y est présentée traite d'objets empiriques tels que les collections de traits verticaux. Cela ne signifie pas qu'elle fasse l'objet d'une confirmation expérimentale ou qu'elle puisse être réfutée par l'expérience. Comme toute théorie empirique, elle construit ses objets par abstraction en les identifiant à des entités qui sont en même temps sensibles et universelles. Le caractère sensible de ces entités vient du fait qu'elles ne se présentent que sous la forme d'objets, déterminés dans le temps et l'espace, dont les propriétés sensibles (ou certaines des propriétés sensibles) décident des propriétés de ces mêmes entités ; leur caractère universel vient en revanche de ce qu'on décide d'en considérer les différentes présentations comme des manifestations du même objet, et qu'on limite et codifie l'ensemble des procédures jugées aptes à fournir des renseignements sur cet objet. Tout au plus, on aurait pu se réclamer d'un système d'axiomes pour fixer ces procédures. Mais on a préféré le faire différemment, en se réclamant de notre capacité de distinguer l'acte de compter de tout autre acte portant sur une collection d'objets.

Ce qui est particulier à la théorie exposée dans le chapitre 1, par rapport aux autres théories empiriques, c'est qu'elle fixe *a priori* et une fois pour toutes, aussi bien les pratiques portant sur les présentations de ses objets et aptes à fournir des renseignements sur eux, que les procédures permises pour parvenir à une présentation de ces objets. Ainsi, aucune réfutation n'est possible et la théorie qu'on a exposée peut être reconnue à la fois comme empirique et comme mathématique, et donc (en tant que telle) infalsifiable par l'expérience.

Les démonstrations qui interviennent dans cette théorie se fondent ainsi, en dernière instance, sur des pratiques réglées, portant sur des objets sensibles tels que les collections de traits verticaux. Il suffit, pour valider de telles démonstrations, de s'assurer qu'elles ne dépendent pas de la nature particulière des objets sensibles sur lesquels elles portent, et peuvent donc être répétées sur n'importe quelles autres collections de traits verticaux (et même sur n'importe quelles autres collections d'objets). Mais, si on ne doute pas que ces preuves soient correctes, on peut penser qu'elles ne font pas émerger la logique strictement formelle qu'on voudrait trouver à la base de la plus fondamentale des théories mathématiques, celle des nombres entiers positifs. C'est la raison qui a conduit plusieurs mathématiciens, vers la fin du XIX$^{e}$ siècle, à chercher une théorie formelle de ces nombres, c'est-à-dire un système logique dans lequel on pût retrouver (convenablement réinterprétés) tous les théorèmes connus portant sur les nombres entiers positifs.

NOTE HISTORIQUE 2.1. D'après l'historiographie courante, une crise profonde, concernant les fondements mêmes des mathématiques, s'est abattue sur cette discipline, entre la fin du XIX$^{ème}$ siècle et le début du XX$^{ème}$. Pour soutenir ce jugement, on se réclame d'abord de la naissance des géométries non euclidiennes ; on cite ensuite les paradoxes de l'infini, ceux apparus à l'intérieur de la théorie des fonctions de variable réelle, et enfin ceux qui concernèrent la théorie des ensembles. Tout cela

aurait montré aux mathématiciens qu'une grande partie des convictions qu'ils avaient maintenues pendant des siècles, parfois des millénaires, n'étaient fondées que sur des sentiments d'évidence qui se révélaient trop faibles pour soutenir l'attaque inexorable des raisons de la logique.

Même si la lecture d'un tel fragment de l'histoire des mathématiques qui se réclame d'une opposition entre l'intuition et la logique me paraît largement insatisfaisante, il n'y a pas de doute que ces phénomènes conduisirent les mathématiciens à repenser les modalités de fondation de leurs théories, et même à aborder en général la question des critères de légitimité tant des prémisses d'une théorie mathématique que des preuves acceptées à l'intérieur de ces théories. La fondation de l'arithmétique proposée par Frege dans ses *Grundlagen*, dont on a parlé dans le chapitre 1, et celles de Dedekind et Peano, dont on va parler dans la suite, sont, du moins en partie, des filles directes de cette réflexion.

En restant à un niveau de généralité plus élevé, on distingue habituellement entre trois approches dans les réponses qui furent données à ces problèmes : l'approche logiciste, inaugurée par Frege, tendant à une réduction des mathématiques à la théorie des ensembles et, plus généralement, à la logique ; l'approche intuitionniste, généralement associée au nom du mathématicien hollandais L. E. J. Brouwer (cf. note 6.4), affirmant qu'une théorie mathématique ne pouvait faire confiance qu'à des arguments finitaires et constructifs ; et l'approche formaliste, qui, après avoir été, en quelque sorte, annoncée par les travaux de Dedekind et Peano, aurait été finalement codifiée par David Hilbert, qui, dans les années 1920 siècle, consacra plusieurs mémoires à la question des fondements des mathématiques.

Malheureusement, la plupart des textes historiques et philosophiques non consacrés explicitement à une analyse des conceptions de Hilbert, présentent le formalisme en termes presque caricaturaux, souvent pour rendre plus facile la tâche de la critique. On dit souvent que l'ambition formaliste est de réduire les mathématiques à un pur jeu formel, dans lequel n'interviendraient que des successions et des transformations de symboles. À en croire ces caricatures, le mathématicien formaliste ne ferait que jongler avec des symboles, auxquels il n'aurait attaché aucune signification différente de celle qui leur est assignée par les règles syntactiques qui président à leurs combinaisons.

Mais, naturellement, ni Hilbert, ni aucun mathématicien ou philosophe des mathématiques sérieux, n'a jamais soutenu une telle absurdité. La conviction de Hilbert était plutôt que les enchaînements logiques, non directement constructifs et finitaires, propres à une théorie mathématique, doivent être aptes à être traduits en preuves formelles, conduites à l'intérieur de systèmes, dont on devait pouvoir démontrer finitairement et constructivement la cohérence (le fait que pour tout énoncé $p$ formulable dans le système, $p$ et non-$p$ ne sont pas en même temps des théorèmes) et la complétude syntactique (le fait que pour tout énoncé $p$ formulable dans le système, ou bien c'est un théorème $p$, ou bien c'est un théorème non-$p$). On sait qu'en démontrant que tout système formel cohérent, assez riche pour pouvoir contenir l'arithmétique, est syntactiquement incomplet (c'est le célèbre théorème d'incomplétude de Gödel, démontré par ce dernier en 1931), Gödel rendit vaines les espérances de Hilbert.

Cela ne conduit pourtant pas les mathématiciens à abandonner l'idée que la formalisation d'une preuve ou d'une théorie pouvait apporter, plutôt qu'un fondement certain, au moins une clarification des relations logiques inhérentes à cette preuve ou théorie, et une explicitation de ses conditions et de ses prémisses. C'est sous cette

forme que l'idéal formaliste reste vivant parmi les mathématiciens (même si, en partie sous la poussée de nouvelles exigences d'application et de la plus large capacité de calcul induite par l'avènement des ordinateurs, on a aujourd'hui une tendance toujours plus forte à travailler à l'intérieur de théories non formalisées) ; le formalisme n'est jamais pensé par un mathématicien autrement que comme une forme de présentation et/ou une modalité d'objectivation d'idées profondes, concernant la structure d'un monde que le mathématicien vise, par ses efforts, à interroger et à comprendre. C'est aussi de cette manière qu'on doit étudier et comprendre les théories formelles : non pas comme des systèmes fermés et dépourvus de toute raison extérieure, mais comme le résultat de l'effort de compréhension d'une réalité préalable.

**Lectures possibles** : F. Gonseth, *Les mathématiques et la réalité*, Alcan, Paris, 1936 (réimprimé par Blanchard, Paris, 1974) ; P. Benacerraf and H. Putnam (ed. by), *Philosophy of Mathematics. Selected readings*, Cambridge Univ. Press, Cambridge, London, New York, New Rochelle, Melbourne, Sydney, 2nd ed., 1983 ; J.-C. Pont, « Aux sources du conventionnalisme », *Les savants et l'épistémologie vers la fin du* XIX$^{\text{ème}}$ *siècle*, M. Panza et J.-C. Pont, éds., , Blanchard, Paris, 1995, pp. 109-144.

* * *

Né à Königsberg en 1862, David Hilbert étudia les mathématiques à l'université de sa ville natale, où il fut nommé professeur en 1892. En 1895 il se transféra à Göttingen, où il resta jusqu'à la fin de sa carrière, pour rentrer enfin à Königsberg, où il mourut en 1943. Avec Poincaré (cf. note 1.5), Hilbert fut probablement le dernier mathématicien universel de l'histoire. Ses contributions fondamentales concernent pratiquement la totalité des domaines des recherches mathématiques. Outre les travaux qu'on a évoqués ci-dessus, les philosophes des mathématiques citent souvent pour ses études sur les fondements de la géométrie euclidienne, dans lesquels, en même temps qu'il inaugura la longue saison de l'axiomatisation géométrique, il parvint à dévoiler les directrices profondes des développements de cette discipline, à partir d'Euclide jusqu'à Descartes et à la naissance de la géométrie projective.

Dans le deuxième congrès international de mathématiques, tenu à Paris en 1900, on demanda à Hilbert de prévoir les lignes de développement des mathématiques pour le siècle qui s'annoncait selon lui. Hilbert répondit en énonçant vingt-trois problèmes ouverts qui, à son opinion, auraient occupé les mathématiciens des générations successives. Un siècle plus tard, on ne peut que rester étonné de la capacité de prévision qu'il démontra à cette occasion : ces problèmes furent et, sont encore en partie, au centre des recherches mathématiques. Si, à l'aube du XXI$^{\text{ème}}$ siècle, on voulait faire de même, on ne saurait pas trouver de mathématicien capable du même exploit. Ce que Hilbert fit à lui tout seul, il y a un siècle, ne pourrait être fait aujourd'hui que par une équipe relativement large de mathématiciens, avec des spécialisations différentes.

**Lectures possibles** : C. Reid, *Hilbert*, Springer Verlag, Berlin, Heidelberg, New York, 1970 ; P. Cassou-Noguès, *Hilbert*, Les Belles Lettres, Paris, 2001 ; J. Gray, *Le Défi de Hilbert. Un siècle de mathématiques*, Dunod, Paris, 2003.

Parmi ces tentatives, deux méritent une attention particulière : celle du mathématicien allemand R. Dedekind et celle du mathématicien italien G. Peano. Ces deux théories ont naturellement des affinités, mais elles diffèrent aussi sur beaucoup d'aspects. Tandis que Dedekind construit, à partir de la donnée préalable d'un ensemble infini, la succession infinie des nombres entiers positifs comme une chaîne satisfaisant à certaines conditions, et peut donc démontrer

les principales propriétés des nombres entiers positifs comme des propriétés des éléments de la chaîne, Peano ne part que de cinq axiomes fixant les propriétés d'un ensemble présenté d'emblée comme l'ensemble des nombres entiers positifs (ou naturels, comme on dira dans la suite). Ici je me limite à présenter la théorie de Peano, sans doute plus simple et plus abordable que celle de Dedekind, sous la forme qui m'apparaît la plus convenable (qui n'est d'ailleurs pas, à strictement parler, celle choisie par Peano lui-même). Je ferai l'hypothèse que le lecteur soit familier avec quelques notions élémentaire, qui font l'objet d'un premier cours de logique, même si, de temps à autre, j'introduirai des précisions qui me paraîtront être utiles.

NOTE HISTORIQUE 2.2. Entre 1884 et 1891, quatre auteurs essayèrent, en partant de points de vues différents, de fournir des fondements pour l'arithmétique. D'abord Frege, avec ses *Grundlagen* de 1884, dont on a parlé dans la chapitre 1, ensuite Richard Dedekind, en 1888, avec le mémoire *Was sind und was sollen die Zahlen ?,* et Giuseppe Peano, une année plus tard, avec ses *Arithmetices Principia*, nova methodo exposita, et enfin Edmund Husserl, en 1891, avec sa *Philosophie der Arithmetik*. Si les motivations de Frege concernaient surtout l'analyse logique du langage et celles de Husserl visaient plutôt une recherche sur les origines psychologiques des concepts numéraux, Dedekind et Peano avaient en vue une véritable fondation mathématique de l'arithmétique.

Comme Frege, Dedekind pensait que pour fonder l'arithmétique il faut se réclamer de la notion d'ensemble. Mais, tandis que Frege semble prendre cette notion comme une notion logique primitive, en se contentant de contribuer à sa clarification philosophique, Dedekind fut un des premiers, avec G. Cantor, à concevoir une véritable théorie mathématique des ensembles. D'après lui, l'arithmétique doit être pensée comme une théorie de certaines sortes d'ensembles qualifiés de « chaînes », et caractérisés comme on le verra ci-dessous.

On définira par la suite, avec plus de précision, la notion d'application. Pour l'instant on peut se limiter à penser une application comme une loi qui associe tout élément d'un ensemble $A$ donné à un élément d'un ensemble $B$ également donné, éventuellement coïncidant avec $A$, de telle sorte que si $a$ est un élément de $A$ qui est associé par cette loi à un élément $b$ de $B$, alors il n'est associé qu'à cet élément de $B$, de sorte qu'aucun élément de $A$ n'est associé par cette loi, en même temps, à deux ou plusieurs éléments de $B$. Si les deux ensembles $A$ et $B$ coïncident, alors l'application est une application de cet ensemble sur lui-même et associe des éléments d'un ensemble $A$ donné à des éléments de ce même ensemble, de telle sorte qu'aucun élément de $A$ n'est associé en même temps à deux ou plusieurs éléments de $A$. Soit alors $S$ un ensemble donné, $\Phi$ une application de $S$ sur lui-même et $K$ un sous-ensemble (non vide) de $S$, tel que l'application $\Phi$ associe à tout élément de $K$ un élément de $S$. On dira que $K$ est une chaîne de $S$, et en particulier une $\Phi$-chaîne de $S$, si l'ensemble $\Phi(K)$ de tous les éléments de $S$ qui sont associés par $\Phi$ à des éléments de $K$ est inclus dans $K$. Imaginons maintenant que $T$ soit un sous-ensemble non vide quelconque d'un ensemble $S$ donné, et considérons toutes les $\Phi$-chaînes de $S$ qui contiennent $T$. L'intersection de ces $\Phi$-chaînes ne sera évidemment pas vide et elle sera dite « $\Phi$-chaîne de $T$ ». Si $T$ se réduit à un seul élément $x$ de $S$, alors la $\Phi$-chaîne de $T$ sera dite aussi « $\Phi$-chaîne de $x$ ». Soit maintenant $N$ un ensemble tel qu'il existe une application $F$ de $N$ sur lui-même, qui est à son tour telle que $N$ coïncide avec la $\Phi$-chaîne d'un élément $n$ de $N$ qui n'appartient pas à l'ensemble $\Phi(N)$ de tous les éléments de $N$ qui sont associés par $\Phi$ à des éléments de $N$. On dira que l'ensemble $N$ est « simplement infini ». D'après Dedekind, l'arithmétique n'est

rien d'autre que la théorie d'un ensemble simplement infini quelconque. Le lecteur motivé pourra prouver à lui tout seul, une fois qu'il aura pris connaissance de la définition de progression qu'on donnera ci-dessous, qu'un ensemble est simplement infini si et seulement s'il est une progression. Cela lui montrera que la formalisation de l'arithmétique proposée par Dedekind est logiquement équivalente à celle proposée par Peano.

Plutôt que de chercher, comme Dedekind, à construire explicitement des ensembles vérifiant les lois de l'arithmétique, Peano était intéressé à énoncer des axiomes à partir desquels tous les théorèmes de l'arithmétique pouvaient être déduits par l'application de lois d'inférence purement logiques. Convaincu de la nécessité de préciser le langage des mathématiques, et de réduire tout argument mathématique à une pure déduction formelle conduite à l'intérieur d'un langage préalablement donné, Peano conçut l'oeuvre de fondation de l'arithmétique comme un effort de formalisation. Il fut de cette manière un des pionniers de la logique moderne ; on raconte que sa rencontre avec Russell fut à l'origine du tournant qui porta ce dernier à abandonner ses conceptions idéalistes et transcendantales, et à se consacrer aux recherches qui le conduisirent à la rédaction, avec A. P. Whitehead, des *Principia Mathematica*. Son texte de 1889 est en latin ; plus tard, Peano inventera même une longue toute nouvelle — le *latino sine flexione* — prénant la forme d'un latin simplifié, dans le but de libérer la communication et l'exposition scientifique des imprécisions et des suppositions implicites qui affectent les langues vernaculaires.

**Lectures possibles** : D. Gillies, *Frege, Dedekind and Peano on the Foundations of Arithmetic*, Van Gorcum, Assen, 1982 ; J.-P. Belna, *La notion de nombre chez Dedekind, Cantor, Frege*, Vrin, Paris, 1996.

* * *

Richard Dedekind naquit à Brunswick en Allemagne, le 6 octobre 1831, et mourut également à Brunswick, le 12 février 1916. Il étudia à l'université de Göttingen où il rencontra Bernhard Riemann et devint un élève du « prince des mathématiques », Friedrich Gauss. Après avoir été assistant de Dirichlet, le successeur de Gauss, il fut nommé en 1858 comme professeur à l'École Polytechnique de Zurich et en 1862, il retourna à Brunswick comme professeur à l'École Polytechnique, où il resta jusqu'à la fin de sa vie. Ses contributions les plus importantes aux développements des mathématiques concernent la théorie des nombres, les fondements de l'arithmétique et de l'analyse, en particulier la définition des nombres réels et la caractérisation mathématique de la notion de continuité, sur lesquels on reviendra dans le chapitre 6.

**Lecture possibles** : P. Dugac, *Richard Dedekind et les fondements des mathématiques*, Vrin, Paris, 1976.

* * *

Né à Spinetta, près de Cuneo en Italie, le 27 août 1858 et mort à Turin le 20 avril 1932, Giuseppe Peano fit ses études à l'université de Turin, où il fut nommé professeur à l'âge de trente-deux ans. Bien qu'il soit surtout connu pour ses travaux de pionnier en logique formelle et par son essai sur les fondements de l'arithmétique, il consacra la plupart de ses recherches mathématiques à des questions d'analyse et à la mise en place d'un « calcul géométrique ». En 1891, il fonda la *Rivista di Matematica*, autour de laquelle il réunit un groupe de jeunes collaborateurs dont certains

devinrent, comme Pieri et Burali-Forti, des mathématiciens de première envergure. En 1895 il publia la première édition de ce qu'il avait conçu comme son chef d'oeuvre, le *Formulario*, une exposition, selon les normes d'une déduction purement formelle et écrite dans un langage purement logique, de l'ensemble des mathématiques connues. Peano en prépara cinq éditions successives, mais le *Formulario* ne connut toutefois pas le succès que son auteur avait espéré. De même que le *latino sine flexione*, le formalisme de Peano, mis à part quelques symboles isolés, comme le symbole « $\in$ » indiquant l'appartenance d'un élément d'un ensemble, disparut graduellement de la scène mathématique internationale, et ne survécut pas à son auteur.

**Lectures possibles** : H. C. Kennedy, *Peano. Life and Works of Giuseppe Peano*, Reidel Pub. Comp., Dordrecht, Boston, London, 1980 ; G. Heinzmann, *Poincaré, Russell, Zermelo et Peano. Textes de la discussion (*1906-1912*) sur les fondements des mathématiques : des antinomies à la prédicativité*, Blanchard, Paris, 1986.

## 1. L'ensemble des nombres naturels : les cinq axiomes de Peano

0n va commencer notre exposition par la définition suivante :

DÉFINITION 1.1. *On appelle « progression » un ensemble $\mathfrak{P}$ non vide, sur lequel est définie une relation binaire notée « $\mathbf{P}$ », telle que chaque élément de $\mathfrak{P}$ est dans la relation $\mathbf{P}$ avec un et un seul élément de $\mathfrak{P}$ distinct de lui-même, et :*

- **(*i*):** *en $\mathfrak{P}$ il y un élément, disons $\alpha$, tel qu'aucun élément de $\mathfrak{P}$ n'est dans la relation $\mathbf{P}$ avec $\alpha$ (c'est-à-dire qu'il n'y a pas de $x$ appartenant à $\mathfrak{P}$ tel que $x\mathbf{P}\alpha$) ;*
- **(*ii*):** *il n'y a aucun élément de $\mathfrak{P}$, tel que plusieurs éléments distincts de $\mathfrak{P}$ soient dans la relation $\mathbf{P}$ avec lui (c'est-à-dire que si $y$ et $z$ sont des éléments distincts de $\mathfrak{P}$, alors il n'y pas en $\mathfrak{P}$ un élément $x$, tel que $y\mathbf{P}x$ et $z\mathbf{P}x$) ;*
- **(*iii*):** *pour chaque élément $x$ de $\mathfrak{P}$, on peut passer, par une succession finie d'étapes, de $\alpha$ à $x$, en passant à chaque étape de l'élément considéré à celui avec lequel cet élément est dans la relation $\mathbf{P}$ (ainsi, si $x$ est l'élément de $\mathfrak{P}$ tel que $\alpha\mathbf{P}x$, on passe d'abord de $\alpha$ à $x$, et si $y$ est l'élément de $\mathfrak{P}$ tel que $x\mathbf{P}y$, on passe ensuite de $x$ à $y$, et ainsi de suite).*

REMARQUE 2.1. Qu'on observe que la notion de relation, ainsi qu'elle est définie en logique moderne, et ainsi qu'on l'emploie ici, est telle que le fait qu'un objet $x$ est en une certaine relation avec un objet $y$ est bien différent du fait que l'objet $y$ est en cette même relation de avec l'objet $x$. Une relation $\mathbf{R}$ peut bien sûr être symétrique, c'est-à-dire que pour tout couple d'objets $x$ et $y$, si $x\mathbf{R}y$ alors $y\mathbf{R}x$. Tel est par exemple le cas de la relation 'être concitoyen de'. Ceci n'est pourtant pas le cas de toute relation, et, en particulier, ce n'est pas le cas de la relation $\mathbf{P}$ définie sur $\mathfrak{P}$. En outre, même si $\mathbf{R}$ est une relation symétrique, l'être de $x$ dans la relation $\mathbf{R}$ avec $y$ n'est pas la même chose que l'être de $y$ dans la relation $\mathbf{R}$ avec $x$. Ainsi, il est bien possible que tout élément d'un ensemble $E$ soit dans une relation $\mathbf{R}$ avec un autre élément de $E$, et qu'il y ait en $E$ un certain élément $x$, tel qu'aucun autre élément de $E$ ne soit dans la relation $\mathbf{R}$ avec $x$. Ceci est justement le cas pour l'ensemble $\mathfrak{P}$, l'objet $\alpha$ et la relation $\mathbf{P}$ qui interviennent dans la définition précédente.

La définition 1.1 permet de démontrer aisément le théorème suivant :

THÉORÈME 1.1. *L'ensemble des nombres entiers positifs (tels qu'ils ont été définis dans le chapitre 1) est une progression.*

**Preuve** Il s'agit de vérifier que l'ensemble $\{\{|\}, \{|,|\}, \{|,|,|\}, \ldots\}$ (ou éventuellement l'ensemble $\{\emptyset, \{|\}, \{|,|\}, \{|,|,|\}, \ldots\}$) satisfait à toutes les conditions intervenant dans la définition 1.1, ce qui est facile à faire en prenant le nombre $\{|\}$ (ou éventuellement le nombre $\emptyset$) pour l'élément $\alpha$ de cet ensemble et en identifiant la relation **P** avec la relation qui intervient entre tout nombre (entier et positif) $n$ et son successeur $\sigma(n)$. □

S'il est facile d'aboutir à cette preuve, il est également facile de prouver que, à partir de l'ensemble des nombres entiers positifs (tels qu'ils ont été définis dans le chapitre 1), il est possible de construire d'autres progressions, distinctes de cet ensemble. Un exemple immédiat est donné par l'ensemble $\{1, 3, 5, \ldots\}$ dans lequel on prend encore $\alpha = 1$ et on identifie la relation **P** avec la relation qui intervient entre tout nombre (entier et positif) $n$ et le successeur $\sigma(\sigma(n))$ de son successeur. La construction d'autres exemples ne comporterait aucune difficulté et est laissée au lecteur comme exercice.

REMARQUE 2.2. Le théorème 1.1 n'est pas une conséquence quelconque de la définition 1.1 ; dans un sens, il est sa raison d'être même. Cette dernière définition a été en effet conçue de manière à exprimer la structure logique de l'ensemble des nombres entiers positifs, tels que nous les apprenons avant toute formalisation de l'arithmétique. On a là un exemple typique d'une dialectique intrinsèque à toute sorte de formalisation. Si les définitions et les axiomes qui fournissent la base d'un système formel sont, par rapport au déroulement des déductions à l'intérieur de ce même système, des points de départ non justifiés, des prémisses imposées par un acte thétique parfaitement libre du mathématicien, ils sont aussi imposés par le but ultime de l'acte de formalisation, qui est généralement celui de retrouver, comme conséquences de ces prémisses, des théorèmes bien connus à l'avance. Si, dans un sens, rien n'oblige à choisir une définition ou un axiome plutôt qu'un autre (pourvu qu'on reste cohérent), aucun mathématicien ne saurait exploiter cette liberté pour construire des théories parfaitement arbitraires. Aucune construction mathématique ne peut être comprise sans tenir compte du but qu'elle poursuit, qui est généralement celui d'exprimer, au moyen d'un système abstrait et général, des connexions déjà observées sous une forme ou un aspect particulier. L'hostilité que certains éprouvent face aux mathématiques et à leur formalisme dépend, dans la plupart des cas, de l'incompréhension de cette dialectique, et de la conviction profondément erronée, souvent induite par un mauvais enseignement, que les prémisses et les modes d'enchaînement d'une théorie mathématique sont des commandements indiscutables, dictés par une autorité externe, dont la volonté et les raisons sont totalement insaisissables.

La définition 1.1 nous permet aussi de prouver un théorème qui justifie *a priori* toute la construction de Peano :

THÉORÈME 1.2. *Un ensemble $\mathfrak{H}$ est une progression si et seulement s'il remplit les conditions suivantes :*

**P.1):** *$\mathfrak{H}$ n'est pas vide et il contient en particulier un élément, noté « $x_0$ », qui satisfait aux conditions (P.3) et (P.5) ;*

**P.2):** *sur $\mathfrak{H}$ est définie une application $\Phi$, associant tout élément $x$ de $\mathfrak{H}$ à un (et un seul) élément $\Phi(x)$ du même $\mathfrak{H}$, c'est-à-dire que $\Phi$ est telle que :*

$$\text{si } x \text{ appartient à } \mathfrak{h}, \text{ alors } \Phi(x) \text{ appartient à } h.$$

**P.3):** *il n'y a pas d'élément $x$ de $\mathfrak{h}$ tel que :*

$$x_0 = \Phi(x)$$

**P.4):** *si $x$ et $y$ appartiennent à $\mathfrak{h}$ et $\Phi(x) = \Phi(y)$, alors $x = y$ ;*

**P.5):** *si* $\mathfrak{S}$ *est un sous-ensemble de* $\mathfrak{h}$ *tel que :*

*(i)* $x_0$ *appartient à* $\mathfrak{S}$ *;*

*(ii) si* $x$ *appartient à* $\mathfrak{S}$*, alors* $\Phi(x)$ *appartient à* $\mathfrak{S}$ *;*

*alors* $\mathfrak{S}$ *coïncide avec* $\mathfrak{H}$ *(c'est-à-dire que chaque* $x$ *appartenant à* $\mathfrak{H}$ *appartient à* $\mathfrak{S}$*).*

REMARQUE 2.3. On note que la condition d'unicité indiquée entre parenthèses dans la condition (P.2) est implicite dans la notion même d'application, car on appelle « application » toute association entre deux ensembles qui associe chaque élément du premier ensemble à un et un seul élément du deuxième. On dénote généralement une application par le symbole « $\varphi \ : A \to B$ », où « $\varphi$ » est le nom de l'application et $A$ et $B$ sont deux ensembles, dits respectivement « ensemble de départ » et « ensemble d'arrivée » de $\varphi$, l'application $\varphi$ étant dite, de ce fait, « application de $A$ vers $B$ ». L'élément $y$ de $B$ qui résulte associé, par une application $\varphi$, à un élément $x$ de $A$ est dit « image de $x$ selon $\varphi$ » et est généralement noté « $\varphi(x)$ », de sorte que l'égalité « $y = \varphi(x)$ » nous dit justement que $y$ est l'image de $x$ selon $\varphi$. On observe qu'il n'est pas nécessaire que $A$ et $B$ soient des ensembles distincts. Le même ensemble peut servir en effet aussi bien d'ensemble de départ que d'ensemble d'arrivée pour une application. Si $A$ est cet ensemble, alors on appelle l'application en question « application de $A$ sur lui-même ». Ceci est le cas de l'application $\Phi$ intervenant dans le théorème précédent, qui est justement une application de $\mathfrak{H}$ sur lui-même.

Une application est ainsi un type particulier de fonction, car on appelle « fonction » toute association entre deux ensembles (dit respectivement « ensemble de départ » et « ensemble d'arrivée » de la fonction) qui associe chaque élément d'un sous-ensemble quelconque du première ensemble (éventuellement chaque élément du premier ensemble) à un et un seul élément du deuxième. Si $f$ est une fonction et $A$ et $B$ sont respectivement son ensemble de départ et son ensemble d'arrivée (ce qu'on note également par le symbole « $f \ : A \to B$ » ), alors on dit, comme dans le cas plus restraint d'une application, que l'élément $y$ de $B$ qui résulte associée par $f$ à l'élément $x$ de $A$ est *l'image* de $x$ selon $f$ et on le note par le symbole « $f(x)$ ».

Comme la définition précédente le dit, il n'est donc pas nécessaire qu'une fonction $f$ associe tout élément de son ensemble de départ à un (et un seul) élément de son ensemble d'arrivée. Pour avoir une fonction de $A$ vers $B$, il suffit que chacun parmi certains éléments de $A$ soit associé à un (et un seul) élément de $B$. Par exemple si on prend comme ensemble de départ et d'arrivée l'ensemble des nombres entiers positifs (tels qu'on les a définis dans le chapitre 1), et comme loi d'association celle qui associe à un nombre entier positif $x$ le nombre entier positif $x - 27$, il est clair que seulement les nombres entiers plus grands ou égaux à 27 sont associés par cette fonction à un (et un seul) nombre entier positif. Le sous-ensemble de l'ensemble de départ d'une fonction $f$ formé par tous les éléments de cet ensemble qui résultent associés par $f$ à un (et un seul) élément de l'ensemble d'arrivée est dit « domaine de $f$ » (ou, quelque fois, « domaine de définition de $f$ » ).

Ainsi, une application n'est rien d'autre qu'une fonction dont l'ensemble de départ coïncide avec le domaine de définition. Ceci étant dit, notons que rien n'oblige une fonction ou, plus en particulier, une application à être telle que tout élément de son ensemble d'arrivée soit tel qu'un élément de son ensemble de départ lui soit associé par cette même fonction ou application. Si on prend encore comme ensemble de départ et d'arrivée l'ensemble des nombres entiers positifs, et comme loi d'association une fonction qui associe à un nombre entier positif $x$ le nombre entier positif $x + 27$, il est clair que seulement les nombres entiers

plus grands ou égaux à 27 sont images selon $f$ d'un autre nombre entier positif. Le sous-ensemble de l'ensemble d'arrivée $B$ d'une fonction ou d'une application $f$ formé par toutes les images des éléments de l'ensemble de départ de $f$ est dit « image du domaine de $f$ ».

Une fonction ou application $f$ qui associe tout élément de son domaine à un élément distinct de son ensemble d'arrivée (de sorte que chaque élément de l'image de son domaine résulte être associé par $f$ à un et un seul élément de son domaine) — de sorte que si $x$ et $y$ sont deux éléments distincts du domaine de $f$, alors les images de $x$ et $y$ selon $f$ sont aussi distinctes — est dite « injective » ou même directement « injection ». Une fonction ou application $f$ dont l'ensemble d'arrivée coïncide avec l'image de son domaine est dite « surjective » ou simplement « surjection ». Enfin, une fonction ou application qui est en même temps injective et surjective est dite « bijective » ou simplement « bijection ». Il sera facile de vérifier que ces définitions s'accordent aux définitions des expressions « être en bijection » et « être en injection » données — dans un cas particulier — dans le paragraphe 1, une fois qu'on a décidé de considérer l'association qui associe entre eux les éléments de deux collections d'objets comme une application, dont ces collections sont respectivement l'ensemble de départ et l'ensemble d'arrivée. Finalement, il ne sera pas difficile de comprendre que l'application $\Phi$ qui intervient dans le théorème précédent est définie comme une application de $\mathfrak{H}$ sur $\mathfrak{H}$ l'image de son domaine étant l'ensemble $\mathfrak{H} - x_0$ formé en soustrayant de $\mathfrak{H}$ l'élément $x_0$. Cette application sera donc injective, mais elle ne sera pas surjective et elle ne sera donc non plus bijective.

La preuve du théorème 1.2 est longue, mais non difficile. Il s'agit de montrer que tout ensemble qui satisfait aux conditions intervenant dans la définition 1.1 remplit aussi les conditions (P.1)-(P.5) et, réciproquement, que tout ensemble qui satisfait aux conditions (P.1)-(P.5) satisfait aussi aux conditions intervenant dans la définition 1.1. Il faut faire bien attention au fait que j'aie dit « tout ensemble » et non « un ensemble ». La différence entre les deux formulations est claire : si on se contentait de la deuxième, on devrait conclure que pour démontrer le théorème 1.2, il suffit d'exhiber une progression qui satisfasse aux conditions (P.1)-(P.5). Or, le théorème 1.1 nous assure justement que l'ensemble des nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, est une progression. Il suffirait donc de se fonder sur les résultats atteints dans le paragraphe 3 pour conclure qu'un tel ensemble satisfait aussi aux conditions (P.1)-(P.5), et prétendre ainsi avoir déjà démontré le théorème. Le vice de cet argument tient à ce qu'il est possible que les raisons qui font que l'ensemble des nombres entiers positifs —tels qu'ils ont été définis dans le chapitre 1— est une progression, ne coïncident pas avec celles qui font que ce même ensemble satisfait aux conditions (P.1)-(P.5). En utilisant un tel argument, on montrerait alors seulement que l'ensemble des nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, est une progression, et qu'il satisfait aux conditions (P.1)-(P.5), mais non pas qu'un ensemble est une progression si et seulement s'il satisfait à ces dernières conditions. Ceci étant dit, voyons la preuve du théorème 1.2 :

**Preuve du théorème 1.2** Je partage cette preuve en deux parties qui prouvent respectivement les deux directions de la double implication qu'il faut prouver (je rappelle que pour prouver que $A$ si et seulement si $B$, il faut prouver que si $A$ alors $B$ et que si $B$ alors $A$) :

($a$) Imaginons d'abord qu'une progression $\mathfrak{P}$ soit donnée. Étant justement une progression, $\mathfrak{P}$ n'est pas vide et possède un élément $\alpha$ qui se comporte comme la définition 1.1 le prescrit. Rien ne nous empêche ainsi de noter cet élément $\alpha$ de $\mathfrak{P}$ par le symbole « $x_0$ ». Pour montrer que $\mathfrak{P}$ satisfait à la condition (P.1), il suffira donc de montrer que $\alpha$ satisfait aux conditions (P.3) et (P.5), ce qu'on va faire ci-après. Comme $\mathfrak{P}$ est une progression, alors pour chaque élément $x$ de $\mathfrak{P}$ il y a un élément $y$ de $\mathfrak{P}$ tel que $x\mathbf{P}y$, $\mathbf{P}$ étant telle qu'elle respecte toutes les conditions de la définition 1.1. Pour définir sur $\mathfrak{P}$ une application $\Phi$ qui satisfasse à la condition

(P.2), il suffit alors de poser, pour tout élément $x$ de $\mathfrak{P}$, la convention :

$$y = \Phi(x) \quad \text{si et seulement si} \quad x\mathbf{P}y$$

Comme cette définition est toujours possible, $\mathfrak{P}$ satisfait à la condition (P.2). Il est de même facile de vérifier que, grâce à cette définition et en vertu des conditions (*i*) et (*ii*) de la définition 1.1, $\mathfrak{P}$ satisfait aussi aux conditions (P.3) et (P.4). Reste la condition (P.5). Remarquons d'abord que, selon la définition précédente de $\Phi$, pour chaque $x$ appartenant à $\mathfrak{P}$, l'image $\Phi(x)$ est unique et elle est distincte de $x$. Prenons maintenant un élément quelconque $z$ de $\mathfrak{P}$ et construisons le sous-ensemble de $\mathfrak{P}$ qui contient tous les éléments de $\mathfrak{P}$ appartenant à la chaîne permettant de passer dans $\mathfrak{P}$ de $x_0$ (qui n'est autre que $\alpha$) à $z$. Il est clair que $x_0$ appartient à cette chaîne et que si $x$ lui appartient, alors son image $\Phi(x)$ lui appartiendra aussi, en vertu de la définition de $\Phi$, et que c'est le cas quel que soit $z$. Imaginons maintenant que $\mathfrak{S}$ soit un sous-ensemble de $\mathfrak{P}$, que $x_0$ appartienne à $\mathfrak{S}$ et que $\mathfrak{S}$ soit tel que si $x$ lui appartient, alors son image $\Phi(x)$ lui appartient aussi. Ceci dit, considérons encore un élément quelconque $z$ de $\mathfrak{P}$. Si $z = x_0$, alors il appartient à $\mathfrak{S}$. En revanche, si $z \neq x_0$, alors, en vertu de ce qui vient d'être dit, il sera l'image d'un élément de $\mathfrak{P}$ qui est l'image d'un autre élément de $\mathfrak{P}$ qui est l'image d'un autre élément de $\mathfrak{P}$ et ainsi de suite. À l'issue d'un nombre fini d'étapes, on arrivera ainsi à $x_0$. Donc, $z$ appartient à $\mathfrak{S}$ et $\mathfrak{S}$ coïncide avec $\mathfrak{P}$, car tout élément $z$ de $\mathfrak{P}$ appartient à $\mathfrak{S}$, et $\mathfrak{S}$ est, par hypothèse, un sous-ensemble de $\mathfrak{P}$. L'ensemble $\mathfrak{P}$ satisfait donc aussi à la condition (P.5). Ici s'achève la première partie de la preuve.

(*b*) Construisons maintenant un ensemble $\mathfrak{H}$ qu'on ne caractérisera que par le fait qu'il satisfait aux conditions (P.1)-(P.5). Cet ensemble n'est pas vide, en vertu de (P.1). Si l'on en reste à (P.2), il pourra ne contenir qu'un élément $x_0$, pourvu qu'on ait $\Phi(x_0) = x_0$. Le diagramme suivant (où la flèche indique l'association induite par l'application $\Phi$) illustre cette situation :

Première Figure p. 88

Pourtant, si c'était le cas, notre ensemble ne pourrait satisfaire à la condition (P.3). Il doit donc contenir au moins un autre élément $x_1 \neq x_0$. Si on en restait là, il serait possible pourtant que notre ensemble soit composé seulement des éléments $x_0$ et $x_1$, pourvu que $x_1 = \Phi(x_1)$. Le diagramme suivant (où les flèches indiquent à nouveau les associations induites par l'application $\Phi$) illustre cette situation :

Seconde Figure p. 88

Mais, encore une fois, si c'était le cas, notre ensemble ne pourrait pas satisfaire à la condition (P.4), car on aurait $\Phi(x_0) = \Phi(x_1)$ et $x_0 \neq x_1$. Il est clair que, pour la même raison, on ne pourra jamais compléter notre ensemble en lui ajoutant des éléments distincts des précédents et en s'arrêtant là. Donc, notre ensemble devra contenir une chaîne ouverte d'éléments commençant par $x_0$ et contenant des images distinctes pour chacun de ses éléments. Mais il pourrait aussi contenir, à côté de la chaîne de ces éléments, d'autres éléments, constituant une ou plusieurs chaînes, séparées les unes des autres. Et ces chaînes, ne contenant pas $x_0$, pourraient être aussi bien linéaires, et ouvertes, soit d'un côté, soit des deux, que circulaires, comme le montre le diagramme suivant (où les flèches indiquent encore une fois les associations induites par l'application $\Phi$) :

$$\mathfrak{H} = \left\{ \begin{array}{ccccccccccccc} x_0 & \to & x_1 & \to & x_2 & \to & \ldots & & & & x_{\nu''} & & \\ & & & & & & & & & \nearrow & & \searrow & & \\ x_\nu & \to & x_\mu & \to & x_\lambda & \to & \ldots & & \vdots & & & & x_{\mu''} \\ & & & & & & & & & \nwarrow & & \swarrow & \\ \ldots & \to & x_{\nu'} & \to & x_{\mu'} & \to & x_{\lambda'} & \to & \ldots & & x_{\lambda''} & & \end{array} \right\}$$

Mais si c'était le cas, notre ensemble contiendrait au moins un sous-ensemble $\mathfrak{S}$ qui ne satisferait pas à (P.5). Donc la chaîne ouverte commençant par $x_0$, c'est-à-dire

$$x_0 \to x_1 = \Phi(x_0) \to x_2 = \Phi(x_1) = \Phi(\Phi(x_0)) \to \ldots$$

doit coïncider avec l'ensemble $\mathfrak{H}$. À ce point, il suffit de montrer qu'un ensemble de la sorte est une progression, en répétant un raisonnement semblable à celui qui a permis de démontrer le théorème 1.1. Ceci achève la preuve. □

Remarque 2.4. Qu'on observe que, lors de la deuxième partie de la démonstration précédente, on a prouvé, en passant, que tout ensemble qui satisfait aux conditions (P.1)-(P.4) intervenant dans le théorème 1.2 (et donc, *a fortiori*, tout ensemble qui satisfait aux conditions (P.1)-(P.5) intervenant dans ce même théorème) est infini. Comme un ensemble de cette sorte est nécessairement une progression, cela signifie qu'une progression est nécessairement un ensemble infini, bien qu'il y ait évidemment beaucoup d'ensembles infinis qui ne sont pas des progressions. Ici, on considère les notions d'ensemble fini et d'ensemble infini comme acquises. On pourrait définir pourtant un ensemble infini comme un ensemble non fini, et un ensemble fini comme un ensemble qui satisfait à ce que C. S. Peirce appelait, en suivant De Morgan, le « syllogisme de la quantité transposée ».

L'exemple choisi par Peirce pour illustrer ce syllogisme est fort joli. Imaginons qu'il n'y ait pas plus de jeunes françaises que de jeunes français. On sait (c'est Balzac qui l'observe dans la *Physiologie du mariage*) que chaque jeune français se vante d'avoir séduit au moins une jeune française. Comme, au sens propre, une femme ne peut être séduite qu'une fois, le syllogisme de la quantité transposée nous conduit à conclure que, à en croire les vanteries des jeunes français, aucune jeune française n'est vierge. Cette conclusion n'est pourtant correcte qu'à condition qu'il n'y ait qu'un nombre fini de jeunes françaises. En inversant l'argument, on pourrait ainsi appeler un ensemble « fini », lorsqu'il est tel qu'il satisfait à une inférence comme celle-ci.

Lorsqu'on généralise l'exemple de Peirce, on s'aperçoit qu'il porte sur la considération d'une fonction surjective, celle qui associe chaque jeune française qui ne soit plus vierge au jeune français qui l'a séduite. L'ensemble de départ de cette fonction est l'ensemble des jeunes françaises, son ensemble d'arrivée est celui des jeunes français. Notre conclusion équivaut ainsi à affirmer que l'ensemble de départ de cette fonction correspond à son domaine de définition : cette fonction est donc une application. Imaginons alors que deux jeunes françaises aient été séduites par le même jeune français. Il en suivrait qu'il y a plus de jeunes françaises que de jeunes français, contre notre hypothèse. L'application en question doit donc être non seulement surjective, mais aussi injective, c'est-à-dire qu'elle doit être une bijection.

Considérons alors un ensemble quelconque et une application bijective quelconque de cet ensemble vers un de ses sous-ensembles. La question est la suivante : est-il possible que l'ensemble d'arrivée (qui correspond par définition à l'image du domaine) de cette application soit une partie propre de son domaine (c'est-à-dire, un sous-ensemble de cet ensemble qui ne coïncide pas avec ce même ensemble) ? On pourra raisonner comme dans

le cas de l'exemple de Peirce : si la réponse est négative, alors on dira que notre ensemble est fini, si elle est positive, on dira qu'il est infini. On obtiendra une définition qui, depuis l'époque de Peirce, est devenue classique : un ensemble est infini s'il peut être mis en bijection avec une de ses parties propres, autrement il est fini. Il est facile alors de vérifier qu'une progression est un ensemble infini, car l'application $\Phi$ définie sur $\mathfrak{H}$ comme ci-dessus est bien une bijection dont le domaine est $\mathfrak{H}$ et l'image du domaine est $\mathfrak{H} - \mathfrak{x}_0$ qui est évidemment une partie propre de $\mathfrak{H}$.

Informellement, cette belle définition équivaut à celle-ci : un ensemble est infini s'il contient autant d'éléments qu'une de ses parties propres. Inversant l'implication et en acceptant de savoir *a priori* ce qu'est un ensemble infini, on pourra dire qu'un ensemble infini contient autant d'éléments que certaines de ses parties propres. Voici un exemple facile : il y a autant de nombres entiers positifs que de nombres pairs, car l'ensemble des nombres entiers positifs peut être mis en bijection avec l'ensemble des nombres pairs (en associant 0 à 0, 2 à 1, 4 à 2, 6 à 3, et généralement $2i$ à $i$, quel que soit le nombre entier positif $i$). Si on réfléchit bien on comprendra aussi que, dans ce même sens, il y a autant de nombres entiers positifs que de nombres entiers positifs plus grands que 27, que 100, ou que 1315. La définition de progression vise, entre autres, à caractériser généralement un ensemble qui possède cette remarquable propriété.

Note Historique 2.3. L'exemple de Peirce se trouve dans un article intitulé « The law of Mind », publié dans la revue *The Monist* en 1892 et il est généralisé dans la troisième de ses *Cambridge Conferences*, prononcées à Cambridge (U.S.A.) en 1898. Voici ce que Peirce écrivit à cette occasion : « Les multitudes finies se caractérisent ainsi : s'il y a une relation dans laquelle chaque individu dans un tel système se tient par rapport à quelque autre mais aucun tiers ne se tient par rapport à cet autre, alors, par rapport à chaque individu du système, quelque autre individu se tient dans cette relation ». Dit en d'autres termes : si du fait qu'on peut définir sur les éléments d'un ensemble une relation $R$, telle que, pour chaque élément $x$ de cet ensemble, il y a un élément $y$ de ce même ensemble, distinct de $x$, tel que $xRy$, cette relation étant telle que, quel que soit $y$, si $xRy$ et $zRy$, alors $x = z$, il suit que pour chaque élément $y$ de cet ensemble il y a un élément $x$ de ce même ensemble, distinct de $y$, tel que $xRy$, alors cet ensemble est fini.

Pour comprendre la situation, considérons l'ensemble $\{0, 1, 2, 3\}$ et supposons que chaque élément de cet ensemble soit dans une relation $R$ avec un autre élément de ce même ensemble, cette relation étant telle que deux éléments distincts de cet ensemble ne peuvent pas être dans la relation $R$ avec le même élément de ce même ensemble. Imaginons que 0 est dans la relation $R$ avec 1 ($0R1$), 1 avec 2 ($1R2$), et 2 avec 3 ($2R3$). Il est clair alors que les conditions qu'on a supposées ne sont satisfaites qu'à condition que 3 soit dans la relation $R$ avec 0 ($3R0$). Il en résulte que pour tout élément de l'ensemble, il y a en un autre qui est dans la relation $R$ avec lui. Cet ensemble est donc fini. L'ensemble $\{0, 1, 2, 3, 4, ...\}$ est en revanche tel qu'il y a une relation, la relation 'être successeur de', qui satisfait à toutes les conditions qu'on a supposées, et qui est néanmoins telle qu'un des éléments de l'ensemble, évidemment 0, est tel qu'aucun autre élément de cet ensemble n'est dans cette relation avec lui. Cet ensemble est donc infini. Dans le premier cas, la relation $R$ correspond à une bijection de l'ensemble $\{0, 1, 2, 3\}$ sur lui-même, tandis que dans le deuxième cas, la relation 'être successeur de' correspond à une bijection de l'ensemble $\{0, 1, 2, 3, 4, ...\}$ vers sa partie propre $\{1, 2, 3, 4, ...\}$.

L'idée de Peirce de définir le fini en termes de satisfaction du syllogisme de la quantité transposée, ou, ce qui est équivalent, de l'impossibilité pour un ensemble d'être en bijection avec une de ses parties propres, tient évidemment à une inversion de l'ordre logique le plus naturel, qui est d'ailleurs, en même temps, l'ordre historique. Historiquement, les mathématiciens ont commencé par reconnaître l'implication inverse : un ensemble infini peut être mis en bijection avec une de ses parties propres. Ils le firent d'abord, depuis l'antiquité, en considérant cette propriété comme paradoxale et en éprouvant un certain malaise à son égard. Le premier à observer que cette propriété correspond à un fait mathématique indiscutable et à la traiter comme une propriété caractéristique et parfaitement formulable des ensembles infinis fut B. Bolzano, qui lui consacra le paragraphe 20 de son pamphlet *Paradoxien des Unendlichen* (*Paradoxes de l'infini*), publié, trois ans après la mort de son auteur, en 1851.

Pour affirmer qu'un ensemble infini peut être mis en bijection avec une de ses parties propres, il faut cependant avoir défini *a priori* ce qu'est un ensemble infini, et cela ne semble faisable qu'en se réclamant de quelque chose comme la dimension de cet ensemble, ou sa générativité. L'idée de Peirce, d'invertir l'implication et de l'utiliser comme une définition des ensembles infinis, revient donc à réduire l'idée d'infinité à un comportement relationnel des éléments d'un ensemble, les uns par rapport aux autres, de sorte à éviter, dans la définition des ensembles infinis, toute référence aux idées, souvent vagues, de dimension et de générativité. On verra, plus loin, en particulier dans les chapitres 4 et 6, comment, à partir de la reconnaissance du caractère infini de l'ensemble des nombres entiers positifs, il est ensuite possible de définir une hiérarchie d'infinités qui permet de donner un sens précis à la notion de dimension, en passant par celle de cardinalité.

**Lectures possibles** : S. Peirce, *Le raisonnement et la logique des choses. Les conférences de Cambridge (1898)*, éd. du Cerf, Paris, 1995 ; B. Bolzano, *Paradoxes de l'infini*, Seuil, Paris, 1993.

* * *

Charles Sanders Peirce fut le deuxième des cinq enfants de Benjamin Peirce, professeur d'astronomie et de mathématiques à Harvard, un des intellectuels et des politiciens les plus influents des jeunes États Unis d'Amérique. Il naquit le 10 septembre 1839 à Cambridge et grandit dans une maison fréquentée par la plus illustre société américaine. Après une carrière scolaire plutôt médiocre, en dépit du génie que lui reconnaissait son père, il entra en 1867 à l'Institut Géodésique Fédéral, où se dernier travaillait aussi. Quitté par son épouse, il eut le tort, aux yeux de plusieurs bien-pensants, d'aller vivre avec une autre femme, avant d'avoir obtenu le divorce. Ce fut un scandale qui marqua toute la vie de Peirce : sur le point d'obtenir une chaire de logique à l'université John Hopkins de Baltimore, où il avait enseigné longtemps comme lecteur, il fut renvoyé du monde académique, qu'il avait côtoyé depuis son enfance. Après la mort de son père, en 1890, il abandonna l'Institut Géodésique et se retira, avec sa seconde femme, dans une maison de campagne en Pennsylvanie, où il se consacra à des études de plus en plus isolées, dans une situation matérielle de plus en plus dégradée. Après sa mort, en 1914, on trouva dans sa maison quelques 80.000 feuillets de notes qui s'ajoutaient aux nombreux articles qu'il avait publiés. L'étude de ces notes, qui furent depuis publiées partiellement et dans le plus grand désordre, dans les *Collected Papers of C. S. Peirce*, n'est pas encore terminée, bien que leur influence ait été déjà très grande. Loin des communautés académiques, Peirce sut

forger des conceptions qui, un siècle plus tard, montrent encore leur extraordinaire originalité.

**Lectures possibles** : C. Hookway, *Peirce*, Routledge & Kegan Paul, London, Boston, Melbour, Henley, 1985 ; C. Tiercelin, *La pensée-signe. Étude sur C.S. Peirce*, Chambon, Nîmes, 1993 ; S. Marietti, *Icona e diagramma. Il segno matematico in Charles Sanders Peirce*, LED, Milano, 2001.

Grâce au théorème 1.2, on sait non seulement que l'ensemble des nombres entiers positifs (tels qu'ils ont été définis auparavant), remplit les conditions (P.1)-(P.5) — ce que d'ailleurs on savait déjà —, on sait aussi que toute progression satisfait à ces conditions. L'acte fondateur de la théorie de Peano consiste justement à identifier les nombres entiers positifs, qu'on appellera dorénavant « nombres naturels », avec les éléments d'une progression particulière, c'est-à-dire avec un certain ensemble qui répond aux conditions (P.1)-(P.5), ainsi promues au rang d'axiomes de la théorie des nombres naturels. Il n'est naturellement pas nécessaire de caractériser davantage un tel ensemble ; il suffit de nommer convenablement ses éléments de manière à les distinguer, à l'occasion, des éléments de toute autre progression — qui, de toute façon, sera en bijection avec cet ensemble et pourra par conséquent, lorsqu'elle sera considérée séparément, être identifiée avec lui. On pourra exprimer la même idée en d'autres termes : la nécessité de distinguer l'ensemble des nombres naturels d'une autre progression, quelle qu'elle soit, ne se présente que lorsqu'on veut considérer en même temps différentes progressions, distinctes les unes des autres, et identifier une et une seule de celles-ci à cet ensemble ; dans ce cas, il suffira pourtant d'identifier une progression quelconque à l'ensemble des nombres naturels, et de caractériser les autres progressions en fonction de celle-ci. Les nombres naturels ne seront alors que les éléments d'une progression quelconque, et donc l'arithmétique ne sera que la théorie d'une progression quelconque.

Si on note par le symbole « $\mathbb{N}$ » l'ensemble des nombres naturels, les axiomes de Peano pourront alors être formulés comme suit :

**Axiomes de Peano**

Axiome 1, $\alpha$ est un nombre naturel ; en symboles :

$$\alpha \in \mathbb{N}$$

Axiome 2. Si $x$ est un nombre naturel, alors il y a un et un seul nombre naturel $x'$ qui est son successeur ; en symboles :

$$x \in \mathbb{N} \Rightarrow \exists! y \in N \text{ tel que } y = x'$$

Axiome 3. Il n'y a pas de nombre naturel dont $\alpha$ est le successeur ; en symboles :

$$\neg \exists x \in \mathbb{N} \text{ tel que } x' = \alpha$$

Axiome 4. Chaque nombre naturel qui soit le successeur d'un (autre) nombre naturel est le successeur d'un seul nombre naturel ; en symboles :

$$x, y \in \mathbb{N} \Rightarrow [x' = y' \Rightarrow x = y]$$

Axiome 5. Si $\mathfrak{S}$ est un ensemble de nombres naturels (c'est-à-dire un sous-ensemble de $\mathbb{N}$), si $\alpha$ appartient à $\mathfrak{S}$, et si du fait que $x$ appartient à $\mathfrak{S}$, il suit que $x'$ appartient à $\mathfrak{S}$, alors $\mathfrak{S}$ contient tous les nombres naturels ; en symboles :

$$\mathfrak{S} \subseteq \mathbb{N} \Rightarrow ([(\alpha \in S) \wedge (x \in S \Rightarrow x' \in S)] \Rightarrow [x \in N \Rightarrow x \in S])$$

Le lecteur n'aura aucune difficulté à vérifier que ces axiomes correspondent aux conditions (P.1)-(P.5), lorsqu'on décide d'identifier $x_0$ avec $\alpha$, de nommer l'image $\Phi(x)$ de $x$ « successeur de $x$ », et de la noter par le symbole « $x'$ ».

REMARQUE 2.5. Bien que fort commode, la représentation symbolique des axiomes précédents n'est évidemment pas essentielle. Elle n'a d'autre but que de rendre explicite la structure logique de la condition qu'elle exprime. Les symboles « $\neg$ », « $\Rightarrow$ », « $\wedge$ », « $\exists$ », « $\in$ » et « $\subseteq$ » qui y interviennent peuvent être pensés comme des constantes logiques, c'est à dire des symboles qui restent invariants en passant d'une théorie particulière à une autre n'appartenant qu'au langage logique général dans lequel cette théorie est exprimée. Je fais ici l'hypothèse que le lecteur soit familier avec ces symboles. Si cela n'était pas le cas, il pourrait comprendre leur signification en comparant l'expression symbolique des axiomes précédents avec leur énoncé discursif. Pour l'aider, je dirais seulement que « $\neg$ » est le symbole de négation qui traduit l'expression « non ... », « $\Rightarrow$ » est le symbole d'implication qui traduit l'expression « si ... alors ... », « $\wedge$ » est le symbole de conjonction qui traduit l'expression « ... et ... », « $\exists$ » est le symbole d'existence qui traduit l'expression « il y a un ... », « $=$ » est le symbole d'égalité, valant ici comme une identité, traduisant l'expression « ... est le même que ... » ou « ... est identique à ... », « $\in$ » est le symbole d'appartenance qui traduit l'expression « ... appartient à ... », et enfin « $\subseteq$ » est le symbole d'inclusion qui traduit l'expression « ... est inclus dans ... ». Dans la suite, on trouvera, à côté de celles-ci, deux autres constantes logiques : « $\vee$ » et « $\Leftrightarrow$ », indiquant respectivement la disjonction inclusive « ou ... ou ... ou les deux » et la double implication « ... si et seulement si ... ». Quant au symbole « $\exists!$ » est le symbole, il est généralement utilisé pour indiquer la condition d'existence et unicité. L'écriture « $\exists! y \mathcal{A}(y)$ » nous dit donc qu'il existe un et un seul $y$ qui satisfait à la condition indiquée par « $\mathcal{A}(y)$ ». Naturellement, ce symbole n'est pourtant pas primitif, et peut donc être éliminé. Au lieu de « $\exists! y \mathcal{A}(y)$ », on écrira alors « $\exists y \mathcal{A}(y) \wedge [(\mathcal{A}(y) \wedge \mathcal{A}(z)) \Rightarrow y = z]$ ». L'écriture « $\exists! y \mathcal{A}(y)$ » n'est donc rien d'autre qu'une abréviation commode d'une écriture plus longue et complexe.

Certains lecteurs pourraient être surpris de ne pas trouver parmi ces symboles, et dans l'expression symbolique des axiomes de Peano, le symbole « $\forall$ » d'universalisation, traduisant d'habitude l'expression « pour tout ... ». Si je ne l'ai pas employé, et je ne l'emploierai pas non plus dans la suite, c'est pour souligner ce qui, de mon point de vue, est une caractéristique profonde des mathématiques. En mathématiques, une proposition universelle n'est en général que l'expression d'une condition suffisante. Elle ne dit jamais, á la rigueur, que tout $x$ satisfait à la condition $A$, mais plutôt que tout $x$ qui satisfait à la condition $B$, satisfait aussi à la condition $A$. Mais dire ceci signifie dire qu'il suffit que $x$ satisfasse à la condition $B$ pour qu'il satisfasse aussi à la condition $A$. C'est d'ailleurs sous cette dernière forme, que les logiciens identifient avec une formule ouverte (car elle présente une variable libre, c'est-à-dire une variable qui n'appartient au rang d'aucun quantificateur), qu'une proposition universelle est, en dernière instance, généralement démontrée en mathématique. Ainsi, s'il est souvent discursivement commode d'adopter des expressions telles que « pour tout ... » ou « quel que soit ... », la structure logique des conditions universelles dans l'énoncé desquelles entrent ces expressions est celle d'une implication ouverte. De ce fait, je ne peux pas personnellement comprendre la raison qui pousse la plupart des logiciens à penser qu'une formule ouverte n'a pas, à proprement parler, de sens et de valeur de vérité. Il me semble au contraire que les mathématiques font un usage essentiel des formules ouvertes. Dans la suite de mon exposé, je m'en tiendrai à cette conviction, qu'il m'a semblé nécessaire d'expliciter.

À côté des constantes logiques dont on vient de parler, les axiomes de Peano font aussi usage de trois termes propres à la théorie des nombres naturels, qui, lorsque ces

axiomes sont pris comme points de départ d'une théorie, ne font l'objet d'aucune définition précédente. Ces termes, qui sont dits de ce fait « primitifs », sont évidemment « $\alpha$ », « nombre naturel » et « successeur ». La définition de ces termes est pourtant donnée, implicitement, par les axiomes de Peano eux-mêmes. En effet, tirer des conséquences de ces axiomes signifie, en dernière instance, montrer comment ces termes peuvent se combiner entre eux, une fois que leurs combinaisons exprimées par ces axiomes sont acceptées.

NOTE HISTORIQUE 2.4. D'un point de vue logique, on peut décrire une théorie formelle comme un système déductif caractérisé par : un langage fixé, donnant la liste complète des symboles qu'on utilise pour écrire les énoncés de la théorie ; des règles de bonne formation de ces énoncés, spécifiant quelles combinaisons de symboles peuvent valoir comme énoncés de la théorie ; des axiomes, c'est-à-dire des énoncés qu'on suppose comme points de départs de toute déduction ; des règles d'inférence, fixant les transformations symboliques qu'on peut opérer sur des énoncés donnés, et qui valent comme de pas déductifs. On distingue généralement deux sortes d'axiomes : les axiomes logiques et les axiomes propres. Les axiomes logiques ne portent que sur les constantes logiques qui interviennent dans le langage, et ne dépendent donc pas de la nature particulière de la théorie ; à des équivalences près, leur variation ne dépend ainsi que du choix de la logique qu'on veut faire opérer dans la théorie (ce point sera plus clair après la lecture de la note 6.4). Les axiomes logiques portent en revanche sur les constantes individuelles, prédicatives, relationnelles et fonctionnelles, intervenant dans le langage, c'est-à-dire les symboles de ce langage qui sont censés se référer respectivement aux objets particuliers de la théorie, à leurs propriétés, aux relations que ces objets entretiennent entre eux, et aux fonctions définies sur ceux-ci. Ces axiomes varient donc avec la théorie et on peut même dire qu'ils servent à caractériser la théorie à laquelle ils participent. Dans certaines présentations, il est possible de substituer aux axiomes propres et aux règles d'inférence des règles dites « d'introduction » et « d'élimination », fixant les modalités par lesquelles on peut former des énoncés, à partir d'autres énoncés donnés, en introduisant ou en éliminant des constantes logiques. On dit alors qu'on travaille dans un système de *déduction naturelle*. Il n'est pas difficile de montrer l'équivalence entre les deux formes de présentation.

Souvent, dans les textes mathématiques, même quand il s'agit de présenter une théorie formelle, on évite de spécifier préalablement le langage de cette théorie, en introduisant ses symboles au fur et à mesure que cela est nécessaire, on suppose connaître *a priori* les règles de bonne formation, et on donne pour acquises les propriétés (ou, si on préfère, la signification) des constantes logiques. La présentation d'une théorie formelle se réduit ainsi à la spécification des axiomes propres, dans lesquels on devra alors faire intervenir toutes les constantes non logiques primitives de la théorie (on dit qu'une constante non logique d'une théorie n'est pas primitive si elle est introduite par le biais d'une définition explicite qui introduit cette constante comme une abréviation d'une combinaison de symboles dont on dispose préalablement). Ces constantes ne peuvent évidemment faire l'objet d'aucune définition préalable aux axiomes dans lesquels elles apparaissent, car chaque définition demanderait de disposer préalablement d'un *definiens*, c'est-à-dire d'une structure symbolique qu'on pourrait faire entrer dans la définition comme ce en fonction de quoi on définit la nouvelle constante, et ceci porterait à une régression *ad infinitum*. Les seules définitions acceptables pour les constantes non logiques primitives d'une théorie formelle sont donc des définitions implicites.

Les cinq axiomes de Peano sont évidemment des axiomes propres. La formulation précédente de ces axiomes répond pourtant plus qu'à un idéal de précision formelle, à une exigence de transparence conceptuelle. Si on analyse soigneusement ces axiomes, ainsi qu'on les a énoncés ci-dessus, on se rend compte en effet qu'ils font référence à une notion préalable qui ne fait l'objet d'aucune définition implicite. Il s'agit évidemment de la notion d'ensemble. Si on voulait se libérer de cette notion préalable, on devrait soit fournir d'autres axiomes propres servant a la caratériser sous forme d'une constante non logique (ce qui revient á immerger les axiomes de Peano en la théorie formelle des ensembles), soit présenter ces derniers axiomes comme de pures séquences de symboles. Ces axiomes ne seraient alors que les points de départ d'une déduction. Au lieu d'écrire « $\alpha \in \mathbb{N}$ », on devrait écrire par exemple « $N(\alpha)$ », les symboles « ( » et « ) » valant comme constantes logiques, et les symboles « $N$ » et « $\alpha$ » comme constantes non logiques primitives, respectivement prédicative et individuelle, à côté desquelles on devra successivement introduire l'autre constante non logique, primitive et fonctionnelle, « $'$ ».

Au sens strict, la théorie des nombres naturels qu'on présente ici n'est donc pas encore une théorie formelle, au sens dans lequel la notion de théorie formelle est présentée dans les textes de logique. Il est pourtant difficile de trouver un texte mathématique qui respecte jusqu'au bout les contraintes énoncées dans ces textes. L'idée de formalisation propre aux mathématiques vivantes est en effet assez différente de celle fixée par les prescriptions de la logique formelle.

**Lectures possibles** : A. Tarski, *Introduction to Logic and to the Methology of Deductive Sciences*, Oxford Univ. Press, New York, 2nd ed., 1946 ; René David, Karim Nour, Christophe Raffali, *Introduction à la logique. Théorie de la démonstration. Cours et exercices corrigés*, Dunod, Paris, 2001.

Remarque 2.6. Les axiomes de Peano étant posés, la théorie des nombres naturels ne sera constituée que par les théorèmes qui en seront déduits. Avant de passer à la démonstration de quelques-uns de ces théorèmes (qui correspondront aux théorèmes énoncés dans le chapitre 1, même si leur preuve ne pourra qu'être tout autre), il est bon de faire une dernière observation. Bien que l'on ait, pour éviter trop de distinctions préalables, appelé $\mathbb{N}$ « ensemble », il est à proprement parler plus qu'un ensemble, au sens où il ne consiste pas en la simple collection de certains éléments. La caractérisation de $\mathbb{N}$ fait intervenir d'emblée une application $(-)'$ définie sur ses éléments, à partir de laquelle il sera facile, comme on le verra dans le paragraphe suivant, de définir un ordre pour ces éléments. Pourtant, une fois que $\mathbb{N}$ a été caractérisé par le biais des cinq axiomes de Peano, on peut faire abstraction de l'application $(-)'$ et ne considérer que l'ensemble de ses éléments, indépendamment de toute fonction ou relation définie sur eux. Pour plus de clarté, on pourrait noter « N » l'ensemble des éléments de $\mathbb{N}$, considérés sans égard à l'application $(-)'$ définie sur eux, en réservant l'usage du symbole « $\mathbb{N}$ » pour indiquer la donnée de cet ensemble et de l'application $(-)'$ définie sur ses éléments.

## 2. Ordre des nombres naturels

Dans le chapitre 1, on a parlé d'une manière informelle d'ordre, en se bornant à suggérer l'idée que les nombres entiers positifs forment un système ordonné, parce que pour tout couple de nombres entiers positifs distincts, $n$ et $m$, on peut dire lequel précède l'autre. On a aussi parlé, de manière également informelle, de classes d'équivalence. Ici, il faut commencer à être plus précis. On va d'abord poser les définitions suivantes :

Définition 2.1. *Une relation binaire* $\mathbf{R}$ *est dite « relation d'équivalence » sur un ensemble* $E$*, si et seulement si :*

**(*i*):** *elle est réflexive sur* $E$ *; c'est-à-dire que pour tout* $x$ *appartenant à* $E$*,* $x\mathbf{R}x$ *;*

**(*ii*):** *elle est symétrique sur* $E$ *; c'est-à-dire que pour tout* $x$ *et* $y$ *appartenant à* $E$ *: si* $x\mathbf{R}y$ *alors* $y\mathbf{R}x$ *;*

**(*iii*):** *elle est transitive sur* $E$*, c'est-à-dire pour tout* $x$*,* $y$*,* $z$ *appartenant à* $E$ *: si* $x\mathbf{R}y$ *et* $y\mathbf{R}z$*, alors* $x\mathbf{R}z$*.*

L'identité est évidemment une relation d'équivalence, même si elle n'est pas la seule. Dans le chapitre 1 (p. 4), on a observé qu'une relation d'équivalence est une relation qui s'établit entre des objets lorsque ceux-ci sont tels qu'ils ne peuvent pas être distingués lorsqu'ils ne sont considérés que sous un certain aspect. On peut même dire que des objets sont entre eux dans une relation d'équivalence lorsqu'ils peuvent être au moins partiellement caractérisées en faisant référence à une identité, par example lorsqu'ils partagent une même propriété ou sont en la même relation avec le même objet. La définition de relation d'équivalence ne fait ainsi que généraliser les conditions logiques propres à la relation d'identité qui est sous-jacente à toute relation d'équivalence.

Définition 2.2. *Une relation binaire* $\mathbf{R}$ *est dite « relation d'ordre strict » sur un ensemble* $E$*, si et seulement si :*

**(*i*):** *elle est anti-réflexive sur* $E$ *; c'est-à-dire qu'il n'y a pas de* $x$ *appartenant à* $E$*, tel que* $x\mathbf{R}x$ *;*

**(*ii*):** *elle est transitive sur* $E$*.*

Remarque 2.7. On observe que si, pour quelques $x$ et $y$ appartennant à $E$, on avait en même temps $x\mathbf{R}y$ et $y\mathbf{R}x$, $\mathbf{R}$ étant une relation d'ordre strict, alors, grâce à la transitivité de cette relation, on aurait aussi $x\mathbf{R}x$, ce qui ne peut pas être le cas, car une relation d'ordre strict est anti-réflexive. Il s'ensuit qu'une relation d'ordre strict est nécessairement telle que pour tout $x$ et $y$ appartenant à $E$, si $x\mathbf{R}y$, alors il n'est pas le cas que $y\mathbf{R}x$.

Il est facile de voir que la relation $<$ définie dans la définition 2.2 du chapitre 1 est une relation d'ordre strict.

Considérons maintenant l'ensemble des nombres entiers strictement positifs, et les relations $<$ et $=$ définies sur cet ensemble, et définissons, à partir de ces relations, une troisième relation « $\leq$ », telle que lorsque $x$ et $y$ appartiennent à cet ensemble, alors $x \leq y$ si et seulement si : soit $x = y$, soit $x < y$. Il n'est pas difficile de vérifier qu'une telle relation est réflexive et transitive sur l'ensemble des nombres entiers strictement positifs, et qu'elle est telle que si $x$ et $y$ sont deux éléments de cet ensemble tels que $x \leq y$, et $y \leq x$, alors $x = y$. On l'appellera « relation d'ordre ».

Pour généraliser la définition, imaginons qu'une relation d'ordre strict $\prec$ soit définie sur les éléments d'un ensemble $E$, et que cette relation soit telle que pour tout couple d'éléments distincts de $E$, $x$ et $y$, si ce n'est pas le cas que $x \prec y$, alors il est le cas que $y \prec x$ (qu'on note que comme des conditions $y \prec x$ et $x \prec y$ il s'ensuivrait, d'après la transitivité de $\prec$, que $y \prec y$, contre la condition de anti-réflexivité de $\prec$, de la il s'ensuit aussi que si $y \prec x$, alors ce n'est pas le cas que $x \prec y$). On peut alors définir, à partir de cette relation, une relation d'équivalence $\approx$ de la manière suivante : si $x$ et $y$ sont deux éléments de $E$, alors $x \approx y$ si et seulement s'il n'est le cas ni que $x \prec y$, ni que $y \prec x$. Le lecteur pourra vérifier par lui-même que la relation $\approx$ ainsi définie est une relation d'équivalence. Une fois qu'on a définie ainsi la relation d'équivalence $\approx$ sur $E$, on peut énoncer la condition d'anti-symétrie comme il suit :

une relation $\mathbf{R}$ est anti-symétrique sur $E$ lorsque, pour tout $x$ et $y$ appartenant à $E$, si $x\mathbf{R}y$ et $y\mathbf{R}x$ alors $x \approx y$.

Si l'ensemble $E$ sur lequel on travaille est tel qu'on ait définit sur lui, indépendamment de tout relation d'ordre strict, une relation d'égalité (qui peut éventuellement coïncider avec une simple identité) notée « $=$ », et que l'on estime qu'une relation d'ordre puisse être définie sur $E$ à partir de cette égalité, alors on pourra définir la condition d'anti-symétrie pour une relation définie sur $E$, indépendamment de la considération de toute relation d'ordre strict définie sur $E$. Cela se fera ainsi : une relation $\mathbf{R}$ est anti-symétrique sur $E$ lorsque, pour tout $x$ et $y$ appartennant à $E$, si $x\mathbf{R}y$ et $y\mathbf{R}x$ alors $x = y$.

Cette deuxième démarche est celle généralemment utilisée par les mathématiciens. Dans un cas comme dans l'autre, la caractérisation de la condition de anti-symétrie pour une relation définie sur $E$ permet de dire en général ce qu'on entend comme une relation d'ordre sur un ensemble $E$ :

Définition 2.3. *Une relation binaire* $\mathbf{R}$ *est dite « relation d'ordre » sur* $E$*, si et seulement si :*

**(*i*):** *elle est réflexive sur* $E$ *;*

**(*ii*):** *elle est anti-symétrique sur* $E$ *;*

**(*iii*):** *elle est transitive sur* $E$*.*

On conclura alors que la relation '$<$ ou $=$' (notée généralement « $\leq$ » ), définie sur l'ensemble des nombres entiers positifs (tels qu'ils ont été définis dans le chapitre 1) est une relation d'ordre.

En se réclamant des définitions 2.1 et 2.3, on peut préciser ce qu'on entend par « ensemble ordonné ». On dit généralement qu'un ensemble $E$ est ordonné s'il est muni d'une relation d'ordre. Cependant, l'expression « être muni d'une relation d'ordre » peut apparaitre ambiguë ou vague. Ce que cette définition rend pourtant clair est que la propriété d'être ordonné, prédiquée d'un ensemble, ne dépend pas tout simplement de la nature de cet ensemble. Un ensemble ne résulte ordonné que si l'on a défini sur les éléments de cet ensemble une relation d'ordre, dont la donnée n'est généralement pas concomitante à la donnée de l'ensemble lui-même. Considérons l'ensemble des nombres entiers positifs tels qu'ils ont été définis dans le chapitre 1. Bien que la manière par laquelle ces nombres ont été définis rende très naturel de définir sur ces mêmes nombres une relation d'ordre, ce n'est qu'après que cette relation ait été définie, et relativement à cette même relation, que cet ensemble est ordonné. Quelque chose de similaire peut être dit pour l'ensemble des nombres naturels, bien que les éléments de cet ensemble ne soient pas donnés un à la fois — comme cela a été en revanche le cas des éléments de l'ensemble des nombres entiers positifs, en tant qu'ils ont été définis dans le chapitre 1 — mais tous à la fois et en se réclamant de l'application $(-)'$. En effet, ce ne sera qu'après qu'on a défini, en se réclamant de l'application $(-)'$, une relation d'ordre sur les nombres naturels, qu'on pourra dire que l'ensemble des nombres naturels est ordonné, relativement à cette relation d'ordre. La manière la plus simple pour exprimer cette situation sans ambiguïté est de considérer un ensemble ordonné comme un couple donné par un ensemble et d'une relation d'ordre définie sur cet ensemble. Pour exprimer la fait que un certain ensemble $E$ et une certaine relation d'ordre $\mathbf{R}$ forment un ensemble ordonnée, on dira alors que $E$ est ordonné relativement à $\mathbf{R}$, ou même que le couple $< E, \mathbf{R} >$ est un ensemble ordonné, ou enfin que $\mathbf{R}$ est un ordre sur $E$. On aura alors, pour plus de précision, la définition suivante :

Définition 2.4. *Un ensemble* $E$ *est dit « ordonné relativement à la relation* $\mathbf{R}$ *» (ou un couple* $< E, \mathbf{R} >$ *est dit un « ensemble ordonné », ou* $\mathbf{R}$ *un « ordre » sur* $E$*) si et seulement si la relation* $\mathbf{R}$ *est une relation d'ordre sur* $E$ *; et, pour tout couple d'éléments de* $E$ $x$ *et* $y$*, il est*

*possible de dire si* $x\mathbf{R}y$ *ou non, en symboles :*

$$x, y \in E \Rightarrow [(x\mathbf{R}y) \vee \neg (x\mathbf{R}y)]$$

Cette définition ne règle pas encore la question, car il est clair que quand nous pensons à l'ordre des nombres entiers positifs nous pensons à une condition plus forte : nous pensons que si $x$ et $y$ sont des nombres entiers positifs, distincts entre eux, alors, soit $x$ précède $y$, soit $y$ précède $x$. Nous sommes donc amenés à distinguer entre les deux notions dont relèvent les définitions suivantes :

DÉFINITION 2.5. *Un ensemble* $E$ *est dit « totalement ordonné relativement à la relation* $\mathbf{R}$ *» (ou un couple* $< E, \mathbf{R} >$ *est dit un « ensemble totalement ordonné », ou* $\mathbf{R}$ *un « ordre total sur* $E$ *» ) si et seulement si la relation* $\mathbf{R}$ *est une relation d'ordre sur* $E$ *; et, pour tout couple d'éléments de* $E$ $x$ *et* $y$*, soit* $x\mathbf{R}y$*, soit* $y\mathbf{R}x$*, en symboles :*

$$x, y \in E \Rightarrow [(x\mathbf{R}y) \vee (y\mathbf{R}x)]$$

DÉFINITION 2.6. *Un ensemble* $E$ *est dit « partiellement ordonné relativement à la relation* $\mathbf{R}$ *» (ou un couple* $< E, \mathbf{R} >$ *est dit un « ensemble partiellement ordonné », ou* $\mathbf{R}$ *un « ordre partiel sur* $E$ *» ) si et seulement si la relation* $\mathbf{R}$ *est une relation d'ordre sur* $E$ *; et il y a en* $E$ *un couple d'éléments* $x$ *et* $y$*, tel que* $x\mathbf{R}y$*, et un couple d'éléments* $v$ *et* $w$*, tel que ni* $v\mathbf{R}w$*, ni* $w\mathbf{R}v$*, en symboles :*

$$\exists x, y, v, w \in E \text{ tels que } [(x\mathbf{R}y) \wedge \neg (v\mathbf{R}w) \wedge \neg (w\mathbf{R}v)]$$

REMARQUE 2.8. Une relation d'ordre habituelle en logique et en mathématiques est la relation d'inclusion entre ensembles, notée généralement par le symbole « $\subseteq$ » : elle a lieu entre deux ensembles $D$ et $E$ si et seulement si $D$ est inclus dans $E$ (qu'on note la différence entre le fait d'être inclus dans un ensemble et le fait d'appartenir à un ensemble : $x$ appartient à l'ensemble $E$ si et seulement si $x$ est un élément de $E$, tandis qu'un ensemble $D$ est inclus dans un ensemble $E$ si et seulement si $D$ est un sous-ensemble de $E$). Soit alors $E$ un ensemble d'ensembles, par exemple l'ensemble composé par les ensembles $\mathfrak{X} = \{a, b\}$, $\mathfrak{Y} = \{a, c, d\}$ et $\mathfrak{Z} = \{b\}$, c'est-à-dire :

$$E = \left\{ \begin{array}{l} \mathfrak{X} = \{a, b\} \\ \mathfrak{Y} = \{a, c, d\} \\ \mathfrak{Z} = \{b\} \end{array} \right\}$$

où $a, b, c, d$ sont des objets quelconques. Il est facile de voir que le couple $< E, \subseteq >$ est un ensemble partiellement ordonné, car : $\mathfrak{Z} \subseteq X$ et ni $\mathfrak{Z} \subseteq Y$, ni $\mathfrak{Y} \subseteq Z$.

Si $E$ est un ensemble quelconque, dont les éléments ne sont pas des nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, alors le couple $< E, \leq >$ (où $\leq$ est la relation d'ordre qu'on a définie dans le chapitre 1, relativement aux nombres entiers positifs), n'est pas un ensemble ordonné. En revanche, si $\mathfrak{N}$ est l'ensemble des nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, alors le couple $< \mathfrak{N}, \leq >$ est un ensemble totalement ordonné.

Ci-dessus, on a dit que, en se réclamant de l'application $(-)'$ qui intervient dans les axiomes de Peano, il est facile de définir une relation d'ordre sur l'ensemble $\mathbb{N}$ des nombres naturels. Les définitions précédentes nous permettent de comprendre ce que cela signifie : l'application $(-)'$ induit tout naturellement un ordre, et en particulier un ordre total sur l'ensemble des objets qu'elle contribue à définir (c'est-à-dire les nombres naturels). En fait, si $x$ est un nombre naturel, alors il peut s'écrire sous la forme $\underbrace{(\ldots((\alpha)'}_{\ldots})'_{\ldots})'$, c'est-à-dire qu'il est le successeur du successeur, du successeur,... de $\alpha$. Ainsi, il est facile (et naturel) d'associer tout nombre naturel

à une chaîne de nombres naturels, et en particulier à la chaîne induite par l'application $(-)'$, qui commence par $\alpha$ et qui termine avec ce nombre. La chaîne associée au nombre $((\alpha')')'$ sera par exemple celle-ci : $\{\alpha, \alpha', (\alpha')', ((\alpha')')'\}$. Si $n$ est un nombre naturel, on notera la chaîne des nombres naturels qui lui est associée par le symbole « $\mathcal{S}_n$ ». Il est alors clair que toute chaîne définie de cette manière est un ensemble de nombres naturels. La définition suivante est alors immédiate :

DÉFINITION 2.7. *On dira que le nombre naturel $n$ est inférieur ou égal au (ou plus petit ou égal que le) nombre naturel $m$, ce qu'on notera « $n \leq m$ » (ou que le nombre naturel $m$ est plus grand ou égal au nombre naturel $n$, ce qu'on notera « $m \geq n$ » ) si et seulement si $n$ appartient à la chaîne $\mathcal{S}_m$ associée à $m$ ; en symboles :*

$$n, m \in \mathbb{N} \Rightarrow [(n \leq m) \Leftrightarrow (n \in \mathcal{S}_m)]$$

Il est facile de voir que cette définition est équivalente à la suivante :

$$n, m \in \mathbb{N} \Rightarrow [(n \leq m) \Leftrightarrow (\mathcal{S}_n \subseteq \mathcal{S}_m)]$$

qui, au lieu de s'appuyer sur la relation d'appartenance entre un élément et un ensemble, s'appuie sur la relation d'inclusion entre deux ensembles.

REMARQUE 2.9. Qu'on remarque l'usage particulier qu'on fait ici de la constante logique « $\Leftrightarrow$ ». À gauche de cette constante on fait apparaître une expression dont on ne connaît pas encore la signification et qui est justement définie par la relation de double implication qui la lie à l'expression qui apparaît à droite de cette constante. La symétrie logique de la double implication s'accompagne donc ici d'une asymétrie épistémologique, car, si le symbole « $\Leftrightarrow$ » assure l'équivalence des conditions exprimées par les deux expressions qui se rangent de ses deux côtés, d'un point de vue épistémologique ces conditions sont essentiellement distinctes : celle de gauche est celle qu'on doit définir, et qu'on est justement en train de définir — le *definiendum*, comme on le dit d'habitude en se réclamant d'un gérondif latin — celle de droite est celle qui fournit cette définition — le *definiens*, comme on l'appelle, en se réclamant cette fois d'un participe latin. Dans certains textes, on souligne cette situation en employant dans ces cas, à la place du symbole « $\Leftrightarrow$ », le symbole « $=_{df}$ » qu'on lit généralement « ... est égal par définition à ... ». Lorsque la définition en question fait partie d'une exposition discursive d'une théorie, cette deuxième convention est certainement plus propre. Mais si la définition sert comme prémisse pour des déductions formelles faisant intervenir la syntaxe habituelle des constantes logiques, alors une telle convention ne garantit une définition convenable qu'à condition qu'on s'accorde pour substituer (au moins mentalement) au symbole « $=_{df}$ » le symbole « $\Leftrightarrow$ », lors de la déduction. Elle relève donc d'une distinction qui demande à être éliminée tout de suite après avoir été introduite.

Cette différence entre exposition discursive et déduction formelle dépend de la nature propre d'une déduction formelle : en tant que telle, celle-ci ne porte pas en effet sur les conditions que les symboles qui y interviennent expriment, mais sur ces symboles eux-mêmes ; comme on le dit habituellement, elle relève de la syntaxe de ces symboles et non pas de leur sémantique. Et, si ceci est le cas, comme ce sera souvent le cas par la suite, la différence épistémologique qu'on a remarquée cesse d'être pertinente. C'est pourquoi j'ai préféré utiliser ici le symbole « $\Leftrightarrow$ », plutôt que le symbole « $=_{df}$ ».

En partant de la définition 2.7, il est facile de démontrer le théorème suivant :

THÉORÈME 2.1. *La relation $\leq$ est une relation d'ordre sur $\mathbb{N}$.*

**Preuve** Supposons que $n$, $m$ et $p$ sont trois nombres naturels.

*i*) Comme $n \in \mathcal{S}_n$, il s'ensuit que $n \leq n$ et la relation $\leq$ est ainsi réflexive sur $\mathbb{N}$.

*ii*) Supposons que $n \neq m$ et $n \leq m$. Alors $n \in \mathcal{S}_m$ et donc :

$$\begin{aligned} \mathcal{S}_m &= \{\alpha, \alpha', ..., n, ..., m\} \\ \mathcal{S}_n &= \{\alpha, \alpha', ..., n\} \end{aligned}$$

Mais si on suppose aussi que $m \leq n$, ceci est impossible, car de cette dernière condition il s'ensuit que $m \in \mathcal{S}_n$ et donc

$$\mathcal{S}_n = \{\alpha, \alpha', ..., m, ..., n\}$$

Donc, si $n$ et $m$ sont deux nombres distincts, il n'est pas possible qu'il soit en même temps le cas que $n \leq m$ et $m \leq n$. Donc si $n \leq m$ et $m \leq n$, alors $n = m$ et la relation $\leq$ est ainsi anti-symétrique sur $\mathbb{N}$.

*iii*) si $n \leq m$ et $m \leq p$, alors $n \in \mathcal{S}_m$ et $m \in \mathcal{S}_p$ et donc $n \in \mathcal{S}_p$ et par conséquent $n \leq p$ ; la relation $\leq$ est donc transitive sur $\mathbb{N}$. □

REMARQUE 2.10. Le symbole « $x \neq y$ » intervient ici et dans la suite, quels que soient $x$ et $y$, comme une abréviation, pour indiquer qu'il n'est pas le cas que $x = y$. La relation $\neq$ ne doit donc pas être prise comme une relation nouvelle qu'on n'aurait pas définie.

Le théorème 2.1 suggère la définition suivante :

DÉFINITION 2.8. *On dira que le nombre naturel n est inférieur au (ou plus petit que le) nombre naturel m, ce qu'on notera :« $n < m$ », (ou que le nombre naturel m est plus grand que le nombre naturel n, ce qu'on notera « $m > n$ » ) si et seulement si $n \leq m$ et $n \neq m$.*

De la définition 2.8, il est facile de démontrer le théorème suivant, dont la preuve est laissée comme exercice au lecteur :

THÉORÈME 2.2. *La relation $<$ est une relation d'ordre strict sur $\mathbb{N}$.*

Le théorème 2.1 ayant été démontré, il sera aussi facile de prouver le théorème suivant :

THÉORÈME 2.3. *$\mathbb{N}$ est totalement ordonné relativement à $\leq$ (ou, si on préfère : $< \mathbb{N}, \leq >$ est un ensemble totalement ordonné ; ou encore : $\leq$ est un ordre total sur $\mathbb{N}$).*

**Preuve** Le théorème 2.1 nous assure que $\leq$ est une relation d'ordre sur $\mathbb{N}$. Il suffit alors de montrer que pour tous $n$ et $m$ appartenant à $\mathbb{N}$, soit $n \leq m$, soit $m \leq n$. On fait alors l'hypothèse que ce ne soit pas le cas que $n \leq m$, c'est-à-dire que $n$ n'appartienne pas à $\mathcal{S}_m$. Pour prouver le théorème, il suffit alors de montrer que $m$ appartient à $\mathcal{S}_n$ et donc $m \leq n$. Or, il est clair que si $n$ n'appartient pas à $\mathcal{S}_m$, alors on peut arriver à $m$, en partant de $\alpha$, et en passant à chaque étape du nombre considéré à son successeur, sans passer par $n$. Mais comme les nombres naturels forment une progression relativement à la relation de successeur, cela signifie que pour arriver à $n$, en partant de $\alpha$ et en passant à chaque étape du nombre considéré à son successeur, il faut passer par $m$, donc : $m \in \mathcal{S}_n$. □

REMARQUE 2.11. La preuve précédente fait évidemment usage de l'équivalence entre la condition $A \vee B$ et la condition $\neg A \Rightarrow B$, quelles que soient les conditions $A$ et $B$.

Si le théorème 2.3 nous garantit que pour n'importe quel couple de nombres naturels $n$ et $m$, soit $n \leq m$ soit $m \leq n$, il ne nous dit pas, deux nombres naturels quelconques $n$ et $m$ étant donnés, si $n \leq m$ ou $m \leq n$. La définition 2.8 est pourtant telle qu'il n'est pas difficile de déterminer, dans chaque cas particulier, laquelle de ces deux conditions est satisfaite. Il sera d'abord facile de démontrer le théorème suivant :

THÉORÈME 2.4. *Si n et m sont des nombres natreturels, alors :*

**(*i*):** $\alpha \leq n$ ;

**(*ii*):** *si* $n \leq m$, *alors* $n < m'$.

**Preuve** Pour ce qui est de $(i)$, il suffit d'observer que, quel que soit le nombre naturel $n$, $\alpha \in \mathcal{S}_n$ et donc $\alpha \leq n$. La preuve n'est pas plus difficile pour $(ii)$, car si $n \leq m$, alors $n \in \mathcal{S}_m$, mais, quel que soit le nombre naturel $m$,

$$\begin{aligned} \mathcal{S}_m &= \{\alpha, \alpha', (\alpha')', ..., m\} \\ \mathcal{S}_{m'} &= \{\alpha, \alpha', (\alpha')', ..., m, m'\} \end{aligned}$$

et donc $\mathcal{S}_m \subseteq \mathcal{S}_{m'}$, et, par conséquent, $n \in \mathcal{S}_{m'}$, c'est-à-dire $n \leq m'$. D'autre part, si $n = m'$, alors $n$ n'appartient pas à $\mathcal{S}_m$ et donc il n'est pas le cas que $n \leq m$, de sorte que si $n \leq m$, alors il n'est pas le cas que $n = m'$ et donc, par la définition, 2.8, $n < m'$. □

En exploitant ce théorème, il est ensuite facile de décider, pour tout couple de nombres naturels $n$ et $m$ si $n \leq m$ ou $m \leq n$. Par exemple, il suffit de poser $n = \alpha'$, pour tirer de ce théorème que $\alpha < \alpha'$. De là, comme $\alpha' \leq \alpha'$, il s'ensuit que $\alpha < \alpha' < (\alpha')'$ et, donc, par la transitivité de $<$, $\alpha < (\alpha')'$. En continuant à raisonner de cette manière on parviendra aisément à la conclusion suivante :

$$\alpha < \alpha' < (\alpha')' < ((\alpha')')' < (((\alpha')')')' < ... \tag{2}$$

d'où il est facile de conclure que, quel que soit le nombre naturel $n$, $n < n'$. On arrive également à cette même conclusion en raisonnant par l'absurde (des considérations générales sur la nature logique et la légitimité des preuves par l'absurde seront présentées dans le chapitre 6). Imaginons que ce n'est pas le cas que $n < n'$, alors, d'après la clause $(ii)$ du théorème 2.4, ce ne peut pas être le cas que $n \leq n$, mais $n = n$ et donc $n \leq n$. Il s'ensuit qu'il n'est pas possible que ce ne soit pas le cas que $n < n'$, donc, quel que soit le nombre naturel $n$, il faudra que $n < n'$.

Démontrer le théorème suivant sera également facile :

THÉORÈME 2.5. *Si* $n$ *est un nombre naturel, alors il n'y a pas de* $m \in \mathbb{N}$ *tel que* $n < m < n'$.

**Preuve** Quels que soient les nombres naturels $n$ et $m$, si $n < m$, alors $n \in \mathcal{S}_m$ et $n \neq m$ et si $m < n'$, alors $m \in \mathcal{S}_{n'}$ et $m \neq n'$. Or,

$$\begin{aligned} \mathcal{S}_m &= \{\alpha, \alpha', (\alpha')', ..., m\} \\ \mathcal{S}_{n'} &= \{\alpha, \alpha', (\alpha')', ..., n, n'\} \end{aligned}$$

et ainsi, si $n < m$, alors

$$\mathcal{S}_m = \{\alpha, \alpha', (\alpha')', ..., n, ..., m\}$$

et si $m < n'$

$$\mathcal{S}_{n'} = \{\alpha, \alpha', (\alpha')', ..., m, ..., n'\}$$

Mais, comme $n'$ suit immédiatement $n$ dans toutes les chaînes qui contiennent $n$ et $n'$, ce ne peut être le cas, et donc ce n'est pas possible, quels que soient les nombres naturels $n$ et $m$, que $n < m < n'$. □

Dans le chapitre 4, on verra que cela revient à dire que l'ensemble $\mathbb{N}$ n'est pas « dense » relativement à la relation $\leq$ : ce n'est pas vrai qu'on puisse, pour tout couple de nombres naturels, trouver un nombre naturel autre que ceux-ci, qui soit compris entre ces deux nombres selon la relation $\leq$. On comprendra plus tard la signification profonde de cette circonstance.

REMARQUE 2.12. La manière dans laquelle on a défini ci-dessus la relation $\leq$ sur $\mathbb{N}$ peut paraître insatisfaisante dans le contexte d'une théorie axiomatique telle qu'est celle que l'on vise ici à présenter. Quel que soit le nombre naturel $n$, on ne peut en effet supposer que l'on ait bien définie la chaîne $\mathcal{S}_n$ qui lui est associée qu'à condition d'admettre qu'on sache

raisonner sur le système formé par les conséquences des axiomes de Peano. Si on ne savait pas douter qu'on sache le faire, on peut vouloir se limiter, dans la présentation d'une théorie axiomatique des nombres entiers, à ne considérer que des relations parmi ces nombres qui peuvent être définies en restant à l'intérieur de ce système. Il y a différentes manières de satisfaire cette exigence.

Une de celles-ci, empruntée à la définition des nombres entiers positifs donnée par Frege (cf. la note 1.2), fait usage de ce qu'on qualifie en logique d'ancestrale d'une relation donnée. Si $\mathbf{R}$ est une relation binaire dont on suppose qu'elle a déjà été définie, on qualifie d'ancestrale de cette relation une autre relation binaire, habituellement notée « $\mathbf{R}^*$ », définie à partir de $\mathbf{R}$, et telle que que $x\mathbf{R}^*y$ si et seulement si $y$ possède toutes les propriétés $\mathbf{R}$-héréditaires qui $x$ possède, c'est-à-dire que du fait qu'une propriété est $\mathbf{R}$-héréditaire et que $x$ la possède, il s'ensuit que $y$ la possède aussi. Une propriété est dite à son tour $\mathbf{R}$-héréditaire ou héréditaire relativement à $\mathbf{R}$ si tout couple d'objets $x$ et $y$ sur lesquels $\mathbf{R}$ est définie, qui soient tels que $x\mathbf{R}y$, sont aussi tels que du fait que $x$ possède cette propriété il s'ensuit que $y$ la possède également. Prenons la relation '(être) père' et supposons que Jean soit le père de Pierre. Du fait que Jean est un humain, il s'ensuit que Pierre l'est aussi. Donc la propriété '(être) humain' est héréditaire relativement à la relation '(être) père'. Elle n'est pas la seule ; la propriété '(être) bipède' est par exemple héréditaire relativement à la relation '(être) père'. Supposons maintenant que $y$ soit tel que du fait qu'une propriété soit $\mathbf{R}$-héréditaire et que Jean la possède, il s'ensuit que $y$ la possède aussi. Jean est alors lié à $y$ par l'ancestrale de la relation '(être) père', qu'on pourrait vraisemblablement identifier avec la relation '(être) ancêtre' (d'où le terme « ancestrale » dérive par synecdoque).

L'idée est alors de définir la relation d'ordre stricte $<$ sur les nombres naturels comme l'ancestral de la relation '(être) prédécesseur', c'est-à-dire la relation qui lie tout nombre naturel $n$ à son successeur $n'$, puis passer de là à la relation d'ordre $\leq$ en ajoutant la condition d'égalité. On commence alors par définir la relation '(être) prédécesseur' sur $\mathbb{N}$ comme il suit : si $n, m \in \mathbb{N}$ alors $n$ est le prédécesseur de $m$ (en symboles : $n\mathbf{P}m$) si et seulement si $m = n'$. Puis on définit l'ancestrale de cette relation comme il suit : si $n, m \in \mathbb{N}$ alors $n\mathbf{P}^*m$ si et seulement si

$$\mathcal{G} \subseteq \mathbb{N} \Rightarrow \left[ \left( \begin{array}{c} \mu \in \mathbb{N} \Rightarrow [n\mathbf{P}\mu \Rightarrow \mu \in \mathcal{G}] \wedge \\ \nu, \mu \in \mathbb{N} \Rightarrow [(\nu\mathbf{P}\mu \wedge \nu \in \mathcal{G}) \Rightarrow \mu \in \mathcal{G}] \end{array} \right) \Rightarrow n \in \mathcal{G} \right]$$

Enfin, on définit la relation d'ordre $\leq$ comme il suit : si $n, m \in \mathbb{N}$ alors $n \leq m$ si et seulement si $n\mathbf{P}^*m$ ou $n = m$. Le lecteur motivé pourra s'exercer à montrer que de cette définition suivent les théorèmes 2.1-2.5.

Si dans la présentation précédente on n'a pas suivi ce parcours ce n'est que pour éviter d'introduire trop des difficultés. C'est pourtant du fait qu'un tel parcours, ou d'autres analogues, sont possibles qu'il s'en suit que le parcours qu'on a suivi est légitime et tant que raccourci d'un parcours plus difficile, mais plus propre.

Remarque 2.13. Avant de conclure le présent paragraphe, deux remarques me semblent nécessaires. D'abord, il convient de noter que dans la théorie de Peano, on a suivi l'ordre inverse de celui de la théorie des nombres entiers positifs exposée dans le chapitre 1. Tandis que dans cette dernière théorie on est passé de la relation d'ordre strict $<$ à la notion de successeur, on est passé ici de la relation de successeur à la relation d'ordre $\leq$. Ensuite, on observera que dans le chapitre 1, on n'a parlé de l'ensemble des nombres entiers positifs que pour se référer à un ensemble d'objets d'une nature particulière (l'ensemble des collections de traits verticaux, ou, pour être plus précis, de leurs classes d'équivalence sous la relation d'égalité), dont on a exhibé certains exemplaires. Ici on a en revanche présenté l'ensemble

$\mathbb{N}$ avant de spécifier la nature de ses éléments (et même sans spécifier du tout cette nature) et avant d'en exhiber un seul (car il est clair que, pris isolément, le symbole « $\alpha$ » ne renvoie pas à un nombre naturel et n'est qu'un symbole vide de signification). Il me semble possible de résumer ces deux observations dans l'affirmation suivante : la présentation des nombres entiers positifs réalisée dans le chapitre 1 est une présentation constructive, et ne demande pas que l'ensemble de ces nombres soit présenté d'emblée comme un ensemble sur lequel est définie une application qui, comme on l'a vu, induit un ordre ; en revanche, la présentation des nombres naturels selon l'axiomatique de Peano est une présentation corrélative et, comme telle, elle exhibe d'emblée l'ensemble des nombres naturels, et l'exhibe comme un ensemble sur lequel est définie une application qui, comme on l'a vu, induit un ordre (cf. note 1.4). Si l'on insiste sur le deuxième aspect de cette distinction, on dira alors que l'exposition du chapitre 1 présente les nombres entiers positifs comme des cardinaux, tandis que l'axiomatique de Peano présente directement les nombres naturels comme des ordinaux.

## 3. L'addition et la multiplication sur les nombres naturels et leurs opérations inverses

D'après la définition donnée ci-dessus, les nombres naturels ne sont que les éléments d'une certaine progression qu'on ne caractérise que par l'acte consistant à nommer son élément générateur et l'application qui induit la génération. On ne pourra donc définir aucune opération sur ces nombres, en se réclamant de la nature particulière de ses éléments, comme on l'a fait dans le chapitre 1, pour les nombres entiers positifs. La seule possibilité que nous ayons est de définir l'addition et la multiplication sur les nombres naturels, en nous réclamant de l'application $(-)'$ qui conduit de chaque nombre naturel à son successeur.

Avant de montrer comment cela est possible, une prémisse est nécessaire : la recherche d'une définition de l'addition et de la multiplication ne vise, dans le contexte de la théorie de Peano, qu'à définir sur $\mathbb{N}$ deux applications de $\mathbb{N}^2$ —l'ensemble de tous les couples possibles d'éléments de $\mathbb{N}$ — vers $\mathbb{N}$ lui-même, qui se comportent relativement aux nombres naturels exactement comme l'addition et la multiplication, définies sur les nombres entiers positifs tels qu'ils ont été définis dans le chapitre 1, se comportent relativement à ces derniers nombres. Cela signifie que si $n$, $m$ et $p$ sont trois collections de traits verticaux et $\chi(n)$, $\chi(m)$ et $\chi(p)$ sont les nombres naturels associés à $n$, $m$ et $p$ par une bijection $\chi$ qui conserve toutes les propriétés d'ordre, alors il faut que l'addition et la multiplication définies sur $\mathbb{N}$ soient telles que :

$$\begin{array}{l} \chi(n) + \chi(m) = \chi(p) \text{ si et seulement si } n + m = p \\ \chi(n) \cdot \chi(m) = \chi(p) \text{ si et seulement si } n \cdot m = p \end{array} \tag{3}$$

Ces conditions ne peuvent cependant pas entrer dans la définition cherchée, car cela conduirait à définir des opérations sur $\mathbb{N}$ en fonction des propriétés d'autres opérations définies sur les collections de traits verticaux, ce qui rendrait la théorie de Peano dépendante de la théorie développée dans le chapitre 1. Les conditions (3) ne doivent donc être pensées que comme des conséquences auxquelles les définitions données doivent conduire, et ne pourront être vérifiées qu'*a posteriori*, une fois qu'on pourra comparer les deux théories complètement constituées.

Remarque 2.14. Voici un autre bel exemple de ce qu'on a ci-dessus qualifié de dialectique intrinsèque à toute formalisation

Les nombreuses remarques contenues à ce propos dans le chapitre 1 devraient avoir convaincu le lecteur des avantages pratiques qui dérivent du fait qu'on considère la collection vide comme un nombre et qu'on inclut donc le zéro dans l'ensemble des nombres entiers positifs. Cela incite

à se demander s'il est possible d'intégrer dans l'ensemble des nombres naturels un nombre qui se comporte face aux autres nombres naturels comme se comporte la collection vide face aux autres collections de traits verticaux. C'est facile : il suffit de considérer l'élément $\alpha$ de $\mathbb{N}$ comme le correspondant, dans cet ensemble, de la collection vide. Cela nous suggère de poser d'emblée les conditions suivantes :

$$(4) \qquad \begin{array}{rcl} n & \in & \mathbb{N} \Rightarrow n + \alpha = n \\ n & \in & \mathbb{N} \Rightarrow n \cdot \alpha = \alpha \end{array}$$

Observons maintenant que dans la preuve du théorème 1.1 on a identifié la relation $\mathbf{P}$ qui intervient dans la définition d'une progression $\mathfrak{P}$ avec la relation qui intervient entre tout nombre entier et positif $n$ et son successeur $\sigma(n)$ et qu'ensuite, pour montrer, lors du théorème 1.2, que toute progression satisfait aux conditions qui nous ont données les cinq axiomes de Peano, on a défini l'application $(-)'$ comme une application qui associe tout élément $x$ de $\mathfrak{P}$ à l'élément $y$ de $\mathfrak{P}$ tel que $x\mathbf{P}y$. Cela nous suggère d'ajouter aux conditions (4) les conditions suivantes, attestant que l'addition et la multiplication sur $\mathbb{N}$ se comportent relativement à $\alpha'$ comme l'addition et la multiplication sur l'ensemble des nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, se comportent relativement à $\sigma(\emptyset) = \{|\}$ :

$$(5) \qquad \begin{array}{rcl} n & \in & \mathbb{N} \Rightarrow n + \alpha' = n' \\ n & \in & \mathbb{N} \Rightarrow n \cdot \alpha' = n \end{array}$$

On pourrait espérer que ces conditions suffisent pour définir l'addition et la multiplication sur la totalité des nombres naturels, par récurrence, c'est-à-dire en exploitant les possibilités concédées par l'axiome 5 de Peano. Il est pourtant facile de voir qu'il n'en est pas ainsi. L'argument qui suit nous montre comment on peut raisonner pour se convaincre de cette insuffisance ; je ne considère ici que l'exemple de l'addition ; pour la multiplication, on pourra raisonner de manière analogue. Qu'on observe pourtant que cet argument n'est pas encore une preuve d'une telle insuffisance. Il ne fait que nous suggérer de suivre un autre chemin.

On a vu dans le chapitre 1 que si on appelle « 1 » le nombre $\{|\}$ et que $n$ et $m$ sont des collections quelconques de traits verticaux, alors

$$n + \sigma(m) = n + (m + 1) = (n + m) + 1 = \sigma(n + m)$$

Il faudrait alors que, en exploitant les conditions (4) et (5 ) et l'axiome 5, on puisse parvenir à démontrer l'implication suivante :

$$(6) \qquad n, m \in \mathbb{N} \Rightarrow n + m' = (n + m)'$$

Si c'était le cas, on en aurait terminé, car de (4), (5) et (6), il serait facile de tirer les conséquences suivantes :

$$(7) \qquad n \in \mathbb{N} \Rightarrow \begin{cases} n + \alpha = n \\ n + \alpha' = n' \\ n + (\alpha')' = [n + \alpha']' = (n')' \\ n + ((\alpha')')' = [n + (\alpha')']' = ((n')')' \\ \textit{etc.} \end{cases}$$

et on aurait ainsi défini par récurrence l'addition entre tout nombre naturel $n$ et tout autre nombre naturel. Ensuite, il serait facile de démontrer que l'addition, ainsi définie, est commutative et associative et montrer ainsi, *a posteriori*, que la condition (3) est respectée relativement à l'addition.

Remarque 2.15. Comme on l'a dit, définir l'addition et la multiplication sur $\mathbb{N}$ se réduit à définir une application qui associe à tout couple d'éléments de $\mathbb{N}$ un élément de

$\mathbb{N}$. Or, comme dans les implications 7, le nombre $n$ est quelconque et qu'il est additionné successivement à tous les nombres naturels, cette implication fournit l'image de tout couple d'éléments de $\mathbb{N}$ selon l'application $a : \mathbb{N}^2 \to N$, qui définit l'addition :

$$n \in \mathbb{N} \Rightarrow \begin{cases} a(< n, \alpha >) = n \\ a(< n, \alpha' >) = n' \\ a(< n, (\alpha')' >) = (n')' \\ a(< n, ((\alpha')')' >) = ((n')')' \\ etc. \end{cases}$$

Elle est donc une définition parfaitement convenable de l'addition sur $\mathbb{N}$.

Il est pourtant nécessaire d'observer que, quel que soit $n$, une telle implication ne nous fournit l'image du couple $< n, m >$, c'est-à-dire le résultat de l'addition $n + m$, $m$ étant un nombre naturel quelconque, qu'en fonction des images de tous les couples $< n, \alpha >$, $< n, \alpha' >$, $< n, (\alpha')' >$, ..., $< n, p >$, $p$ étant le nombre naturel tel que $p' = m$. Ce qui nous assure que, en procédant de cette manière, on peut obtenir le résultat de toute addition $n + m$, quels que soient les nombres $m$ et $n$, est précisément le cinquième axiome de Peano, qui, comme on l'a vu dans la preuve du théorème 1.2, équivaut à la condition (*iii*) qui intervient dans la définition 1.1. Cet axiome nous assure en effet que la chaîne $\alpha$, $\alpha'$, $((\alpha)')'$,... coïncide avec $\mathbb{N}$. Une définition de cette sorte, s'appuyant en dernière instance sur le cinquième axiome de Peano, est généralement dite « récursive ». Même si on ne l'a pas noté explicitement, on s'est ci-dessus déjà réclamé d'un argument récursif lors des observations qui ont suivi la preuve du théorème 2.4. Par la suite, on verra comment on peut se fonder sur une procédure récursive pour démontrer des théorèmes qui peuvent être formulés de manière à énoncer que tout nombre naturel jouit d'une certaine propriété. Comme à chaque propriété qu'on peut prédiquer d'un nombre naturel, on peut associer l'ensemble des nombres naturels qui satisfont à cette propriété, qui n'est rien qu'un sous-ensemble de $\mathbb{N}$, il suffira, pour conclure la démonstration, de définir cet ensemble et de montrer que $\alpha$ lui appartient et que si un nombre naturel $x$ quelconque lui appartient — ce qu'on qualifie en général d'hypothèse inductive —, alors le nombre $x'$ lui appartient aussi. En effet, à partir de ces prémisses, le cinquième axiome de Peano nous permettra de conclure que le sous-ensemble de $\mathbb{N}$ composé des nombres naturels qui satisfont à la propriété en question coïncide avec $\mathbb{N}$, ce qui signifie, évidemment, que tout nombre naturel appartient à ce sous-ensemble et satisfait ainsi à la propriété en question.

Voyons alors s'il est possible de passer de (4) et (5) à (6), en exploitant l'axiome 5 (ou tout autre axiome de Peano). Définissons d'abord un sous-ensemble $S$ de $\mathbb{N}$ comme suit : pour chaque $p$ appartenant à $\mathbb{N}$, $p$ appartient à $S$ si et seulement si, pour tout $n$ appartenant à $\mathbb{N}$, on a

$$n + p' = (n + p)'$$

Il s'agirait alors de montrer que l'ensemble $S$, ainsi défini, coïncide avec $\mathbb{N}$. Voyons d'abord si $\alpha$ appartient à $S$ ou non. Il suffit pour cela de vérifier si pour tout $n$ appartenant à $\mathbb{N}$, $n + \alpha' = (n + \alpha)'$. C'est facile, car les conditions (5) et (4) nous assurent respectivement que $n + \alpha' = n'$ et $n + \alpha = n$, d'où il suit justement que

$$(n + \alpha)' = n' = n + \alpha'$$

donc $\alpha$ appartient à $S$. Il suffirait alors de montrer, pour s'assurer que $S$ coïncide avec $\mathbb{N}$, que, $s$ étant un nombre quelconque, si $s \in S$ alors $s'$ appartient à $S$. Supposons alors que $s$ soit un nombre naturel, et que pour tout $n$ appartenant à $\mathbb{N}$, on ait $n + s' = (n + s)'$. En exploitant

les conditions (4) et (5), il faudrait alors déduire de là que

$$n + (s')' = (n + s')' \tag{8}$$

Or, de (5), il suit que

$$n + (s')' = n + (s' + \alpha')$$

et

$$(n + s')' = (n + s') + \alpha'$$

Si on pouvait se réclamer de l'associativité de l'addition, on pourrait tirer de là que $n + (s')' = (n + s')'$, comme il s'agirait justement de démontrer, et on pourrait le faire même sans employer la supposition $n + s' = (n + s)'$. On serait alors en mesure d'affirmer que $S$ coïncide avec $\mathbb{N}$. Ainsi, s'il était légitime de s'appuyer sur l'associativité de l'addition, la 6 pourrait aussi se démontrer sans se réclamer du cinquième axiome de Peano, car de cette propriété et des conditions (4) et (5), il suit, quel que soit le nombre naturel $s$, que $n + s' = n + (s + \alpha') = (n + s) + \alpha' = (n + s)'$. Mais on ne peut pas se réclamer de l'associativité de l'addition sans tomber dans une évidente circularité, car celle-ci est justement une des propriétés de l'addition qu'on voudrait pouvoir déduire de notre définition de cette opération et ni (4) ni (5) ne nous assurent que l'addition est associative. On pourrait alors espérer pouvoir démontrer 8, en exploitant aussi l'hypothèse inductive $n + s' = (n + s)'$, outre (4) et (5). Il est pourtant facile de voir que cette condition supplémentaire ne nous aide pas, car, en associant celle-ci à (5), on tire tout au plus que, quel que soit le nombre naturel $n$, si $s \in S$, alors :

$$n + s' = n + (s + \alpha') = (n + s)' = (n + s) + \alpha'$$

ce qui nous dit seulement que si un certain nombre naturel $s$ appartient à $S$, alors, quel que soit le nombre naturel $n$,

$$n + (s + \alpha') = (n + s) + \alpha'$$

ce qui ne nous est d'aucun secours lorsqu'on sait tout simplement que $\alpha$ appartient à $S$, et qu'on ne dispose d'aucune prémisse fournissant, quel que soit le nombre naturel $s$, le résultat de l'addition $n + s$.

On pourrait alors chercher à prouver qu'également $\alpha'$ appartient à $S$. Pour cela, il faudrait prouver que pour tout nombre naturel $n$

$$n + (\alpha')' = (n + \alpha')'$$

Mais de (5), on conclut tout au plus que, quel que soit le nombre naturel $n$,

$$n + (\alpha')' = n + (\alpha' + \alpha')$$

et

$$(n + \alpha')' = (n + \alpha') + \alpha'$$

et encore un fois, on ne pourrait conclure qu'à condition de présupposer que l'addition est associative sur $\mathbb{N}$.

Cela nous convainc de la nécessité d'ajouter d'autres conditions aux conditions (4) et (5). La voie la plus simple serait de stipuler d'emblée que l'addition et la multiplication sont commutatives et associatives dans $\mathbb{N}$ et que la multiplication y est distributive sur l'addition. Ceci nous conduirait à la définition suivante :

DÉFINITION 3.1. *On appelle respectivement « addition » et « multiplication » sur* $\mathbb{N}$ *les opérations (binaires), notées « + » et « · », qui respectent les conditions suivantes, pour tout triplet de nombres naturels* $n$, $m$ *et* $p$ *:*

| | | |
|---|---|---|
| *i)* | $n + \alpha = n$ | $n \cdot \alpha = \alpha$ ; |
| *ii)* | $n + \alpha' = n'$ | $n \cdot \alpha' = n$ ; |
| *iii)* | $n + m = m + n$ | $n \cdot m = m \cdot n$ ; |
| *iv)* | $n + (m + p) = (n + m) + p$ | $n \cdot (m \cdot p) = (n \cdot m) \cdot p$ ; |
| *v)* | $n \cdot (m + p) = (n \cdot m) + (n \cdot p)$. | |

Une telle définition, bien qu'elle soit adoptée à présent par plusieurs traités d'arithmétique, a pourtant un défaut majeur : elle se réclame d'un nombre inutilement élevé de conditions, dont on devrait d'ailleurs démontrer, si on voulait être rigoureux, qu'elles ne sont pas contradictoires et qu'elles définissent respectivement deux opérations uniques.

Une définition beaucoup plus élégante et essentielle fut choisie par Peano lui-même. Elle pourrait être formulée comme suit :

Définition 3.2. *On appelle respectivement « addition » et « multiplication » sur* $\mathbb{N}$ *les opérations (binaires), notées « + » et « · », qui respectent les conditions suivantes, pour tout couple de nombres naturels* $n$ *et* $m$ *:*

| | | |
|---|---|---|
| *i)* | $n + \alpha = n$ | $n \cdot \alpha = \alpha$ ; |
| *ii)* | $n + m' = (n + m)'$ | $n \cdot m' = (n \cdot m) + n$. |

C'est à cette définition qu'on va se référer dans la suite.

Démontrons, d'abord, à partir de cette définition, les propriétés fondamentales de l'addition :

Théorème 3.1. *Si* $n$*,* $m$ *et* $p$ *appartiennent à* $\mathbb{N}$*, alors :*

***(i):*** $n + \alpha' = n'$ ;

***(ii):*** $n + (m + p) = (n + m) + p$ *[associativité de l'addition dans* $\mathbb{N}$*]* ;

***(iii):*** $n + m = m + n$ *[commutativité de l'addition dans* $\mathbb{N}$*].*

**Preuve** La preuve de ce théorème se compose naturellement de trois preuves distinctes, dont chacune relève d'une clause parmi les trois que comporte le théorème. Les preuves de (*ii*) et (*iii*) se font par récurrence, c'est-à-dire qu'elles exploitent l'axiome 5 de Peano. Parmi celles-ci, la preuve de (*iii*) est assez longue, mais n'est guère difficile. La preuve de (*i*) est par contre immédiate. Voici ces trois preuves.

(*i*) De la clause (*ii*) de la définition 3.2, on tire, en posant $m = \alpha$,

$$n + \alpha' = (n + \alpha)'$$

mais selon la clause (*i*) de la même définition, on a $n + \alpha = n$, et de là il suit ainsi

$$n + \alpha' = n'$$

Remarque 2.16. On observe que ce que nous venons de démontrer est que si on se réclame de la définition 3.2, il n'est pas nécessaire de présupposer la première des conditions 5, car elle suit comme un théorème de cette même définition, qui se sert en revanche de la première des conditions 4.

(*ii*) On considère le sous-ensemble $S$ de $\mathbb{N}$, composé par tous les nombres naturels $p$, tels que, quel que soient les nombres naturels $n$ et $m$, on ait

$$n + (m + p) = (n + m) + p \tag{9}$$

et on démontre que $\alpha \in S$ et que si $s$ est un nombre naturel quelconque, alors

$$s \in S \Rightarrow s' \in S$$

d'où on conclut, en exploitant l'axiome 5 de Peano, que $S$ coïncide avec $\mathbb{N}$, c'est-à-dire que l'égalité (9) a justement lieu pour tout triplet de nombres naturels $n$, $m$ et $p$. Voici comment on procède :

($a$) Si dans (9) on pose $p = \alpha$, on a

$$n + (m + \alpha) = (n + m) + \alpha$$

qui, selon la clause ($i$) de la définition 3.2, équivaut à

$$n + m = n + m$$

ce qui est sans doute le cas. Donc $\alpha \in S$.

($b$) De la clause ($ii$) de la définition 3.2, il suit, quels que soient les nombres naturels $n$, $m$ et $s$, que

$$n + (m + s') = n + (m + s)' = [n + (m + s)]' \tag{10}$$

et

$$(n + m) + s' = [(n + m) + s]' \tag{11}$$

Mais, si $s \in S$, alors

$$n + (m + s) = (n + m) + s$$

et donc de (10) et de (11), il suit que

$$n + (m + s') = [(n + m) + s]' = (n + m) + s'$$

et donc si $s \in S$, alors $s' \in S$. $S$ coïncide donc avec $\mathbb{N}$, ce qui conclut la preuve de ($ii$).

($iii$) On procède de la même manière qu'au cours de la preuve de ($ii$), en considérant l'ensemble $S$ des nombres naturels $m$, tels que, quel que soit le nombre naturel $n$, on ait

$$n + m = m + n$$

La preuve est pourtant, dans ce cas, un peu plus laborieuse que précédemment. On prouve d'abord les lemmes suivants :

*Lemme 1* Pour tout nombre naturel $n$, $\alpha + n = n$.

*Lemme 2* Pour tout nombre naturel $n$, $n + \alpha' = \alpha' + n$.

Pour prouver le *lemme 1*, on opère encore par récurrence, en considérant l'ensemble $T$ des nombres naturels $q$ tels que

$$\alpha + q = q$$

On pourra prouver que :

*(a.1)* $\alpha \in T$, car la clause ($i$) de la définition 3.2 nous assure que

$$\alpha + \alpha = \alpha$$

*(b.1)* si $t$ est un nombre naturel quelconque, alors

$$t \in T \Rightarrow t' \in T$$

car, si $t \in T$, alors $\alpha + t = t$ et donc, pour la clause ($ii$) de la définition 3.2,

$$\alpha + t' = (\alpha + t)' = t'$$

de sorte que $T$ coïncide avec $\mathbb{N}$, ce qui conclut la preuve du *lemme 1*.

On opère par récurrence aussi pour prouver le *lemme 2*. On considère l'ensemble $T$ des nombres naturels $q$ tels que

$$q + \alpha' = \alpha' + q$$

et on prouve que :

(*a.2*) $\alpha \in T$, car de la clause (*i*) de la définition 3.2, il suit

$$\alpha' + \alpha = \alpha'$$

tandis que du *lemme 1* (ou de la clause (*i*) du présent théorème qu'on a prouvé ci-dessus), il suit que

$$\alpha + \alpha' = \alpha'$$

d'où il suit que $\alpha' + \alpha = \alpha + \alpha'$ ;

(*b.2*) si $t$ est un nombre naturel quelconque, alors

$$t \in T \Rightarrow t' \in T$$

car si $t \in T$, alors $t + \alpha' = \alpha' + t$ et donc

$$\begin{array}{rll} t' + \alpha' & = (t')' & \text{par la clause } (i) \text{ du présent théorème} \\ & = (t + \alpha')' & \text{par la même clause} \\ & = (\alpha' + t)' & \text{car on a fait l'hypothèse que } t \in T \\ & = \alpha' + t' & \text{par la clause } (ii) \text{ de la définition 3.2} \end{array}$$

de sorte que $T$ coïncide avec $\mathbb{N}$, ce qui conclut la preuve du *lemme 2*.

Ces deux lemmes une fois prouvés, la preuve de (*iii*) est fort simple. En effet :

(*a*) $\alpha \in S$, car la clause (*i*) de la définition 3.2 nous assure que, quel que soit le nombre naturel $n$, on a $n + \alpha = n$ et donc, pour le *lemme 1*, $n + \alpha = \alpha + n$ ;

(*b*) quel que soit le nombre naturel $s$

$$s \in S \Rightarrow s' \in S$$

En fait, si $s \in S$, alors, quel que soit le nombre naturel $n$, on aura

$$n + s = s + n$$

et donc :

$$\begin{array}{rll} n + s' & = (n + s)' & \text{par la clause } (ii) \text{ de la définition 3.2} \\ & = (s + n)' & \text{car on a fait l'hypothèse que } s \in S \\ & = s + n' & \text{par la clause } (ii) \text{ de la définition 3.2} \\ & = s + (n + \alpha') & \text{par la clause } (i) \text{ du présent théorème} \\ & = s + (\alpha' + n) & \text{par le } \textit{lemme 2} \\ & = (s + \alpha') + n & \text{par la clause } (ii) \text{ du présent théorème} \\ & = s' + n & \text{par la clause } (i) \text{ du présent théorème} \end{array}$$

et $S$ coïncide donc avec $\mathbb{N}$, ce qui termine la preuve de (*iii*) et du théorème. □

Remarque 2.17. Les mathématiciens appellent « lemme » un théorème qui n'a pas d'intérêt en tant que tel, mais intervient dans la preuve d'un autre théorème, qui est en revanche considéré comme étant un résultat mathématique intéressant. On dira alors que le premier théorème est un lemme dans la preuve du deuxième. Ils appellent en revanche « corollaire » un théorème qui peut être déduit aisément à partir d'un autre théorème. Ce sera alors un corollaire de ce théorème. Il est clair que la différence entre théorèmes proprement dits, lemmes et corollaires n'est pas de nature logique ; elle est plutôt une distinction pragmatique, et peut varier selon les situations, les points de vue et les contextes. Dans l'histoire des mathématiques, il n'est par rare de trouver le cas de lemmes qui ont joué, après avoir été démontrés, un rôle bien plus important que le théorème auquel ils avaient originairement conduit.

Prouvons maintenant que la multiplication (autant à gauche qu'à droite) est distributive sur l'addition dans $\mathbb{N}$ :

THÉORÈME 3.2. *Si $n$, $m$ et $p$ appartiennet à $\mathbb{N}$, alors :*

***(i)*:** $n \cdot (m + p) = (n \cdot m) + (n \cdot p)$

***(ii)*:** $(n + m) \cdot p = (n \cdot p) + (m \cdot p)$

Avant de prouver ce théorème, on observe que les deux clauses qui le composent ne sont équivalentes qu'à condition que la multiplication soit commutative sur $\mathbb{N}$, chose que nous n'avons pas encore démontré mais que nous démontrerons ci-dessous, en nous réclamant justement de la clause $(ii)$ de ce théorème. Ceci explique la raison de la distinction entre multiplication à droite et multiplication à gauche.

**Preuve du théorème 3.2** On prouve les deux clauses successivement, en raisonnant dans les deux cas par récurrence. Voici respectivement les deux preuves.

$(i)$ Considérons l'ensemble $S$ des nombres naturels $p$, tels que, quels que soient les nombres naturels $n$ et $m$, on ait

$$n \cdot (m + p) = (n \cdot m) + (n \cdot p)$$

Il n'est pas difficile de montrer que :

$(a)$ $\alpha \in S$, car de la clause $(i)$ de la définition 3.2, il suit aussi bien

$$n \cdot (m + \alpha) = n \cdot m$$

que

$$(n \cdot m) + (n \cdot \alpha) = (n \cdot m) + \alpha = n \cdot m$$

$(b)$ si $s$ est un nombre naturel quelconque, alors

$$s \in S \Rightarrow s' \in S$$

car, si $s \in S$, alors

$$n \cdot (m + s) = (n \cdot m) + (n \cdot s)$$

et donc :

$$\begin{array}{lll} n \cdot (m + s') & = n \cdot (m + s)' & \text{par la clause } (ii) \text{ de la définition 3.2} \\ & = [n \cdot (m + s)] + n & \text{par la même clause} \\ & = [(n \cdot m) + (n \cdot s)] + n & \text{car on a fait l'hypothèse que } s \in S \\ & = (n \cdot m) + [(n \cdot s) + n] & \text{par la clause } (ii) \text{ du théorème 3.1} \\ & = (n \cdot m) + (n \cdot s') & \text{par la clause } (ii) \text{ de la définition 3.2} \end{array}$$

et $S$ coïncide donc avec $\mathbb{N}$, ce qui termine la preuve de la clause $(i)$.

$(ii)$ La preuve de la clause $(ii)$ est analogue. On considère l'ensemble $S$ des nombres naturels $p$, tels que, quels que soient les nombres naturels $n$ et $m$, on ait

$$(n + m) \cdot p = (n \cdot p) + (m \cdot p)$$

Il n'est pas difficile de montrer que :

$(a)$ $\alpha \in S$, car de la clause $(i)$ de la définition 3.2, il suit autant

$$(n + m) \cdot \alpha = \alpha$$

que

$$(n \cdot \alpha) + (m \cdot \alpha) = \alpha + \alpha = \alpha$$

$(b)$ si $s$ est un nombre naturel quelconque, alors

$$s \in S \Rightarrow s' \in S$$

car, si $s \in S$, alors

$$(n + m) \cdot s = (n \cdot s) + (m \cdot s)$$

et donc :

$$\begin{array}{lll}
(n+m)\cdot s' & = (n+m)\cdot s + (n+m) & \text{par la clause } (ii) \text{ de la définition 3.2} \\
& = [(n\cdot s)+(m\cdot s)] + (n+m) & \text{car on a fait l'hypothèse que } s \in S \\
& = [[(n\cdot s)+(m\cdot s)]+n] + m & \text{par la clause } (ii) \text{ du théorème 3.1} \\
& = [(n\cdot s)+[(m\cdot s)+n]] + m & \text{par la même clause} \\
& = [(n\cdot s)+[n+(m\cdot s)]] + m & \text{par la clause } (iii) \text{ du théorème 3.1} \\
& = [[(n\cdot s)+n]+(m\cdot s)] + m & \text{par la clause } (ii) \text{ du théorème 3.1} \\
& = [(n\cdot s)+n]+[(m\cdot s)+m] & \text{par la même clause} \\
& = (n\cdot s')+(m\cdot s') & \text{par la clause } (ii) \text{ de la définition 3.2}
\end{array}$$

et $S$ coïncide donc avec $\mathbb{N}$, ce qui termine la preuve de la clause $(ii)$ et du théorème. □

Passons maintenant aux propriétés de la multiplication :

THÉORÈME 3.3. *Si $n$, $m$ et $p$ appartiennet à $\mathbb{N}$, alors :*

***(i)*:** $n\cdot\alpha' = n$ *;*

***(ii)*:** $n\cdot(m\cdot p) = (n\cdot m)\cdot p$ *[associativité de la multiplication dans $\mathbb{N}$];*

***(iii)*:** $n\cdot m = m\cdot n$ *[commutativité de la multiplication dans $\mathbb{N}$].*

**Preuve** La preuve de ce théorème se compose également de trois preuves, dont chacune relève d'une clause distincte parmi les trois que comporte le théorème. Et encore une fois, les preuves de $(ii)$ et $(iii)$ se font par récurrence. Voici ces trois preuves.

$(i)$ Quel que soit le naturel $n$, on a :

$$\begin{array}{lll}
n\cdot\alpha' & = (n\cdot\alpha)+n & \text{par la clause } (ii) \text{ de la définition 3.2} \\
& = \alpha + n & \text{par la clause } (i) \text{ de la définition 3.2} \\
& = n+\alpha & \text{par la clause } (iii) \text{ du théorème 3.1} \\
& = n & \text{par la clause } (i) \text{ de la définition 3.2}
\end{array}$$

ce qui prouve $(i)$.

REMARQUE 2.18. On a ainsi démontré que si l'on se réclame de la définition 3.2, il n'est plus nécessaire de présupposer la deuxième des conditions 5, car elle suit comme un théorème de cette même définition qui se sert en revanche de la deuxième des conditions 4.

$(ii)$ On considère le sous-ensemble $S$ de $\mathbb{N}$, composé par tous les nombres naturels $p$, tels que, quels que soient les nombres naturels $n$ et $m$, on ait

$$n\cdot(m\cdot p) = (n\cdot m)\cdot p$$

On peut prouver facilement que :

$(a)$ $\alpha \in S$, car de la clause $(i)$ de la définition 3.2, il suit aussi bien

$$n\cdot(m\cdot\alpha) = n\cdot\alpha = \alpha$$

que

$$(n\cdot m)\cdot\alpha = \alpha$$

$(b)$ si $s$ est un nombre naturel quelconque, alors

$$s \in S \Rightarrow s' \in S$$

car, si $s \in S$, alors

$$n\cdot(m\cdot s) = (n\cdot m)\cdot s$$

et donc :

$$\begin{array}{lll} n \cdot (m \cdot s') & = n \cdot [(m \cdot s) + m] & \text{par la clause } (ii) \text{ de la définition 3.2} \\ & = [n \cdot (m \cdot s)] + [n \cdot m] & \text{par la clause } (i) \text{ du théorème 3.2} \\ & = [(n \cdot m) \cdot s] + [n \cdot m] & \text{car on a fait l'hypothèse que } s \in S \\ & = (n \cdot m) \cdot s' & \text{par la clause } (ii) \text{ de la définition 3.2} \end{array}$$

et donc $S$ coïncide avec $\mathbb{N}$, et ceci conclut la preuve de $(ii)$.

$(iii)$ Dans ce cas aussi, il faut d'abord prouver deux lemmes :

*Lemme 1* Pour tout nombre naturel $n$, $\alpha \cdot n = \alpha$.

*Lemme 2* Pour tout nombre naturel $n$, $\alpha' \cdot n = n$.

Pour prouver le *lemme 1*, on opère encore par récurrence, en considérant l'ensemble $T$ des nombres naturels $q$, tels que

$$\alpha \cdot q = \alpha.$$

On pourra prouver que :

*(a.1)* $\alpha \in T$, car la clause $(i)$ de la définition 3.2 nous assure que

$$\alpha \cdot \alpha = \alpha$$

*(b.1)* si $t$ est un nombre naturel quelconque, alors

$$t \in T \Rightarrow t' \in T$$

car, si $t \in T$, alors $\alpha \cdot t = \alpha$ et donc, pour les clauses $(ii)$ et $(i)$ de la définition 3.2 :

$$\alpha \cdot t' = (\alpha \cdot t) + \alpha = \alpha + \alpha = \alpha$$

de sorte que $T$ coïncide avec $\mathbb{N}$, ce qui conclut la preuve du *lemme 1.*

La preuve du *lemme 2* se conduit aussi par récurrence. On considère l'ensemble $T$ des nombres naturels $q$ tels que

$$\alpha' \cdot q = q$$

et on prouve que :

*(a.2)* $\alpha \in T$, car de la clause $(i)$ de la définition 3.2, il suit

$$\alpha' \cdot \alpha = \alpha$$

*(b.2)* si $t$ est un nombre naturel quelconque, alors

$$t \in T \Rightarrow t' \in T$$

car si $t \in T$, alors $\alpha' \cdot t = t$ et donc

$$\begin{array}{lll} \alpha' \cdot t' & = (\alpha' \cdot t) + \alpha' & \text{pour la clause } (ii) \text{ de la définition 3.2} \\ & = t + \alpha' & \text{car on a fait l'hypothèse que } t \in T \\ & = t' & \text{pour la clause } (i) \text{ du théorème 3.1} \end{array}$$

de sorte que $T$ coïncide avec $\mathbb{N}$, ce qui conclut la preuve du *lemme 2.*

Ces deux lemmes ayant été prouvés, la preuve de $(iii)$ est assez facile. On considère l'ensemble $S$ des nombres naturels $m$, tels que

$$n \cdot m = m \cdot n$$

et on prouve que :

*(a)* $\alpha \in S$, car la clause $(i)$ de la définition 3.2 nous assure que, quel que soit le nombre naturel $n$, on a $n \cdot \alpha = \alpha$ et le *lemme 1* nous dit que $\alpha \cdot n = \alpha$ ;

$(b)$ quel que soit le nombre naturel $s$

$$s \in S \Rightarrow s' \in S$$

En fait, si $s \in S$, alors, quel que soit le nombre naturel $n$, on aura

$$n \cdot s = s \cdot n$$

et donc :

$$\begin{array}{lll} s' \cdot n & = (s + \alpha') \cdot n & \text{par la clause } (i) \text{ du théorème 3.1} \\ & = (s \cdot n) + (\alpha' \cdot n) & \text{par la clause } (ii) \text{ du théorème 3.2} \\ & = (s \cdot n) + n & \text{par le } \textit{lemme 2} \\ & = (n \cdot s) + n & \text{car on a fait l'hypothèse que } s \in S \\ & = n \cdot s' & \text{par la clause } (ii) \text{ de la définition 3.2} \end{array}$$

et donc $S$ coïncide avec $\mathbb{N}$, ce qui termine la preuve de $(iii)$ et du théorème. □

Pour ce qui est des relations qui s'instaurent entre l'addition et la multiplication définies sur $\mathbb{N}$ et la relation d'ordre $\leq$ qui fait de $\mathbb{N}$ un ensemble totalement ordonné, il n'est guère difficile de démontrer le théorème suivant :

THÉORÈME 3.4. *Si $n$, $m$, $p$ et $q$ appartiennet à $\mathbb{N}$, alors :*

***(i)*:** *si $n < m$, alors $n + p < m + p$ ;*

***(ii)*:** *si $m \neq \alpha$, alors $n < n + m$ ;*

***(iii)*:** *si $n < m$ et $p < q$, alors $n + p < m + q$ ;*

***(iv)*:** *si $n < m$ et $p \neq \alpha$, alors $n \cdot p < m \cdot p$.*

**Preuve** La preuve de ce théorème se compose encore de quatre preuves distinctes. Les voici

$(i)$ Considérons l'ensemble $S$ des nombres naturels $p$, tels que

$$n < m \Rightarrow (n + p < m + p)$$

On peut prouver que :

$(a)$ $\alpha \in S$, car, selon la clause $(i)$ de la définition 3.2, $n + \alpha = n$ et $m + \alpha = m$ ;

$(b)$ pour tout nombre naturel $s$,

$$s \in S \Rightarrow s' \in S$$

Pour prouver cette dernière implication, il faut naturellement prouver que si $s \in S$ et $n < m$, alors, quels que soient les nombres naturels $s$, $n$ et $m$,

$$n + s' < m + s'$$

Pour ce faire, on suppose d'abord que $s \in S$ et $n < m$. De là il suit que

$$n + s < m + s$$

mais, comme on l'a prouvé à la fin du paragraphe 2 ,

$$m + s < (m + s)'$$

de sorte qu'on aura

$$n + s < m + s < (m + s)'$$

Il s'agit d'insérer $(n + s)'$ dans cette séquence en sachant que $n + s < (n + s)'$. On suppose d'abord que $(n + s)'$ est différent aussi bien de $(m + s)$ que de $(m + s)'$. Alors de la clause $(ii)$ du théorème 2.5, il suit que ni les inégalités

$$n + s < m + s < (n + s)' < (m + s)'$$

ni les inégalités

$$n + s < m + s < (m + s)' < (n + s)'$$

ne sont possibles. Donc la seule possibilité est la suivante

$$n + s < (n + s)' < m + s < (m + s)'$$

d'où il suit que

$$(n + s)' < (m + s)'$$

et donc, selon la clause (*ii*) de la définition 3.2,

$$n + s' < m + s'$$

ce qu'il s'agissait de démontrer. Il ne reste donc qu'à considérer les cas $(n + s)' = m + s$ et $(n + s)' = (m + s)'$. Dans le premier cas, on aurait encore

$$(n + s)' < (m + s)'$$

car on sait que $m + s < (m + s)'$. Dans le deuxième cas, on aurait, par l'axiome 4 de Peano,

$$n + s = m + s$$

contre l'hypothèse d'après laquelle $s$ appartient à $S$. Ce dernier cas n'est donc pas possible. Ainsi $S$ coïncide avec $\mathbb{N}$ et cela clôture la preuve de (*i*).

(*ii*) De la clause (*i*) de la définition 3.2 et de la clause (*iii*) du théorème 3.1, il suit que, quel que soit le nombre naturel $n$

$$n = \alpha + n$$

tandis que du théorème 2.4, il suit que, quel que soit le nombre naturel $m$,

$$\alpha \leq m$$

Donc (*ii*) est un corollaire de (*i*), car si $m \neq \alpha$ , alors $\alpha < m$ et donc, selon la clause (*iii*) du théorème 3.1,

$$\alpha + n = n < m + n = n + m$$

ce qui prouve (*ii*).

(*iii*) De la clause (*i*) du présent théorème, il suit que, quels que soient les nombres naturels $n$, $m$, $p$ et $q$, si $n < m$ , alors $n + p < m + p$ et si $p < q$, alors $p + m < q + m$. Mais, par la clause (*iii*) du théorème 3.1, $m + p = p + m$ et $q + m = m + q$, donc

$$\begin{aligned} n + p &< p + m \\ p + m &< m + q \end{aligned}$$

et donc, grâce à la transitivité de $<$,

$$n + p < m + q$$

ce qu'il fallait démontrer.

(*iv*) On considère maintenant l'ensemble $S$ des nombres naturels $p$ tels que

$$n < m \Rightarrow n \cdot p < m \cdot p$$

Il est clair que $\alpha$ n'appartient pas à $S$, car, quels que soient les nombres naturels $n$ et $m$, de la clause (*i*) de la définition 3.2, il suit que $n \cdot \alpha = m \cdot \alpha = \alpha$. Si on prouve toutefois que $\alpha' \in S$ et que, quel que soit le nombre naturel $s$,

$$s \in S \Rightarrow s' \in S$$

on aura prouvé que $S$ coïncide avec l'ensemble $\mathbb{N}$ privé de l'élément $\alpha$. Pour le comprendre, il suffit d'observer que l'ensemble $\mathbb{N}$ privé de l'élément $\alpha$ satisfait aux axiomes 1-5 de Peano, lorsqu'on aura posé $x_0 = \alpha'$, car cet ensemble est justement une progression. La preuve se déroule alors comme toutes les preuves par récurrence ci-dessus, et se compose des deux parties suivantes :

(*a*) $\alpha' \in S$, car, selon la clause (*i*) du théorème 3.3, quels que soient les nombres naturels $n$ et $m$, on a $n \cdot \alpha' = n$ et $m \cdot \alpha' = m$ ;

(*b*) quel que soit le nombre naturel $s$, si $s \in S$, alors $s' \in S$. Pour prouver cette implication, il faut prouver que, pour tout couple de nombres naturels $n$ et $m$, si $s \in S$ et $n < m$, alors $n \cdot s' < m \cdot s'$. Mais, si $s \in S$ et $n < m$, alors $n \cdot s < m \cdot s$ et donc, selon la clause (*iii*) du présent théorème,

$$n \cdot s + n < m \cdot s + m$$

ce qui, selon la clause (*ii*) de la définition 3.2, équivaut justement à

$$n \cdot s' < m \cdot s'$$

ce qu'il fallait démontrer. □

Les définitions de la soustraction et de la division, et la preuve de leurs propriétés fondamentales, sont maintenant très faciles. Il suffit d'élever au rang de définition le théorème 5.1 :

DÉFINITION 3.3. *On appelle respectivement « soustraction » et « division » sur* $\mathbb{N}$ *les opérations (binaires), notées « − » et « : », qui, quels que soient les nombres naturels n, m et p, satisfont aux conditions suivantes :*

**(*i*):** $n - m = p$ *si et seulement si* $n = p + m$ *;*

**(*ii*):** $n : m = p$ *si et seulement si* $n = p \cdot m$*, pourvu que* $m \neq 0$.

Grâce à la commutativité de l'addition et de la multiplication, il est ensuite facile de démontrer que cette définition entraîne la conséquence suivante :

THÉORÈME 3.5. *Si n, m et p appartiennet à* $\mathbb{N}$*, alors :*

**(*i*):** $n - m = p$ *si et seulement si* $m = n - p$ *;*

**(*ii*):** $n : m = p$ *si et seulement si* $m = n : p$.

La preuve est laissée au lecteur à titre d'exercice.

À ce point, la preuve de résultats analogues à ceux exposés dans le paragraphe 1 est facile et on peut également la laisser comme exercice pour le lecteur.

REMARQUE 2.19. Avant de conclure le présent paragraphe, il me semble nécessaire de réfléchir sur les résultats qu'on a atteints et sur la nature des arguments qui nous ont permis de les démontrer. Après avoir exploré la possibilité de définir l'addition et la multiplication sur $\mathbb{N}$ par le biais des conditions 4 et 5, on a finalement choisi (en suivant la suggestion originaire de Peano) la définition 3.2. Cette définition est essentiellement différente de celles qu'on a données dans le chapitre 1 pour l'addition et la multiplication sur les nombres entiers positifs : au lieu d'indiquer des procédures effectives aptes à produire un nombre à partir de la donnée de deux nombres, elle ne fait qu'indiquer les propriétés fondamentales d'une application définie sur les éléments d'un ensemble. Les théorèmes 3.1-3.5 ne sont que des conséquences de la détermination de ces propriétés. Bien que, pour éviter un exposé trop abstrait, j'aie préféré adopter une présentation largement discursive, il est clair que le cœur des preuves de ces théorèmes consiste en dérivations formelles ne se réclamant que de la syntaxe induite par la définition 3.2, par les axiomes de Peano (en particulier le cinquième) et par la logique propositionnelle élémentaire. C'est exactement pour rendre possible cette sorte d'arguments que la construction de Peano a été originairement conçue (et c'est pour montrer cette forme d'argumentation à l'œuvre que j'ai décidé d'introduire dans mon exposé la preuve des théorèmes 3.1-3.5 à partir de la définition 3.2 et des axiomes de Peano). Cela ne doit pourtant pas induire le lecteur à penser que l'objectif d'une formalisation comme celle de Peano puisse être de transformer les mathématiques en un pur jeu formel.

L'objectif d'une formalisation est plutôt de montrer la structure relationnelle sous-jacente à une ou plusieurs théories mathématiques, ces dernières n'étant que l'étude de certains objets abstraits, exprimant des formes invariantes que l'œil du mathématicien est capable de saisir dans le monde qui l'entoure. Ainsi, pour ne prendre qu'un exemple, si la preuve de la commutativité de l'addition consiste dans la déduction de l'égalité « $n + m = m + n$ », à partir des égalités exhibées dans la définition 3.2, il ne faut pas croire que le but de la théorie de Peano, quant à la commutativité de l'addition, soit de parvenir finalement à écrire cette égalité. Le but de cette théorie est plutôt de montrer la nature logique de l'opération d'addition, de disséquer cette opération et de retrouver ses propriétés comme des conséquences des propriétés fondamentales que l'on a cru pouvoir reconnaître en elle. Si on refuse d'apprendre à jouer le jeu du formalisme, on se condamne à ne pas pouvoir disposer d'un outil essentiel du mathématicien, mais si on croit pouvoir réduire les mathématiques à l'exercice de ce jeu, on se condamne à ne pas comprendre le but qu'elles poursuivent et à rester étranger à la dynamique de leur développement.

## 4. Noms et symboles des nombres naturels et théorèmes particuliers concernant ces nombres

Dans le présent chapitre, de même que dans le chapitre 1, la question de la représentation et de la dénomination des nombres ne se présente qu'à la fin, lorsque la théorie des nombres naturels a été complètement édifiée. Elle ne répond qu'à une exigence pratique. Comme on a démontré dans les paragraphes précédents que les nombres naturels se comportent, relativement les uns aux autres, comme les nombres entiers positifs, tels qu'ils ont été définis dans le chapitre 1, le lecteur n'aura aucune difficulté à comprendre que les mêmes systèmes de dénomination et de numérotation s'appliquent aussi bien à ceux-ci qu'à ceux-là. Simplement, le référent des mêmes noms et des mêmes symboles n'est pas le même dans les deux cas : dans un cas, ces noms et ces symboles se réfèrent à des collections de traits verticaux, dans l'autre ils se réfèrent aux éléments d'un ensemble totalement ordonné formant une progression. Pour éviter des confusions, il est pourtant souhaitable que les objets distincts qui, dans les deux cas, fournissent la signification du même terme, jouent dans les deux systèmes le même rôle. C'est parce que cette condition est respectée que dans les applications de l'arithmétique on n'a jamais besoin de spécifier la nature des objets qui constituent la signification des termes numéraux employés. De plus : le respect de cette condition permet d'assigner, dans les deux cas, la même signification aux termes composés en fonctions des termes élémentaires. Ainsi, si on accepte d'employer, par exemple, le système décimal habituel de numérotation et notation symbolique, le nombre noté « 5.423 » est dans les deux cas le résultat de la somme $5 \cdot (10^3) + 4 \cdot (10^2) + 2 \cdot (10) + 3 \cdot 1$. Il est donc clair que les algorithmes d'addition, de multiplication, de soustraction et de division des nombres représentés par des symboles composés sont les mêmes dans les deux cas ; il n'est guère nécessaire de les exposer ici à nouveau.

Qu'on accepte donc d'emblée le système de numérotation décimale habituel. On aura alors les représentations et les dénominations suivantes :

| | | | | |
|---|---|---|---|---|
| $\alpha$ | $\longrightarrow$ | 0 | $\longrightarrow$ | zéro |
| $\alpha' = 0'$ | $\longrightarrow$ | 1 | $\longrightarrow$ | un |
| $(\alpha')' = (0')' = 1'$ | $\longrightarrow$ | 2 | $\longrightarrow$ | deux |
| $((\alpha')')' = ((0')')' = (1')' = 2'$ | $\longrightarrow$ | 3 | $\longrightarrow$ | trois |
| ... | | ... | | ... |
| $8'$ | $\longrightarrow$ | 9 | $\longrightarrow$ | neuf |
| $(8')' = 9'$ | $\longrightarrow$ | 10 | $\longrightarrow$ | dix |
| ... | | ... | | ... |

Soient maintenant $n$ et $m$ deux nombres naturels représentés dans ce système de numérotation par deux symboles composés

$$\rho_p ... \rho_2 \rho_1 \rho_0 \qquad \text{et} \qquad \tau_q ... \tau_2 \tau_1 \tau_0$$

où les symboles « $\rho_p$ », ..., « $\rho_0$ » et « $\tau_q$ »,...,« $\tau_0$ » représentent des nombres naturels compris entre 0 et 9. Il est clair que ces deux nombres pourront aussi se représenter ainsi :

$$\rho_p \cdot (10^p) + ... + \rho_2 \cdot (10^2) + \rho_1 \cdot (10) + \rho_0$$
$$\tau_q \cdot (10^q) + ... + \tau_2 \cdot (10^2) + \tau_1 \cdot (10) + \tau_0$$

$p$ et $q$ étant des nombres naturels. Grâce à la commutativité et à l'associativité de l'addition et à la distributivité de la multiplication sur l'addition, leur somme pourra alors se représenter ainsi

$$\rho_p \cdot (10^q) + \tau_q \cdot (10^p) + ... + [\rho_2 + \tau_2] \cdot (10^2) + [\rho_1 + \tau_1] \cdot (10) + [\rho_0 + \tau_0]$$

Cela montre bien que pour chaque couple de nombres naturels, dont un au moins se laisse représenter par un symbole composé dans le système de numérotation choisi, la somme de ces nombres peut être calculée en réduisant leur addition à des additions entre nombres représentés par des symboles élémentaires. Il est facile de voir qu'il en est de même pour le produit, la différence et le quotient. Le passage des nombres comme collections de traits verticaux aux nombres naturels ne produit donc pas de changements à cet égard.

Un changement profond intervient en revanche en ce qui concerne l'addition et la multiplication entre nombres qui sont représentés, dans le système de numérotation choisi, par des symboles élémentaires, car dans la théorie axiomatique de Peano, il n'est pas possible de calculer les résultats de ces opérations en se réclamant des collections de traits verticaux, comme on l'a fait pourtant dans le chapitre 1. Il se pose alors le problème de comprendre comment un tel calcul peut être fait. La réponse est évidente : ce calcul ne peut se faire qu'en s'appuyant sur les propriétés formelles des opérations sur les nombres naturels énoncées ci-dessus. Dans le cas extrême, où le système de numérotation choisi ne comporterait que deux noms élémentaires, $0 = \alpha$ et $1 = \alpha'$, il ne s'agirait que de justifier les égalités

$$\begin{array}{ll} \alpha + \alpha = 0 + 0 = \alpha = 0 & \alpha \cdot \alpha = 0 \cdot 0 = \alpha = 0 \\ \alpha + \alpha' = 0 + 1 = \alpha' = 1 & \alpha \cdot \alpha' = 0 \cdot 1 = \alpha = 0 \\ \alpha' + \alpha' = 1 + 1 = (\alpha')' = 10 & \alpha' \cdot \alpha' = 1 \cdot 1 = \alpha' = 1 \end{array} \tag{12}$$

qu'on a déjà démontrées dans le paragraphe précédent. On pourrait donc songer à transformer toute addition et multiplication entre nombres représentés par des symboles élémentaires, dans n'importe quel système de numérotation, en additions et multiplications entre nombres représentés dans le système binaire de numérotation ; et réduire ensuite ces additions et multiplications aux six opérations élémentaires (12). Cela réduirait au strict minimum les calculs dont le résultat devrait être justifié en ne se réclamant que des propriétés formelles de l'addition et de la multiplication. En dehors de l'informatique (où une telle réduction de tout nombre à un nombre représenté dans un système de numérotation binaire est indispensable, car un ordinateur n'est rien d'autre qu'une machine travaillant, en dernière instance, sur l'alternative 0-1, c'est-à-dire une machine dite « de Turing », en l'honneur du mathématicien anglais A. Turing, qui fut le premier à concevoir logiquement un ordinateur), cette réduction ennuyeuse n'est pourtant pas nécessaire, car les propriétés formelles de l'addition et de la multiplication permettent de calculer toutes les sommes et tous les produits qu'on veut. Voici, en guise d'exemple, comment la somme $7 + 5$ et le produit $5 \cdot 4$ peuvent être calculés en ne se réclamant que de ces

propriétés. Les mêmes procédés, qui sont essentiellement dus à Leibniz, peuvent naturellement s'appliquer à tout autre exemple.

NOTE HISTORIQUE 2.5. Né à Londres le 23 juin 1912, Alan M. Turing étudia les mathématiques dans cette même ville, au *King's College*, où il fut nommé *fellow* en 1935. Ce fut dans les années 1936-1938 que, en profitant d'un séjour d'étude à l'université de Princeton, où il put travailler avec A. Church, l'un des plus illustres et féconds logiciens de l'époque, il fut en mesure de mener les études qui le conduisirent, entre autre, à publier, en 1937, l'article « On Computable Numbers, With an Application to the *Entscheidungsproblem* ». C'est dans cet article qu'il définit une machine idéale (dite ensuite « machine de Turing » ), dont le fonctionnement devait, dans ses intentions, imiter les procédures computationnelles du cerveau humain.

Turing suppose que sa machine travaille par étapes et possède une mémoire infinie, c'est-à-dire qu'elle se comporte à chaque étape d'une certaine manière plutôt que d'une autre, en fonction du comportement qu'elle a eu dans les étapes précédentes, à partir du début de la computation, quel que soit le nombre de ces étapes. La machine travaille sur un ruban, lui aussi supposé infini, divisé en cases et peut, à chaque étape, observer une case de ce ruban et se comporter de l'une des quatre manières suivantes : déplacer le ruban d'une case à droite ; déplacer le ruban d'une case à gauche ; imprimer un symbole (choisi parmi un ensemble fini de symboles qu'on peut bien imaginer n'être composé que par deux éléments) sur la case qu'elle observe ; effacer le symbole éventuellement imprimé sur cette case. On peut ainsi définir l'activité d'une telle machine (qui n'est rien d'autre qu'une computation) comme une successions de quadruplets,

$$< q_i a_i A_i q_j >$$

où $q_i$ est l'état interne de la machine dans l'$i$-ième étape de son calcul (qui correspond évidemment à la mémoire de son comportement dans les étapes précédentes), $a_i$ est le symbole imprimé dans la case qu'elle observe à cette étape (l'absence de symboles est évidemment traitée comme un symbole, de même que l'espace blanc est traité en typographie comme un caractère), $A_i$ est l'acte qu'elle accomplit à l'étape en question, et $q_j$ est le nouvel état interne de la machine après l'accomplissement de cet acte. Chacun de ces quadruplets peut ainsi être conçu comme l'expression d'un élément atomique d'une computation.

En 1939, Turing retourne au *King's College*, qu'il abandonne pourtant bientôt, car il est employé au département de communication du *Foreign Office*, où il s'occupera, pendant la deuxième guerre mondiale, de décrypter les messages codés des ennemis de son pays. En 1945 il intègre le *staff* du Laboratoire Physique National, et en 1952 il est nommé à l'université de Manchester. Il meurt à Wilmslow, le 7 juin 1954, d'un empoisonnement : malgré les apparences (la mort ayant été causée par l'ingestion d'une pomme ayant macéré dans le cyanure), on a souvent douté qu'il s'agît d'un suicide.

**Lectures possibles** : A. Hodges, *Alan Turing ou l'énigme de l'intelligence*, Payot, Paris, 1988 ; J. Lassègue, *Turing*, Les Belles Lettres, Paris, 1998 ; R. Herken (ed. by), *The Universal Turing Machine. A Half-Century Survey*, Springer Verlag, Wien, New York, 1994.

THÉORÈME 4.1 (Calcul de $7 + 5$). *Dans le système de numérotation décimale, la somme des nombres notés « 7 » et « 5 » est le nombre noté « 12 » .*

**Preuve** Qu'on se rappelle d'abord les conventions notationnelles suivantes

$$
\begin{array}{ll}
8 = 7' & 1 = 0' = \alpha' \\
9 = 8' & 2 = 1' \\
10 = 9' & 3 = 2' \\
11 = 10' & 4 = 3' \\
12 = 11' & 5 = 4'
\end{array}
\tag{13}
$$

En usant de ces conventions et des trois clauses du théorème 3.1, il sera facile de conduire la déduction suivante

$$
\begin{aligned}
7+5 &= 7+4' = 7+(4+1) = 7+(1+4) = \\
&= (7+1)+4 = 7'+4 = 8+4 = \\
&= 8+3' = 8+(3+1) = 8+(1+3) = \\
&= (8+1)+3 = 8'+3 = 9+3 = \\
&= 9+2' = 9+(2+1) = 9+(1+2) = \\
&= (9+1)+2 = 9'+2 = 10+2 = \\
&= 10+1' = 10+(1+1) = \\
&= (10+1)+1 = 10'+1 = 11+1 = \\
&= 11' = 12
\end{aligned}
$$

□

THÉORÈME 4.2 (Calcul de $5 \cdot 4$). *Dans le système de numérotation décimale le produit des nombres notés « 5 » et « 4 » est le nombre noté « 20 » .*

**Preuve** Les conventions notationnelles à rappeler sont énoncées parmi les (13). Une fois qu'elles ont été posées, la clause (*ii*) de la définition 3.2 et les théorèmes 3.1 et 3.3 permettent la déduction suivante :

$$
\begin{aligned}
5 \cdot 4 &= 5 \cdot 3' = 5 \cdot 3 + 5 = \\
&= (5 \cdot 2') + 5 = [(5 \cdot 2) + 5] + 5 = (5 \cdot 2) + (5 + 5) = \\
&= (5 \cdot 1') + (5 + 5) = [(5 \cdot 1) + 5] + (5 + 5) = \\
&= (5 + 5) + (5 + 5)
\end{aligned}
$$

Il suffit à ce point de raisonner comme dans la preuve du théorème précédent pour calculer la somme de $5 + 5$, ce qui donne naturellement $5 + 5 = 10$, et ensuite d'opérer en colonne comme il suit

$$
\begin{array}{cccccccccccc}
1 & 0 & + & & & & & & & & & \\
1 & 0 & = & & & & & & & & & \\
\hline
1' & 0 & = & 2 \cdot (10) & + & 0 & = & 2 \cdot (10) & = & 1 & 0 & \cdot \\
 & & & & & & & & & & 2 & = \\
\hline
 & & & & & & & & & 2 & 0 &
\end{array}
$$

ce qui termine la preuve. □

NOTE HISTORIQUE 2.6. Les *Nouveaux essais sur l'entendement humain* sont, comme on le sait, la réponse de Leibniz à l'*Essay concerning human understanding* de Locke. Ils prennent la forme d'un dialogue entre Philalète, exposant les idées de Locke et lisant de longues parties de son texte, et Théophile, discutant ces idées et exprimant le point de vue critique de Leibniz. On est au paragraphe 10 du chapitre

VII du quatrième livre, lorsque Philalète lit ce passage de l'*Essay* : « Je voudrais bien demander à ces Messieurs, qui prétendent que toute [...] connaissance [qui ne soit pas une connaissance de fait] dépend des principes généraux innés et évidents par eux-mêmes, de quel principe ils ont besoin pour prouver que deux et deux est quatre ? car on connaît la vérité de ces sortes de propositions sans le secours d'aucune preuve ». La réponse de Théophile (Leibniz) ne se fait pas attendre. La voici : « Ce n'est pas une vérité tout à fait immédiate que deux et deux sont quatre, supposé que quatre signifie trois et un. On peut donc la démontrer, et voici comment : *Définitions* : 1) Deux est un et un. 2) Trois est deux et un. 3) Quatre est trois et un. *Axiome* . Mettant des choses égales à la place, l'égalité demeure. *Démonstration* : 2 et 2 est 2 et 1 et 1 (par la déf. 1) [...] 2 et 1 et 1 est 3 et 1 (par la déf. 2) [...] 3 et 1 est 4 (par la déf. 3). Donc (par l'axiome) 2 et 2 est 4. Ce qu'il fallait démontrer ».

Il est facile de comprendre que, formulée de cette façon, la preuve de Leibniz n'est pas tout à fait correcte. Ce dernier n'observe pas, en effet, que la deuxième étape de son argument demande la condition d'associativité de l'addition, qui aurait donc dû être ajoutée parmi les prémisses. Malgré cette imprécision, la preuve de Leibniz est restée dans l'histoire de la philosophie des mathématiques, comme un argument, souvent répété, contre la thèse de Kant (que Locke avait, en un certain sens, anticipée) d'après laquelle les « jugements » arithmétiques sont non seulement *a priori*, mais aussi synthétiques en tant que synthétiques *a priori* . Cette preuve montrerait en effet, selon les opposants de Kant, que ces jugements dérivent du principe d'identité et d'un ensemble plus ou moins large de définitions convenables. Ils seraient donc, certes *a priori*, mais aussi analytiques. L'erreur de Kant viendrait ainsi du fait de ne pas avoir pris en compte les possibilités déductives de la logique formelle, que Leibniz avait déjà, quant à lui, préconisées. Le débat autour de ce point fut particulièrement vif entre la fin du XIX$^{\text{ème}}$ siècle et le début du XX$^{\text{ème}}$, quand les opinions opposées furent soutenues respectivement par Couturat et Cassirer. La reconstruction, même sommaire, de ce débat n'est pas possible ici. Il devrait pourtant être clair que le fait d'avoir utilisé la preuve de Leibniz ne signifie pas que j'accepte l'argument précédent contre la thèse de Kant. Cet argument ne dépend pas, en effet, de la correction de cette démonstration, qui (mis à part l'oubli de la condition d'associativité) est hors de discussion, mais de l'interprétation de cette preuve et de l'évaluation épistémologique du contexte théorique dans lequel elle s'insère.

*Lectures possibles* : E. Cassirer, « Kant und die moderne Mathematik », *Kantstudien*, **12**, 1907, pp. 1-49 ; L. Couturat, « La philosophie des mathématiques de Kant », appendice de : L. Couturat, *Les principes de mathématiques*, F. Alcan, Paris, 1905, pp. 235-308.

Un dernier problème reste ouvert : celui de la signification des termes numéraux dans le langage quotidien. Si on pense que le terme « trois » se réfère à un élément de $\mathbb{N}$ (et en particulier au successeur du successeur du successeur de $\alpha$), que signifie qu'il y a trois pommes dans mon panier ? La réponse n'est pas si facile et dans un sens, elle n'est pas naturelle. C'est justement ce qui a convaincu Frege qu'une axiomatisation comme celle de Peano (ou une construction comme celle de Dedekind) ne résolvait qu'en partie le problème consistant à se demander ce que sont les nombres. Quant à moi, je ne suis pas sûr que le problème soit bien formulé, même si je conviens avec Frege que la question « que signifie qu'il y trois pommes dans mon panier ? » est une bonne question, et même qu'il est crucial de savoir y répondre de manière satisfaisante.

Je conçois plusieurs réponses possibles à cette question, parmi lesquelles la suivante :

— Dire qu'il y a trois pommes dans mon panier signifie dire que la collection des pommes qui sont dans mon panier est en bijection avec l'ensemble des éléments de la chaîne $\mathcal{S}_{3-1}$ associée, dans la théorie de Peano, au nombre dont le nombre dit « trois » est le successeur.

D'aucuns trouveront cette réponse trop baroque ; ils seront peut-être plus convaincus qu'elle est légitime en observant qu'elle est équivalente à la suivante :

— Dire qu'il y a trois pommes dans mon panier signifie dire que la collection des pommes qui sont dans mon panier est en bijection avec la collection des nombres naturels plus petits que le nombre dit « trois ».

Si cette réponse est encore jugée trop abstraite, on pourrait enfin se résoudre à une autre stratégie qui, *pace* Frege, ne me paraît pas préjudiciable à l'avenir de la philosophie des mathématiques. Elle repose sur la constatation que différentes théories, portant sur des objets qui se comportent entre eux de la même manière, sont possibles. Cette simple constatation me semble suggérer que rien ne nous oblige à nous réclamer toujours de la même théorie, et encore moins de prétendre que cette théorie puisse nous dire ce que les nombres sont, et soit la seule à nous dire cela. On pourrait alors répondre à la question précédente, comme on l'a fait dans le chapitre 1, tout en reconnaissant que le terme « trois » renvoie, quand il est considéré relativement à la théorie de Peano, à l'élément de $\mathbb{N}$ qui se comporte dans $\mathbb{N}$ comme la collection $\{|, |, |\}$ se comporte dans l'ensemble des collections de traits verticaux, dans la théorie exposée dans le chapitre 1.

CHAPITRE 3

# Quelques résultats à propos de sommes remarquables de nombres naturels démontrés par récurrence

Dans le paragraphe 3, on a démontré plusieurs théorèmes en appliquant une méthode dite « par récurrence », ou parfois par « induction complète », qui se rapporte au cinquième axiome de Peano. Le lecteur devrait donc être familiarisé avec cette méthode très puissante. Elle sert à prouver des théorèmes généraux, qu'on peut énoncer en affirmant que tous les nombres naturels (ou, plus généralement, tous les éléments d'une progression, et donc aussi tous les nombres naturels plus grands qu'un nombre naturel donné, par exemple zéro, ou tous les nombres pairs, ou toutes les fractions de l'unité, $\frac{1}{1}$, $\frac{1}{2}$, $\frac{1}{3}$,... et ainsi de suite) jouissent d'une propriété (qui dans la plupart des cas peut être exprimée par une formule). Le défaut principal d'une telle méthode vient de sa faiblesse heuristique : pour démontrer que « $P(n)$ » est un théorème pour tout nombre naturel $n$ (ou pour tout élément $n$ d'une certaine progression) — ce qui revient à dire que le sous-ensemble de $\mathbb{N}$, constitué par les nombres naturels $n$, tels que $P(n)$, coïncide avec $\mathbb{N}$ — il faut partir de la conjecture « $n \in \mathbb{N} \Rightarrow P(n)$ », c'est-à-dire qu'il faut imaginer un certain résultat pour pouvoir ensuite le prouver. Ainsi, cette méthode ne résout les problèmes qu'à condition qu'on sache en imaginer la solution correcte. Quelquefois, cette solution a déjà été démontrée. La méthode d'induction complète ne fait alors que fournir une nouvelle preuve du même résultat. En d'autres cas, on ignore si la solution qu'on a imaginée est correcte ou pas ; alors la méthode d'induction complète peut nous assurer que notre supposition était correcte. Naturellement ces derniers cas sont les plus intéressants. Pourtant, pour exercer le lecteur à cette méthode démonstrative fondamentale, je proposerai ci-dessous quelques problèmes faciles, qu'on peut résoudre aussi bien par une preuve directe (c'est-à-dire sans avoir besoin d'imaginer la solution au préalable) que par induction complète, en invitant le lecteur à réfléchir sur les preuves que je vais exposer. D'autres exemples, un peu plus complexes, montreront ensuite la méthode démonstrative par induction complète à l'œuvre dans des cas où il serait bien plus difficile de donner une preuve directe.

## 1. Somme partielle d'une série arithmétique quelconque

Proposons-nous d'abord de rechercher la somme de l'addition suivante :

$$0 + 1 + 2 + 3 + ... + n$$

où $n$ est un nombre naturel quelconque.

Commençons par introduire quelques notations convenables. On indique par la lettre « $i$ » une variable qui varie sur l'ensemble $\mathbb{N}$ des nombres naturels, c'est-à-dire qui peut prendre la valeur de tout nombre naturel ; autrement dit, on dénote par la lettre « $i$ » un nombre naturel indéterminé qui reçoit, dans des circonstances diverses, différentes déterminations. On note ensuite « $u_i$ » une quantité (c'est-à-dire quelque chose qu'on peut se limiter à penser ici comme une entité additionnable à d'autres entités du même type : un nombre naturel, un nombre réel, un segment, un carré, un angle, etc.) également indéterminée et variable, qui se détermine dès

que la variable $i$ est déterminée. On dira que $u_i$ est une fonction de $i$, $i$ étant généralement qualifié d'« indice » de $u_i$. Dans la plupart des cas intéressants, on a une manière très simple d'indiquer le lien qui unit $u_i$ à $i$, en exprimant $u_i$ par une formule explicite dans laquelle intervient le symbole « $i$ » (éventuellement à côté d'autres symboles qui expriment des quantités déterminées). Ainsi, si on pose

$$u_i = 2i + 3$$

on veut signifier que si $i = q$, alors $u_i = u_q = 2q + 3$ ($q$ étant un nombre naturel déterminé quelconque, par exemple 27, ce qui donne $u_i = u_{27} = 2 \cdot 27 + 3 = 57$). Et si on pose, tout simplement

$$u_i = i$$

on veut signifier que si $i = q$, alors $u_i = u_q = q$ (de sorte que, pour en rester à notre exemple, on aura $u_{27} = 27$).

Remarque 3.1. Bien que, au sens strict, le terme « fonction » indique, de même que le terme « application », une association qui associe des éléments d'un certain ensemble à un et un seul élément d'un autre ensemble, les mathématiciens ont pris l'habitude d'employer ce même terme en un sens plus large. Imaginons que $X$ soit un certain ensemble, et qu'on le considère comme ensemble de départ d'une fonction $f$ de $X$ vers $Y$. Si $x$ est un élément de $X$ et si $f$ est telle qu'elle associe à cet élément un (et un seul) élément $y$ de $Y$, alors on dira que la fonction $f$ est définie en $x$. Soit alors $\tilde{X} \subseteq X$ le sous-ensemble de $X$ composé par tous les éléments de $x$ de $X$ tels que $f$ est définie en $x$. $\tilde{X}$ sera alors le domaine de $f$. Au lieu de considérer $x$ comme un élément quelconque mais déterminé de $X$, on peut le considérer comme une variable qui varie sur $X$. $\tilde{X}$ pourra alors être pensé comme la partie du domaine de variation de la variable sur laquelle la fonction est définie. Si l'on fait l'hypothèse que $x$ varie sur $\tilde{X}$, le symbole « $f(x)$ » peut alors être employé en même temps pour dénoter : l'image de $x$ selon la fonction $f$ — qui sera généralement une variable $y$ qui varie sur $Y$, ou, pour être plus précis, sur la partie de $Y$ qui constitue l'image du domaine de $f$—, ou la loi de l'association $f$ elle-même. De même, le terme « fonction » pourra être employé pour dénoter autant cette loi d'association, que la variable $y$, qui sera dite alors « fonction de $x$ », et qui est de ce fait souvent dénotée par le symbole « $y_x$ ». Dire que $u_i$ est une fonction de $i$ revient donc à dire qu'il est l'image, généralement variable, de la variable $i$, qui varie sur l'ensemble $\mathbb{N}$ des nombres naturels, selon une fonction qu'on pourrait dénoter ainsi « $u : \mathbb{N} \to E$ », $E$ étant un ensemble convenable.

Dans les exemples qu'on vient de considérer $\mathbb{N}$ est autant l'ensemble de départ que le domaine de $u$ et il coïncide également avec l'ensemble d'arrivée de cette fonction et, dans le deuxième exemple, aussi avec l'image de son domaine. L'image du domaine de $u$ est en revanche constituée, dans le premier exemple, par l'ensemble des nombres impairs plus grands ou égaux à 3, car, si $i$ est un nombre naturel, la somme $2i + 3$ ne peut qu'être un nombre impair plus grand ou égal à 3, et si $i$ varie sur tout $\mathbb{N}$, $u_i = 2i + 3$ variera justement sur la totalité de l'ensemble des nombres impairs plus grands ou égaux à 3. Dans la suite du présent chapitre on ne considérera que des fonction $u_i$ de $\mathbb{N}$ sur $\mathbb{N}$, mais il m'a semblé utile de souligner que la même notation peut être employée pour indiquer toutes sortes de fonctions $u : \mathbb{N} \to E$, quel que soit l'ensemble $E$. Pourtant, comme cette notation est souvent employée pour indiquer les termes successifs d'une addition, on peut faire l'hypothèse qu'on ait défini sur $E$ une opération dite « addition » et dénotée par le symbole « $+$ », qui a toutes les propriétés formelles de l'addition définie sur $\mathbb{N}$. Evidemment, si $E$ ne coïncide pas avec $\mathbb{N}$, ou, plus en général, s'il n'est pas une progression (ou n'est pas directement reconnu comme une progression, c'est-à-dire que ses éléments ne sont pas distingués et caractérisés en tant

qu'éléments successifs d'une progression — le lecteur comprendra mieux ce que j'entends une fois qu'il aura lu le chapitre 4) l'addition sur $E$ ne pourra pas être définie comme, dans le chapitre 2, on a défini l'addition sur $\mathbb{N}$. Dans les chapitres suivants on rencontrera plusieurs exemples de définition d'une addition sur des ensembles différents de $\mathbb{N}$.

Pour terminer, il faut observer que les notions de variable qui varie sur un ensemble et d'élément indéterminé de cet ensemble ne sont pas équivalentes. On peut en fait imaginer avoir choisi un élément de cet ensemble, sans pourtant spécifier de quel élément il s'agit. Ainsi l'égalité « $i = q$ » qu'on a employée ci-dessus, indique que la variable $i$ a été fixée, même si elle souligne le fait qu'il n'est pas nécessaire de dire quelle valeur déterminée ou constante, comme on dit d'habitude, on lui a assigné. Naturellement la distinction entre variable et constante n'est pas absolue et ne dépend que des conventions et des conditions qui caractérisent le problème ou le domaine d'objets considéré. Pour comprendre cette différence en profondeur, il serait pourtant nécessaire d'esquisser certaines notions fondamentales d'analyse, comme on appelle généralement la théorie des fonctions d'une variable qui varie sur des ensembles continus. Mais cela nous porterait trop loin du but restreint du présent exposé. Ici il suffira de considérer une variable comme un élément indéterminé d'un ensemble spécifié qui est susceptible de recevoir différentes déterminations, ou même qui exprime à la fois toutes les déterminations possibles qui dérivent de son identification à chaque élément de cet ensemble ; une constante sera par contre considérée comme un élément déterminé de cet ensemble, ou du moins susceptible d'une seule détermination possible, qu'il n'est pas, en général, nécessaire de déterminer à son tour. Si je parle de détermination d'une détermination ce n'est pas le fait d'un *lapsus*. En effet, on peut supposer avoir déterminé un élément d'un ensemble sans déterminer comment il a été déterminé. Ceci est par exemple le cas, lorsqu'on dit que $q$ (ou $n$) est un nombre naturel déterminé, ou même un nombre naturel quelconque : on suppose que c'est un nombre naturel déterminé, mais on ne dit pas de quel nombre naturel il s'agit, et on laisse même entendre que chaque nombre naturel pourrait faire l'affaire.

On note ensuite par le symbole « $\sum_{i=p}^{q} u_i$ » ($p$ et $q$ étant deux nombres naturels déterminés, tels que $p \leq q$) la somme $u_p + u_{p+1} + u_{p+2} + ... + u_{q-1} + u_q$, ce qui fournit l'égalité notationnelle suivante

$$\sum_{i=p}^{q} u_i = u_p + u_{p+1} + u_{p+2} + ... + u_{q-1} + u_q$$

En appliquant ces conventions notationnelles, notre problème revient à déterminer la somme de l'addition

$$\sum_{i=0}^{n} i = 0 + 1 + 2 + ... + (n-1) + n$$

quel que soit le nombre naturel $n$. Si on pense $\sum_{i=0}^{n} i$, plutôt que comme une addition, directement comme une somme, alors il s'agira de trouver comment la valeur de $\sum_{i=0}^{n} i$ peut être calculée lorsque le nombre naturel $n$ est fixé d'une manière quelconque. Une façon de répondre à cette question est de trouver une formule explicite, où apparaît le symbole « $n$ », indiquant le calcul qui doit être accompli pour parvenir à la détermination de cette valeur, une fois que la valeur de $n$ a été fixée. On pourrait penser que la formulation du problème contient déjà la réponse, car « $0 + 1 + 2 + ... + (n-1) + n$ » est justement une formule explicite du type de celles

qu'on cherche. Pourtant si on pose, par exemple, $n = 7.655.760$, le calcul indiqué par cette formule est très long, et il est même assez long pour un ordinateur (qui, pour calculer la somme $0+1+2+...+7.655.760$ passe normalement par la formule qu'on va déterminer ci-dessous). Il convient donc de trouver une autre formule qui exhibe un calcul plus immédiat et plus simple. C'est précisément notre problème. Voici comment on peut le résoudre directement.

On suppose que

$$\sum_{i=0}^{n} i = U_n$$

Comme, il est clair que

$$\sum_{i=0}^{n}(n-i) = n + (n-1) + (n-2) + ... + [n-(n-1)] + (n-n) = \sum_{i=0}^{n} i$$

on aura :

$$\begin{array}{rcccccccccccc} \displaystyle\sum_{i=0}^{n} i = & 0 & + & 1 & + & 2 & + & ... & + & (n-1) & + & n & = & U_n \\ \displaystyle\sum_{i=0}^{n}(n-i) = & n & + & (n-1) & + & (n-2) & + & ... & + & 1 & + & 0 & = & U_n \end{array}$$

et donc, en additionnant ces deux sommes terme à terme,

$$\begin{aligned} 2U_n &= \underbrace{n+n+n+...+n}_{n+1 \text{ fois}} \\ &= (n+1)n \end{aligned}$$

d'où on n'aura pas de difficulté à conclure que :

$$U_n = \sum_{i=0}^{n} i = [n(n+1)] \ : 2$$

ou, comme on l'écrit habituellement, en employant la notation qu'on introduira dans le prochain chapitre, pour les nombres fractionnaires,

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{14}$$

$\frac{n(n+1)}{2}$ étant justement le quotient de la division $[n(n+1)] \ : 2$.

Ainsi, si on pose par exemple $n = 7.655.760$, on aura, assez rapidement :

$$\begin{aligned} \sum_{i=0}^{7.655.760} i &= \frac{7.655.760 \cdot 7.655.761}{2} \\ &= \frac{58.610.668.833.360}{2} = 29.305.334.416.680 \end{aligned}$$

L'argument précédent donne directement la solution de notre problème, quel que soit le nombre naturel $n$, c'est-à-dire qu'il la donne sans qu'on ait imaginé cette solution au préalable. Il n'est pourtant pas le seul argument possible pour démontrer que (14) est correcte. Si on fait la conjecture que (14) est correcte, un argument par récurrence peut être employé pour démontrer le théorème suivant :

THÉORÈME 1.1. *Si $n$ est un nombre naturel quelconque, alors :*

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

**Preuve (par induction complète)** La preuve se conduit en deux étapes :
($a$) On prouve d'abord que c'est le cas pour $n = 0$. Ceci est banal, car si $n = 0$, on a

$$\begin{aligned} \sum_{i=0}^{n} i &= \sum_{i=0}^{0} i = 0 \\ \frac{n(n+1)}{2} &= \frac{0 \cdot 1}{2} = 0 \end{aligned}$$

($b$) On prouve ensuite que si $s$ est un nombre naturel quelconque, alors

$$\sum_{i=0}^{s} i = \frac{s(s+1)}{2} \Rightarrow \sum_{i=0}^{s'} i = \frac{s'(s'+1)}{2}$$

Pour ce faire, on suppose que :

$$\sum_{i=0}^{s} i = \frac{s(s+1)}{2}$$

Comme $s' = s + 1$, on aura alors

$$\sum_{i=0}^{s'} i = \sum_{i=0}^{s+1} i = \frac{s(s+1)}{2} + (s+1) \tag{15}$$

Pour continuer la preuve, il faudrait maintenant savoir calculer la somme $\frac{s(s+1)}{2} + (s+1)$, quel que soit le nombre naturel $n$. Or, même si le quotient $\frac{s(s+1)}{2}$ est sans doute un nombre naturel (car un des deux nombres naturels $s$ et $s+1$ est nécessairement pair, et donc le produit $s(s+1)$ est aussi pair — vu que, pour tout couple de nombres naturels $h$ et $k$ on a, à cause de l'associativité de $\cdot$, $(2 \cdot h) \cdot k = 2 \cdot (h \cdot k)$), ce calcul ne peut se faire en général (c'est-à-dire lorsqu'on ne connaît pas ce produit) si on ne dispose pas de l'algorithme d'addition des nombres fractionnaires. On montrera comment déterminer cet algorithme dans le chapitre 4. Pour l'instant le lecteur devra faire appel à ses souvenirs de collégien pour tirer de (15) les égalités suivantes :

$$\begin{aligned} \sum_{i=0}^{s'} i &= \frac{s(s+1) + 2(s+1)}{2} = \frac{s^2 + s + 2s + 2}{2} \\ &= \frac{(s+1)(s+2)}{2} = \frac{s'(s'+1)}{2} \end{aligned}$$

qui clôturent la preuve. □

REMARQUE 3.2. Avant de poser un nouveau problème, interrogeons-nous sur les différences entre les deux preuves précédentes. Une différence est claire et a déjà été remarquée : la première est une preuve directe, c'est-à-dire qu'elle ne demande pas que le résultat qu'on veut obtenir soit déjà connu, et même pas qu'on avance une conjecture énonçant ce résultat ; la deuxième est une preuve indirecte, c'est-à-dire qu'elle part d'une hypothèse énonçant ce résultat. Ce n'est pourtant pas la seule différence. Une autre réside dans le fait que dans la première preuve, on opère sur un symbole, à savoir « $U_n$ », avant de savoir quel nombre il représente, et même avant de savoir comment calculer raisonnablement ce nombre, une

fois que $n$ a été déterminé. Dit d'une autre manière, on suppose connu le résultat cherché, on l'indique par un symbole convenable et on opère sur ce résultat, en exploitant le fait que (à cause de la fermeture de $\mathbb{N}$ relativement à l'addition) ce résultat est sans doute un nombre naturel et doit donc se comporter comme tous les nombres naturels se comportent. Depuis Aristote, les philosophes appellent « analyse » ce type de procédure : dans l'analyse on suppose connu ce qui est cherché et on opère sur celui-ci comme s'il était donné. Les mathématiciens utilisent souvent des procédures de cette sorte, même s'ils ne remarquent plus leur caractère analytique.

NOTE HISTORIQUE 3.1. La distinction entre analyse et synthèse, ou entre analytique et synthétique, a accompagné les mathématiques depuis l'antiquité. Elle a pourtant pris, dans divers contextes historiques et mathématiques, des significations si différentes qu'on est tenté de croire qu'en employant ces termes on ait voulu et on veuille se référer à différentes distinctions qui n'ont entre elles rien ou presque rien en commun. Mon opinion est cependant fort différente. Bien que je reconnaisse la grande variété de significations qui se cachent derrière ces termes, il me semble que ces différentes significations se réclament toutes d'un noyau commun et qu'il est même possible, avec un peu de patience, de reconstruire le parcours historique qui a conduit à l'émergence de ces significations à partir d'une même origine historique.

Cette origine historique correspond, il me semble, à la théorie aristotélicienne de l'analyse. Le terme « analyse » est utilisé par Aristote pour indiquer une forme d'argumentation, un certain type de cheminement de la pensée. Ce qui caractérise une analyse est, d'après Aristote, le fait que le point de départ de l'argument n'est pas donné, mais qu'il est plutôt à atteindre. Un argument analytique suppose, imagine que ce qu'il faut atteindre est donné, et, en partant de cette supposition, cherche à déterminer, à rebours, le processus qui conduit de ce qui est effectivement donné, à ce qui ne l'est pas encore. L'argument analytique s'arrête après avoir indiqué un point de départ possible pour ce processus, et avoir suggéré des moyens pour le mettre en marche et le conduire. À ce point, si on veut atteindre le but qu'on s'est donné, il faut changer d'attitude, agir ou penser d'une autre manière. La nature de cette phase deuxième, qui suit l'analyse, apparaît à Aristote différente selon les divers cas auxquels un argument analytique peut s'appliquer. En suivant une habitude qui était probablement installée parmi les mathématiciens de son temps, et dont on retrouve des exemples dans le *Traité sur la sphère et le cylindre* d'Archimède, Aristote utilise (une seule fois) le terme « synthèse » pour indiquer cette phase deuxième, qui suit une analyse, seulement pour se référer aux constructions géométriques qui suivent une analyse appliquée à la détermination des procédures constructives qui amènent à l'exhibition d'un objet géométrique satisfaisant à une certaine définition ou à certaines conditions. Dans ce cas, le terme « synthèse » pouvait en effet être utilisé dans sa signification habituelle, pour indiquer une composition, une construction. Ce fut probablement Pappus qui, autour du IV$^{\text{ème}}$ siècle av. J.C., commença à utiliser le terme « synthèse » pour se référer en général à toute procédure qui suit une analyse et est suggérée par celle-ci : une procédure où on ne peut que partir de ce qui est donné et travailler sur ceci, pour parvenir enfin à atteindre ce qui est cherché.

Pappus utilisa donc les termes « analyse » et « synthèse » pour se référer à une méthode générale en deux phases distinctes et successives (l'analyse et la synthèse). Cette méthode pouvait, d'après lui, s'appliquer autant à la solution de problèmes qu'à la démonstration de théorèmes. Ce fut à partir du début du XVII$^{\text{ème}}$ siècle que, grâce aux acquisitions, entre autres, de Viète et Descartes, on commença à penser que

la phase analytique, dans la solution d'un problème géométrique, pouvait prendre la forme d'un calcul formel, employant les notations et les règles de l'algèbre, et consistant d'abord en une succession d'équations se transformant les unes en les autres, et puis en la solution formelle d'une de ces équations. Dans l'idée de Viète et de Descartes, cette solution finale devait servir à suggérer une synthèse, c'est-à-dire une construction géométrique apte à résoudre le problème donné. Graduellement, la phase analytique de cette méthode acquit son autonomie. On commença à envisager et à formuler des problèmes nouveaux, qui pouvaient être conçus comme étant résolus lorsqu'on avait exhibé une équation ou qu'on l'avait résolue formellement. C'est l'origine de l'analyse comme théorie mathématique, une origine dont le pronoteur principal fut probablement Newton.

Pour comprendre comment, à partir des conceptions d'Aristote, on est arrivé aux autres nombreuses significations des termes « analyse » et « synthèse », il faudrait se pencher sur un grand nombre de textes et de questions. Je ne peux ici qu'indiquer au lecteur combien cette recherche pourrait être instructive et fascinante.

**Lectures possibles** : B. Timmermans, *La solution des problèmes de Desartes à Kant*, PUF, Paris, 1995 ; M. Otte et M. Panza, éds., *Analysis and Synthesis in Mathematics. History and Philosophy*, Kluwer A. P., Dordrecht, Boston and London, 1997 ; J.-L. Gardies *Qu'est-ce que et pourquoi l'analyse ? Essai de définition*, Vrin, Paris, 2001.

Remarque 3.3. On pourrait penser que ce qui vient d'être dit du nombre $U_n$ vaut aussi pour les nombres $s$ ou $\sum_{i=0}^{s} i$ de la deuxième preuve. Ceci est en un sens vrai, même s'il faut remarquer que $U_n$ est un nombre supposé connu (ou dont on suppose connue la relation opérationnelle cherchée, qui le lie au nombre $n$), que $s$ est une variable indépendante (car aucune détermination préalable n'est susceptible de la fixer), et enfin que $\sum_{i=0}^{s} i$ est une variable qui dépend d'une autre variable, justement de $s$, par une relation opérationnelle qu'on connaît parfaitement. Pourtant, au-delà de ces différences, une analogie profonde demeure entre les deux procédures, au point que certains philosophes pourraient croire que la deuxième aussi est au fond une procédure analytique. Cette analogie peut être vue sous un autre angle : les deux preuves parviennent à démontrer un résultat général — un théorème qui s'applique à n'importe quel nombre naturel $n$, c'est-à-dire à tout nombre naturel et même à tous les nombres naturels — en ne considérant que des archétypes de ces nombres, sous la forme de quelques symboles littéraux convenables. C'est une possibilité typique des mathématiques que d'opérer sur des structures symboliques individuelles qui expriment des formes. Ceci permet de travailler sur des formes à l'aide d'objets parfaitement concrets et déterminés. Kant a caractérisé cet aspect saillant des mathématiques en disant que celles-ci opèrent sur l'universel *in concreto*. Je ne connais rien de plus profond et fondamental qu'un philosophe ait dit pour guider notre effort de compréhension du phénomène mathématique.

Note Historique 3.2. Lors de la séance du 28 mai 1761, la classe de philosophie de l'Académie de Berlin, proposa, pour le prix de 1763, la question suivante : « On demande si les vérités de la métaphysique en général et, en particulier, les premiers principes de la théologie naturelle et de la morale sont susceptibles de la même évidence que les vérités mathématiques et, au cas qu'elles n'en seraient pas susceptibles, quelle est la nature de leur certitude, à quel degré elles peuvent parvenir, et si ce degré suffit à la conviction ».

En 1761, Kant avait trente-sept ans et il était *privatdocent* à l'université de Königsberg, sa ville natale, où il enseignait les sujets les plus divers, des mathématiques, aux sciences naturelles, à la géographie physique, jusqu'à la théologie et à la philosophie ; il avait déjà postulé deux fois, sans succès, pour obtenir, à la même université, la chaire de logique et métaphysique, qu'il obtiendra enfin en 1770. Le sujet du prix de l'Académie était tout à fait adapté à ses intérêts et à ses compétences, et il décida de participer au concours, avec un mémoire auquel il donna le titre suivant : « Recherche sur l'évidence des principes de la théologie naturelle et de la morale ». Comme il arrive souvent, ce ne fut pas le meilleur qui obtint le prix de l'Académie, qui alla à Moses Mendelssohn. Kant obtint néanmoins une mention, ce qui le poussa à publier son essai en 1764.

Cet essai est divisé en quatre « considérations », dont la première concerne une « comparaison générale entre la manière de parvenir à la certitude dans la connaissance mathématique et celle d'y parvenir en philosophie ». Kant y discute quatre différences entre les démarches des mathématiques et de la philosophie : les mathématiques parviennent à leurs définitions synthétiquement, la philosophie y parvient analytiquement ; les mathématiques considèrent le général *in concreto*, la philosophie le considère *in abstracto* ; en mathématiques, il y a un petit nombre de concepts inanalysables et de propositions indémontrables, en phylosopie il y en a beaucoup ; l'objet des mathématiques est simple et facile, celui de la philosophie est difficile et complexe. Comme on le voit, ce sont des ingrédients fondamentaux de ce qui deviendra plus tard la philosophie des mathématiques de Kant. Cependant, dans l'essai de 1763, ce dernier a encore du mal à relier entre eux ces ingrédients et, même dans la *Critique de la raison pure*, la manière selon laquelle il pensera un objet, l'empêchera, il me semble, de saisir le lien profond entre la deuxième différence et la nature synthétique des jugements mathématiques.

Voici, comment, dans l'essai de 1763, il expose cette deuxième différence : « Dans [...] [l'arithmétique] sont d'abord posés, à la place des choses mêmes, leurs signes avec la désignation particulière de leur accroissement ou de leur diminution, de leurs rapports, etc., et on procède ensuite, avec ces signes, selon des règles simples et certaines [...] de telle manière que les choses signifiées elles-mêmes y sont laissées entièrement en dehors de la pensée, jusqu'à ce qu'à la fin, dans la conclusion, la signification de la conséquence soit déchiffrée. [...] en géométrie, pour connaître, par exemple, les propriétés de tous les cercles, on en trace un dans lequel, à la place de toutes les lignes possibles qui se coupent à l'intérieur de celui-ci, on en tire deux d'entre elles. On démontre les rapports de ces lignes et l'on considère en ceux-ci la règle générale des rapports des lignes qui se croisent dans tous les cercles *in concreto*. Si l'on compare à ce procédé celui de la philosophie, on le trouvera entièrement différent. Les signes qu'utilise la réflexion philosophique ne sont jamais autre chose que des mots qui ne font pas voir, dans leur assemblage, les concepts partiels dont est constituée l'idée complète désignée par le mot, ni ne peuvent exprimer, dans leur combinaison, les rapports des pensées philosophiques ».

Dans la *Critique de la raison pure*, Kant sera bien plus clair : « Que l'on donne à un philosophe le concept d'un triangle, et qu'on le laisse découvrir à sa manière le rapport de la somme des angles de ce triangle à l'angle droit. Il n'a rien que le concept d'une figure renfermée entre trois lignes droites, et dans cette figure le concept d'un nombre égal d'angles. Cela étant, il aura beau réfléchir sur ce concept aussi longtemps qu'il voudra, il n'en tirera rien de nouveau. Il peut analyser et éclaircir le concept de

la ligne droite, ou celui d'un angle, ou celui du nombre trois, mais non pas arriver à d'autres propriétés qui ne se trouvent pas du tout dans ces concepts. Mais que le géomètre s'attaque à cette question, il commence aussitôt par construire un triangle. Comme il sait que deux angles droits pris ensemble valent exactement autant que les angles adjacents qui peuvent être tracés à partir d'un point pris sur une ligne droite, il prolonge un côté de son triangle et obtient ainsi deux angles adjacents qui sont égaux à deux droits. Il partage ensuite l'angle externe, en tirant une ligne parallèle au côté opposé du triangle, et il voit qu'il en résulte un angle externe adjacent qui est égal à un angle interne, etc. De cette façon, il arrive par une chaîne d'inférences, toujours guidé par l'intuition, à une solution parfaitement évidente et en même temps universelle de la question ».

Naturellement, ce que Kant veut dire ce n'est pas simplement que les mathématiques font usage, à la différence de la philosophie, de symboles et de règles aptes à soulager l'entendement, comme avait dit Leibniz. Le point de Kant est plutôt que ces symboles et ces règles exhibent en même temps un objet particulier et spatio-temporellement déterminé, sur lequel on peut travailler, pour ainsi dire à la main, et une entité universelle (Kant ne dira jamais, malheureusement, un objet pur), dont les propriétés se lisent directement à partir du résultat de ces opérations concrètes. Cela n'est pas seulement une facilité que les mathématiques se concèdent. C'est une possibilité qui dérive de la nature et des modalités de donation des objets mathématiques. Et c'est justement en observant cette possibilité, qui caractérise essentiellement les mathématiques, que Kant me semble avoir apporté, par sa réflexion, une contribution majeure à la compréhension de cette nature et de ces modalités.

**Lectures possibles** : I. Kant, « Recherche sur l'évidence des principes de la théologie naturelle et de la morale », E. (*sic*!) Kant, *Œuvres philosophiques*, Gallimard, Paris, vol. I, 1980, pp. 205-249 ; M. Panza, « Mathematics acts of reasoning as synthetic *a priori* », *in* M. Otte and M. Panza (ed.), *Analysis and synthesis in Mathematics*, Kluwer, Dordrecht, Boston, London, 1997, pp. 273-326.

Du théorème 1.1 on peut tirer un résultat qui est, au moins apparemment, encore plus général. Ce résultat est exprimé par le théorème suivant :

THÉORÈME 1.2. *Si $n$, $p$ et $q$ sont trois nombres naturels quelconques, alors :*

$$\sum_{i=0}^{n}(p+iq) = \frac{(n+1)(2p+nq)}{2}$$

**Preuve** Grâce à la commutativité et l'associativité de l'addition et à la distributivité de la multiplication sur l'addition, ces opérations étant définies sur $\mathbb{N}$, on aura

$$\begin{aligned}\sum_{i=0}^{n}(p+iq) &= (p)+(p+q)+(p+2q)+...+(p+nq)\\ &= (n+1)p+(0+1+2+...+n)q\\ &= (n+1)p+\left[\sum_{i=0}^{n} i\right]q\end{aligned}$$

De là, suivant le théorème 1.1 et l'algorithme d'addition des nombres fractionnaires déjà employé ci-dessus, on conclut aisément que :

$$\begin{aligned}\sum_{i=0}^{n}(p+iq) &= (n+1)p+\left[\frac{n(n+1)}{2}\right]q \\ &= \frac{2(n+1)p+n(n+1)q}{2} = \frac{(n+1)(2p+nq)}{2}\end{aligned}$$

ce qu'il s'agissait justement de démontrer. □

Il est clair que si $p=0$ et $q=1$, ce résultat est le même que celui exprimé par le théorème 1.1, qui n'est qu'un cas particulier du théorème 1.2.

Si on analyse l'énoncé du théorème précédent et la preuve correspondante, on comprend facilement que les trois nombres naturels $n$, $p$ et $q$ y jouent des rôles fort différents. Si $n$ y fonctionne en effet comme un indice qui détermine le nombre des termes qu'on additionne l'un à l'autre, $p$ et $q$ n'y interviennent que comme des termes quelconques qui s'additionnent entre eux et se multiplient par $1, 2, ..., n, n+1$. Ainsi, si on substitue à $n$ un élément quelconque, disons $x$, d'un ensemble quelconque $E$ distinct de $\mathbb{N}$ (et de tout sous-ensemble de $\mathbb{N}$), on ne sait plus quelle signification il faut donner à l'écriture « $\sum_{i=0}^{x}(p+iq)$ » qui résultera de cette substitution, et notre problème perdra ainsi son sens. Au contraire, si on substitue à $p$ et $q$ deux éléments $a$ et $b$ d'un ensemble $E$ distinct de $\mathbb{N}$, sur lequel on a défini une addition associative et commutative et telle que, pour tout nombre naturel $m$, si $x$ est un élément de $E$, alors $\underbrace{x+x+...+x}_{m \text{ fois}} = m \cdot x$, de sorte que cette multiplication entre un nombre naturel et un élément de $E$ est distributive sur l'addition définie sur $E$, alors toutes les étapes de la preuve précédente peuvent être répétées, et la nouvelle démonstration portera évidemment au même résultat que ci-dessus :

$$\sum_{i=0}^{n}(a+ib) = \frac{(n+1)(2a+nb)}{2}$$

Plus particulièrement, on peut supposer que $a$ et $b$ soient des quantités quelconques ; des temps, des segments, des angles, ou, plus généralement, des nombres réels (sur lesquels on viendra dans le chapitre 6). Il ne sera pas nécessaire ici de donner une définition plus précise du terme « quantité quelconque » ; on reviendra sur ce point dans les chapitres 5 et 6. Ici, il suffit d'accepter que les quantités se comportent relativement à l'addition et à la multiplication avec des nombres naturels comme l'on vient de dire que les éléments de $E$ se comportent. Il n'est pas difficile de comprendre que ce doit être le cas quelles que soient ces quantités. S'il s'agit, par exemple, d'additionner 3 minutes à 4 minutes, on ne s'intéressse pas aux minutes, mais aux nombres 3 et 4 ; il en sera de même pour des segments ou des angles égaux. Ainsi si $\gamma$ est un certain temps, un segment ou un angle, ou n'importe quelle autre quantité, il est certain que trois $\gamma$ plus quatre $\gamma$ font sept $\gamma$ : $3\gamma + 4\gamma = (3+4)\gamma = 7\gamma$.

Le théorème 1.2 pourra alors se formuler ainsi

THÉORÈME 1.3. *Si $n$ est un nombre naturel quelconque et $a$ et $b$ sont deux quantités quelconques, alors :*

$$\sum_{i=0}^{n}(a+ib) = \frac{(n+1)(2a+nb)}{2}$$

Il est clair que ce théorème se prouvera exactement comme le théorème 1.2, en substituant à « $p$ » et « $q$ » respectivement « $a$ » et « $b$ ». Ce dernier théorème résulte ainsi n'être, en dernière instance, qu'un corollaire du théorème 1.1.

Ceci nous montre qu'en mathématiques, on peut parfois généraliser de façon puissante un résultat particulier en ne s'appuyant que sur des remarques très simples. Nous comprenons du coup que la relation entre le particulier et le général n'est pas la même en mathématiques qu'ailleurs. Souvent un résultat mathématique très général ne contient d'essentiel que ce qui est déjà contenu dans un de ses cas particuliers. Le lecteur saisira lui-même que ceci dépend du fait, déjà noté, qu'un résultat mathématique peut s'exprimer souvent par une formule qui est en même temps l'objet d'un calcul et l'expression d'une forme.

Ceci n'empêche pas pourtant qu'une généralisation obtenue de cette manière soit plus informative que le cas particulier à partir duquel elle est démontrée. C'est le cas du résultat énoncé dans le théorème 1.2, qui nous fournit la formule de sommation de n'importe quelle réduite partielle d'une série arithmétique quelconque. Pour comprendre ceci, concentrons notre attention sur l'addition $\sum_{i=0}^{n}(a+ib)$, plutôt que sur la recherche de sa somme. Il est clair que si on pose $u_i = a + ib$, on aura, quel que soit le nombre naturel $i$,

$$u_{i'} - u_i = u_{i+1} - u_i = a + (i+1)b - a - ib = b$$

L'addition $\sum_{i=0}^{n}(a+ib)$ est donc telle que pour passer d'un quelconque de ses termes au terme qui le suit immédiatement, il suffit d'additionner au terme donné un terme constant. Si le premier terme de cette somme est $a$ et le terme constant est $b$, alors le deuxième sera $a+b$, le troisième $(a+b)+b = a+2b$, le quatrième $(a+2b)+b = a+3b$, etc. Une telle addition, réitérée à l'infini, est dite par les mathématiciens « série arithmétique ». L'addition qui fait l'objet du théorème 1.2 est ainsi la *réduite partielle d'ordre n* d'une série arithmétique et sa somme est la *somme partielle* d'une telle série.

REMARQUE 3.4. Pour indiquer qu'une addition $u_0 + u_1 + u_2 + etc.$ est réitérée à l'infini, c'est-à-dire qu'on imagine d'additionner les unes aux autres toutes les valeurs de $u_i$, données par toutes les positions $i = 0\ , i = 1,\ i = 2, ...$, les mathématiciens utilisent le symbole « $\sum_{i=0}^{\infty} u_i$ », le symbole « $\infty$ » étant habituellement utilisé pour indiquer l'infini (le lecteur comprendra mieux l'idée d'une addition infinie après avoir lu le paragraphe 2).

Il est facile de comprendre que toute série arithmétique peut s'écrire sous la forme « $\sum_{i=0}^{\infty}(a+ib)$ », pourvu que $a$ et $b$ soient des quantités — dites respectivement « base » et « raison » de la série arithmétique — qu'on peut déterminer comme on veut, car la seule condition qu'une addition infinie $\sum_{i=0}^{\infty} u_i$ (c'est-à-dire une série) doive respecter pour être une série arithmétique est que pour tout $i$, on ait

$$u_{i'} = u_i + b$$

$b$ étant une constante quelconque. Ainsi, une série arithmétique est complètement déterminée dès qu'on connaît sa base et sa raison. Le théorème 1.2 nous fournit dès lors la somme d'une réduite partielle d'ordre quelconque d'une série arithmétique quelconque, et sa preuve nous montre que cette somme peut toujours être exprimée dans les termes de la somme des premiers $n+1$ nombres naturels.

Remarque 3.5. Pour ce qui est de la somme d'une série arithmétique quelconque, le lecteur est renvoyé au paragraphe 2.

## 2. Somme partielle d'une série géométrique quelconque

À côté des séries arithmétiques, d'autres séries ont pour les mathématiciens un intérêt particulier. Il s'agit des séries dites « géométriques », c'est-à-dire des additions $\sum_{i=0}^{\infty} u_i$, telles que, pour tout $i$, on ait

$$u_{i'} = u_{i+1} = u_i \cdot b$$

$b$ étant encore un terme constant, différent de 1. Il est facile de voir que toute série géométrique peut s'écrire sous la forme générale

$$\sum_{i=0}^{\infty} \left(a \cdot b^i\right) = a + ab + ab^2 + ab^3 + ... + ab^n + ...$$

(où, quel que soit le nombre $m$, $b^m = \underbrace{b \cdot b \cdot ... \cdot b}_{m \text{ fois}}$), de sorte que si $\sum_{i=0}^{\infty} u_i$ est une série géométrique, on aura, pour tout $i$, $u_i = ab^i$, avec $a = u_0$ la « base » de la série géométrique et $b \neq 1$ sa « raison ». Supposons d'abord que $a$ et $b$ soient des nombres naturels, qu'on notera respectivement par « $p$ » et « $q$ ». On aura alors le théorème suivant :

Théorème 2.1. *Si $n$ et $p$ sont des nombres naturels quelconques et $q$ un nombre naturel différent de* 1*, alors :*

$$\sum_{i=0}^{n} \left(p \cdot q^i\right) = p\frac{1 - q^{n+1}}{1 - q}$$

Avant de prouver ce théorème, il faut remarquer que si dans la somme $p\frac{1-q^{n+1}}{1-q}$ de la réduite partielle d'ordre $n$ d'une série géométrique quelconque, on posait $q = 1$, on aurait le produit $p\frac{0}{0}$, et $\frac{0}{0}$ non seulement n'est pas un nombre naturel (d'après le théorème 5.3) mais n'est même pas (comme on le verra dans le chapitre 4), une quantité déterminée et déterminable. Ceci explique la demande que $q$ soit différent de 1. D'ailleurs, si $q = 1$, l'addition $\sum_{i=0}^{n} \left(p \cdot q^i\right)$ se transforme en $\sum_{i=0}^{n} p = (n + 1)p$ qui non seulement est facile à calculer, mais est aussi la réduite partielle d'ordre $n$ d'une série arithmétique de base $p$ et de raison 0. La position $q \neq 1$ ne réduit donc pas la généralité du théorème 2.1.

Comme dans le cas précédent, on donnera ici deux preuves de ce théorème, la première directe, et la deuxième indirecte et par induction complète. Les voici.

**Preuve du théorème 2.1** On fait l'hypothèse que

$$\sum_{i=0}^{n} \left(p \cdot q^i\right) = U_n$$

De là il suit que

$$q\left[\sum_{i=0}^{n} \left(p \cdot q^i\right)\right] = q \cdot U_n$$

et donc

$$\sum_{i=0}^{n}\left(p\cdot q^i\right)-q\left[\sum_{i=0}^{n}\left(p\cdot q^i\right)\right]=U_n-qU_n=\left(1-q\right)U_n$$

Mais, en explicitant les additions, on aura naturellement

$$\begin{aligned}\sum_{i=0}^{n}\left(p\cdot q^i\right)-q\left[\sum_{i=0}^{n}\left(p\cdot q^i\right)\right] &= \left\{\begin{array}{l}\left(p+pq+pq^2+...+pq^n\right)-\\ \quad q\cdot\left(p+pq+pq^2+...+pq^n\right)\end{array}\right.\\ &= \left\{\begin{array}{l}p+(pq-pq)+(pq^2-pq^2)+\\ \quad ...+(pq^{n-1}-pq^{n-1})-pq^{n+1}\end{array}\right.\\ &= p-pq^{n+1}=p(1-q^{n+1})\end{aligned}$$

donc :

$$(1-q)U_n=p(1-q^{n+1})$$

et, si $q\neq 1$,

$$U_n=p\frac{1-q^{n+1}}{1-q}$$

ce qu'il fallait démontrer. □

**Preuve du théorème 2.1 (par induction complète)** La preuve a naturellement deux étapes :

($a$) Si $n=0$, on aura (car, comme l'on le verra, $q^0=1$, pour tout $q$) :

$$\begin{aligned}\sum_{i=0}^{n}\left(p\cdot q^i\right) &= \sum_{i=0}^{0}\left(p\cdot q^i\right)=p\\ p\frac{1-q^{n+1}}{1-q} &= p\frac{1-q}{1-q}=p\end{aligned}$$

et la conjecture $\sum_{i=0}^{n}\left(p\cdot q^i\right)=p\frac{1-q^{n+1}}{1-q}$ est vérifiée dans ce cas.

($b$) Il ne nous reste donc qu'à prouver que, quel que soit le nombre naturel $s$, on a

$$\left[\sum_{i=0}^{s}\left(p\cdot q^i\right)=p\frac{1-q^{s+1}}{1-q}\right]\Rightarrow\left[\sum_{i=0}^{s'}\left(p\cdot q^i\right)=p\frac{1-q^{s'+1}}{1-q}\right]$$

Or,

$$\sum_{i=0}^{s'}\left(p\cdot q^i\right)=\sum_{i=0}^{s+1}\left(p\cdot q^i\right)=\left[\sum_{i=0}^{s}\left(p\cdot q^i\right)\right]+pq^{s+1}$$

et donc, si $\sum_{i=0}^{s} (p \cdot q^i) = p\frac{1-q^{s+1}}{1-q}$, alors (suivant l'algorithme d'addition des nombres fractionnaires)

$$\begin{aligned}
\sum_{i=0}^{s'} (p \cdot q^i) &= p\frac{1-q^{s+1}}{1-q} + pq^{s+1} \\
&= p\frac{\left(1-q^{s+1}\right) + (1-q)\, q^{s+1}}{1-q} \\
&= p\frac{1-q^{s+1}+q^{s+1}-q^{s+2}}{1-q} \\
&= p\frac{1-q^{s+2}}{1-q} = p\frac{1-q^{s'+1}}{1-q}
\end{aligned}$$

ce qui conclut la preuve □

Le théorème 2.1 ayant été prouvé, voyons sous quelles conditions les nombres naturels $p$ et $q$ peuvent être remplacés (autant dans l'énoncé que dans la preuve de ce théorème) par des éléments d'un ensemble $E$ distinct de $\mathbb{N}$. Il est facile de vérifier que, à différence que dans le théorème 1.2, les nombres $p$ et $q$ ne sont pas seulement additionnés entre eux et multipliés par des nombres naturels. Ils sont aussi multipliés entre eux. Or, si on pense la multiplication comme une addition réitérée, il apparaît difficile de comprendre ce que pourrait signifier multiplier deux quantités (par exemple deux segments, deux angles ou deux temps) entre elles. Rien n'empêche, évidemment, de définir formellement sur $E$ une multiplication en définissant une application de $E^2$ à $E$. Evidemment, si $E$ n'est pas une progression, on ne pourra procéder par récurrence, mais rien ne nous pousse à penser qu'une telle définition ne soit pas possible. Pourtant, si on ne sait pas assigner un sens informel à la multiplication entre deux quantités, un sens qu'une telle définition formelle devrait viser à exprimer, cette dernière définition apparaîtra, quelle qu'elle soit, comme arbitraire. Ceci a été pendant plusieurs siècles un obstacle de taille à la possibilité de développer une algèbre des grandeurs géométriques.

NOTE HISTORIQUE 3.3. Imaginons que $n$ et $m$ soient deux nombres entiers positifs. D'après la définition 4.3, la multiplication $n \cdot m$ correspond à la somme $\underbrace{n+n+...+n}_{m \text{ fois}}$. Comme on l'a déjà observé, elle est donc une opération essentiellement distincte de la multiplication $m \cdot n$, qui correspond plutôt à la somme $\underbrace{m+m+...+m}_{n \text{ fois}}$. Si on passe de la théorie des nombres entiers positifs, définis comme collections de traits verticaux, à la théorie des nombres naturels, et que l'on suppose la définition 3.1 avec sa conséquence donnée par le théorème 3.3, cette différence disparaît. Pourtant, j'ai souvent insisté ci-dessus sur le fait que les axiomes et les définitions de la théorie des nombres naturels n'ont d'autre but que de permettre de retrouver comme théorèmes les propriétés déjà connues des nombres entiers positifs, définis comme collections de traits verticaux. La commutativité de la multiplication définie sur les nombres naturels exprime donc l'identité entre les produits des multiplications $n \cdot m$ et $m \cdot n$, référées aux nombres entiers positifs définis comme collections de traits verticaux. En exprimant cette identité, une telle condition cache pourtant la différence essentielle entre ces deux multiplications. Or, cette différence met bien en évidence le fait suivant : dans la multiplication $n \cdot m$, les nombres entiers positifs $n$ et $m$ ne jouent pas le même rôle : le premier est le terme d'une addition, tandis que le deuxième indique

combien de fois cette addition doit être réitérée. Si on peut multiplier deux nombres entiers positifs entre eux (et obtenir comme produit un nombre entier positif) ce n'est donc que parce que le terme de l'addition qu'on veut réitérer est, dans ce cas, tel qu'il peut aussi indiquer combien de fois cette addition doit être réitérée.

Soit maintenant $a$ une quantité quelconque. Il est clair qu'on peut additionner $a$ à elle-même autant de fois qu'on veut, disons $n$ fois. Cette addition réitérée pourra être conçue comme une multiplication de la quantité $a$ par le nombre entier positif $n$. Cela donne un sens à la multiplication $a \cdot n$. On peut certes décider, lorsque $a$ n'est pas un nombre entier positif, de supposer par convention que l'écriture « $n \cdot a$ » est équivalente à l'écriture « $a \cdot n$ », mais on ne peut pas penser que cette dernière écriture indique une addition réitérée du nombre entier positif $n$ un nombre $a$ de fois. On comprend alors que si $a$ et $b$ ne sont pas des nombres entiers positifs, l'écriture « $a \cdot b$ » ne peut pas indiquer une addition réitérée. Si on veut donc donner un sens à cette écriture, il faut abandonner l'espoir de faire reposer ce sens sur le sens de l'opération d'addition définie sur des quantités telles que $a$ et $b$, de la même manière que le sens de l'écriture « $n \cdot m$ » repose sur le sens de l'opération d'addition définie sur les nombres entiers positifs. Le lien qui subsiste entre l'addition et la multiplication, lorsqu'on à faire avec les nombres entiers positifs, ne peut donc pas continuer à subsister dans ce cas : addition et multiplication apparaissent comme deux opérations essentiellement distinctes.

Dans les mathématiques grecques, la multiplication entre deux quantités autres que des nombres entiers positifs n'était simplement pas définie. Plus tard, on commença à utiliser l'écriture multiplicative référée à des segments pour indiquer le rectangle construit sur ces segments. La raison est assez simple à comprendre. Si les deux segments $a$ et $b$ ont une mesure commune, c'est-à-dire qu'il y a un segment $c$ tel que les segments $a$ et $b$ sont respectivement égaux aux produits $c \cdot n$ et $c \cdot m$, $n$ et $m$ étant deux nombres entiers positifs convenables, alors le rectangle construit sur les segments $a$ et $b$ est composé de $n \cdot m$ carrés de côté $c$.

Dans la note historique 4.3 on discutera les définitions données par Euclide, dans les *Éléments*, de la relation de proportionnalité, respectivement référée à quatre nombres entiers et positifs et à quatre quantités quelconques, en particulier à quatre grandeurs (ou quantités continues). On observera qu'en accord avec la première de ces définitions, dire de quatre nombres entiers positifs qu'ils sont en proportion équivaut à affirmer une égalité dont les deux termes sont donnés chacun par un produit de deux nombres entiers positifs. Dans ce cas, il est donc aisé de passer d'une proportion à une équation. En revanche, dire de quatre grandeurs qu'elles sont en proportion n'équivaut nullement, en accord avec la deuxième de ces définitions, à affirmer une égalité entre deux produits. Dans ce cas, le passage d'une proportion à une équation est donc impossible. C'est pour cette raison que, jusqu'au XVII$^{\text{ème}}$ siècle la théorie des équations se développa de manière indépendante de la théorie des proportions, la première se référant aux nombres entiers positifs et la deuxième aux grandeurs.

L'objectif d'une unification de la théorie des nombres entiers positifs et de celle des grandeurs, en une seule théorie des quantités fut finalement atteint, après maints efforts, par Descartes qui donna, le premier, dans sa *Géométrie* de 1637, une définition satisfaisante de la multiplication entre grandeurs. On comprendra que cette unification fut en même temps une réduction de la vieille théorie des proportions entre grandeurs à une nouvelle théorie des équations portant sur n'importe quelle sorte de

quantités. Ce sera justement cette théorie qui donnera origine, un peut plus tard, à l'analyse et, à l'intérieur de celle-ci, au calcul infinitésimal.

**Lectures possibles** : V. Jullien, *Descartes, la Géométrie de* 1637, PUF, Paris, 1996.

Dans les chapitres 4 et 6, on verra comment on peut définir non arbitrairement une multiplication sur les ensembles $\mathbb{Q}$ et $\mathbb{R}$ respectivement des nombres rationnels et des nombres réels. Pour l'instant, il suffira de supposer que $a$ et $b$ sont deux éléments d'un ensemble $E$, sur lequel sont définies une addition et une multiplication associatives et commutatives, telles que la multiplication est distributive sur l'addition. On n'aura alors qu'à supposer que $n \cdot x = \underbrace{x + x + ... + x}_{n \text{ fois}}$ pour pouvoir poser $a$ et $b$ à la place de $p$ et $q$, autant dans l'énoncé que dans la preuve du théorème 2.1, ce qui nous permettra d'obtenir sur le champ le théorème suivant, qui fournit la somme partielle de n'importe quelle réduite partielle d'une série géométrique :

THÉORÈME 2.2. *Si $n$ est un nombre naturel quelconque, $a$ une quantité quelconque et $b$ une quantité quelconque différente de* 1*, alors*

$$\sum_{i=0}^{n} \left(a \cdot b^i\right) = a\frac{1 - b^{n+1}}{1 - b}$$

### 3. Sommes des premiers $n + 1$ carrés et des premiers $n + 1$ cubes

Dans les exemples donnés par les théorèmes 1.1 et 2.1, la preuve par induction complète n'intervient qu'en deuxième instance, lorsqu'une autre preuve a déjà assuré la validité du théorème. Les deux preuves n'ont été données que pour montrer des inductions complètes à l'œuvre. Comme on l'a déjà vu dans le chapitre 2, il y a pourtant des cas où une preuve par induction complète est nécessaire, faute de mieux, ou du moins où elle est plus simple et rapide qu'une preuve directe. Dans le chapitre 2, on a utilisé des preuves par induction complète pour s'assurer de certaines propriétés des opérations d'addition et de multiplication qu'on avait définies auparavant de manière à leur conférer ces propriétés. La conjecture que la preuve par induction complète transformait en théorème se présentait ainsi tout naturellement à l'esprit : elle faisait partie en quelque sorte d'un programme fixé à l'avance.

Dans d'autres cas, c'est plutôt la considération des propriétés des premiers nombres naturels qui suggère une conjecture qui sera validée plus tard par une preuve par induction complète. Dans ce cas, deux sortes d'inductions participent à la même tâche : d'abord une induction simple suggère une généralisation ; ensuite une induction complète transforme cette généralisation en théorème. Deux exemples sont donnés par les théorèmes qui fournissent respectivement la somme des premiers $n + 1$ carrés et des premiers $n + 1$ cubes.

La signification du symbole « $p^q$ », où $p$ et $q$ sont deux nombres entiers naturels, a été donnée dans le chapitre 1. Évidemment, rien ne change si on considère $p$ et $q$ comme des nombres naturels. Ici, on ajoutera que si $q = 2$ on appelle cette puissance un « carré », et si $q = 3$ on l'appelle un « cube », de sorte que les symboles « $p^2$ » et « $p^3$ » indiquent respectivement le carré de $p$ et le cube de $q$. La raison de cette convention linguistique n'est guère difficile à imaginer, ainsi que son origine géométrique.

Les problèmes de la somme des premiers $n+1$ carrés et des premiers $n+1$ cubes consistent ainsi respectivement à rechercher deux formules qui, lorsque la valeur du nombre $n$ a été fixée, permettent de calculer rapidement la valeur des sommes $\sum_{i=0}^{n} i^2$ et $\sum_{i=0}^{n} i^3$. Voici comment l'on procède.

En posant respectivement $n = 0, 1, 2, 3, 4$ on obtient ;

$$\sum_{i=0}^{0} i^2 = 0^2 = 0 \qquad \sum_{i=0}^{0} i^3 = 0^3 = 0$$
$$\sum_{i=0}^{1} i^2 = 0 + 1 = 1 \qquad \sum_{i=0}^{1} i^3 = 0 + 1 = 1$$
$$\sum_{i=0}^{2} i^2 = 0 + 1 + 4 = 5 \qquad \sum_{i=0}^{2} i^3 = 0 + 1 + 8 = 9$$
$$\sum_{i=0}^{3} i^2 = 0 + 1 + 4 + 9 = 14 \qquad \sum_{i=0}^{3} i^3 = 0 + 1 + 8 + 27 = 36$$
$$\sum_{i=0}^{4} i^2 = 0 + 1 + 4 + 9 + 16 = 30 \qquad \sum_{i=0}^{4} i^3 = 0 + 1 + 8 + 27 + 64 = 100$$

Or, on peut vérifier que :

$$\sum_{i=0}^{2} i^2 = 5 = \frac{2 \cdot 3 \cdot 5}{6} \qquad \sum_{i=0}^{2} i^3 = 9 = \frac{(2 \cdot 3)^2}{4} = \frac{36}{4}$$
$$\sum_{i=0}^{3} i^2 = 14 = \frac{3 \cdot 4 \cdot 7}{6} \qquad \sum_{i=0}^{3} i^3 = 36 = \frac{(3 \cdot 4)^2}{4} = \frac{144}{4}$$
$$\sum_{i=0}^{4} i^2 = 30 = \frac{4 \cdot 5 \cdot 9}{6} \qquad \sum_{i=0}^{3} i^4 = 100 = \frac{(4 \cdot 5)^2}{4} = \frac{400}{4}$$

Comme il est clair que

$$\begin{aligned} \sum_{i=0}^{0} i^2 &= \sum_{i=0}^{0} i^3 = 0 = \frac{0 \cdot 1 \cdot 1}{6} = \frac{(0 \cdot 1)^2}{4} \\ \sum_{i=0}^{1} i^2 &= \sum_{i=0}^{1} i^3 = 1 = \frac{1 \cdot 2 \cdot 3}{6} = \frac{(1 \cdot 2)^2}{4} \end{aligned} \tag{16}$$

cela nous permet d'avancer les conjectures suivantes :

$$\begin{aligned} \sum_{i=0}^{n} i^2 &= \frac{n(n+1)(2n+1)}{6} \\ \sum_{i=0}^{n} i^3 &= \frac{\big[n(n+1)\big]^2}{4} \end{aligned}$$

qu'on espère valides pour tout nombre naturel $n$. Deux preuves par induction complète nous assurent que c'est bien le cas et nous permettent d'énoncer le théorème suivant :

THÉORÈME 3.1. *Si $n$ est un nombre naturel quelconque, alors :*

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

*et*

$$\sum_{i=0}^{n} i^3 = \frac{[n(n+1)]^2}{4}$$

**Preuve** Il s'agit évidemment de deux preuves indépendantes, les deux étant par récurrence. La première étape de ces deux preuves est fournie par la (16). Il ne nous reste donc qu'à prouver respectivement que pour tout nombre naturel $s$ on a :

$$\left[\sum_{i=0}^{s} i^2 = \frac{s(s+1)(2s+1)}{6}\right] \Rightarrow \left[\sum_{i=0}^{s'} i^2 = \frac{s'(s'+1)(2s'+1)}{6}\right]$$

et

$$\left[\sum_{i=0}^{s} i^3 = \frac{[s(s+1)]^2}{4}\right] \Rightarrow \left[\sum_{i=0}^{s'} i^3 = \frac{[s'(s'+1)]^2}{4}\right]$$

Ce n'est pas bien difficile. Pour la première implication, il suffit d'observer que si

$$\sum_{i=0}^{s} i^2 = \frac{s(s+1)(2s+1)}{6}$$

alors (suivant l'algorithme d'addition des nombres fractionnaires) :

$$\begin{aligned}
\sum_{i=0}^{s'} i^2 &= \sum_{i=0}^{s+1} i^2 = \left(\sum_{i=0}^{s} i^2\right) + (s+1)^2 \\
&= \frac{s(s+1)(2s+1)}{6} + (s+1)^2 \\
&= \frac{s(s+1)(2s+1) + 6(s+1)^2}{6} \\
&= \frac{(s+1)\left[s(2s+1) + 6(s+1)\right]}{6} \\
&= \frac{(s+1)\left[2s^2 + 7s + 6\right]}{6} \\
&= \frac{(s+1)(s+2)(2s+3)}{6} = \frac{(s')(s'+1)(2s'+1)}{6}
\end{aligned}$$

Quant à la deuxième implication, il suffit d'observer que, si

$$\sum_{i=0}^{s} i^3 = \frac{[s(s+1)]^2}{4}$$

alors, d'après l'algorithme d'addition et de multiplication des nombres fractionnaires, en observant que, quels que soient les nombres naturels $p$, $q$ et $m$,

$$\begin{aligned}
(p \cdot q)^m &= \underbrace{(p \cdot q) \cdot (p \cdot q) \cdot ... \cdot (p \cdot q)}_{m \text{ fois}} \\
&= (\underbrace{p \cdot p \cdot ... \cdot p}_{m \text{ fois}}) \cdot (
\end{aligned}$$

$$under set m \text{ fois} \underbrace{q \cdot q \cdot ... \cdot q}) = p^m \cdot q^m$$

il sera facile de tirer :

$$\begin{aligned}
\sum_{i=0}^{s'} i^3 &= \sum_{i=0}^{s+1} i^3 = \left(\sum_{i=0}^{s} i^3\right) + (s+1)^3 \\
&= \frac{[s(s+1)]^2}{4} + (s+1)^3 \\
&= \frac{s^2(s+1)^2 + 4(s+1)^3}{4} \\
&= \frac{(s+1)^2\left(s^2+4s+4\right)}{4} \\
&= \frac{(s+1)^2(s+2)^2}{4} \\
&= \frac{[(s+1)(s+2)]^2}{4} = \frac{[s'(s'+1)]^2}{4}
\end{aligned}$$

ce qui conclut la preuve. □

Si on compare les théorèmes 1.1 et 3.1, on peut être tenté de penser qu'ils ne sont que deux exemples d'un résultat plus général, fournissant la somme de toutes les premières $n+1$ puissances impaires. Cela nous amènerait à conjecturer que pour tout couple de nombres naturels $n$ et $m$ on ait

$$\sum_{i=0}^{n} i^{2m+1} = \frac{[n(n+1)]^{m+1}}{2^{m+1}}$$

Si ceci était effectivement le cas, on aurait un théorème bien plus puissant et général que les théorèmes 1.1 et 3.1, qui n'en seraient que des cas particuliers. Pourtant la faible induction simple basée sur les seuls cas $m=0$ et $m=1$ nous égare dans ce cas. Pour le voir, il suffit de poser par exemple $m=2$ et $n=3$. Si la conjecture précédente était correcte, on aurait

$$\sum_{i=0}^{3} i^5 = 0+1+32+243 = 276 = \frac{(3\cdot 4)^3}{2^3} = 6^3 = 216$$

ce qui n'est manifestement pas le cas.

Cela nous apprend que, si les mathématiciens proposent souvent des généralisations audacieuses, ils ne peuvent pas se limiter à faire confiance à ces généralisations et doivent toujours les accompagner, non seulement de quelques vérifications, mais aussi d'une preuve déductive.

Remarque 3.6. Il y a un autre enseignement plus particulier qui est contenu dans cet échec. On voit par là que la tâche de généraliser les théorèmes 1.1 et 3.1, en donnant une formule simple, exprimant la somme $\sum_{i=0}^{n} i^m$ pour tout $n$ et $m$ naturels, n'est pas si simple (on reviendra sur ce problème à la fin du paragraphe 4). C'est un exemple facile d'une circonstance que les mathématiciens connaissent fort bien : derrière la structure si simple et régulière de $\mathbb{N}$ se cachent des irrégularités qu'il est souvent difficile d'expliquer, ou, si on préfère le dire ainsi, des régularités si profondes qu'il est souvent fort difficile de les découvrir. La recherche de ces régularités profondes ou, si on veut, d'une explication des irrégularités apparentes, fait l'objet d'une des plus anciennes et fascinantes des théories mathématiques : la théorie dites « des nombres ». Les résultats surprenants et les problèmes encore ouverts dans cette théorie (c'est-à-dire les problèmes qu'on sait formuler, mais qu'on ne sait pas résoudre) ont passionné les mathématiciens de tous les temps et les passionnent encore. L'exemple peut-être le plus connu d'un problème ouvert (et très difficile, si difficile

qu'on peut penser qu'il restera ouvert encore très longtemps), qui avait déjà attiré l'attention d'Euclide, et pour lequel on attend donc une réponse depuis plus de deux mille ans, est celui de la distribution des nombres premiers (nombres naturels qui ne sont divisibles, dans $\mathbb{N}$, que par 1 et par eux-mêmes, c'est-à-dire qu'ils n'ont dans $\mathbb{N}$ aucun diviseur non banal) : comment peut-on calculer l'$n$-ième nombre premier lorsque la valeur de $n$ est fixée, quelle que soit cette valeur ? On ne le sait pas. Un exemple de problème en théorie des nombres qui a été finalement résolu, après une recherche longue de plus de quatre cents ans, est celui du grand théorème (comme on peut enfin l'appeler avec raison) de Fermat, que le mathématicien anglais Andrew Wiles a tout récemment prouvé : si $n$ est un nombre naturel plus grand que 2, alors il n'y a aucun triplet $< x, y, z >$ de nombres naturels différents de 0, tels que $x^n + y^n = z^n$ (ou, si l'on préfère, il n'y a aucun couple de nombres rationnels $\frac{p}{q}$ et $\frac{h}{k}$ différents de 0, tels que $\left(\frac{p}{q}\right)^n + \left(\frac{h}{k}\right)^n = 1$ ; car : si c'était le cas, on aurait aussi $\left(\frac{pk}{qk}\right)^n + \left(\frac{hq}{kq}\right)^n = 1$ et donc $(pk)^n + (hq)^n = (kq)^n$ et le triplet $< pk, hq, kq >$ contredirait le théorème ; et si, pour tout $\frac{p}{q}$, $\frac{h}{k}$ et $n$, $\left(\frac{p}{q}\right)^n + \left(\frac{h}{k}\right)^n \neq 1$, alors $\left(\frac{pk}{qk}\right)^n + \left(\frac{hq}{kq}\right)^n \neq 1$ et donc, pour tout $pk$, $hq$, $kq$, et $n$, $(pk)^n + (hq)^n \neq (kq)^n$). La difficulté de la preuve de Wiles et la complexité des différentes théories mathématiques qu'elle emploie est telle que le seul fait d'évoquer ses idées maîtresses demanderait qu'on rédige plusieurs traités de mathématiques fort sophistiqués.

NOTE HISTORIQUE 3.4. Déjà Euclide avait démontré (*Éléments*, livre IX, prop. 20) qu'il y a une infinité de nombres premiers, ou, pour s'exprimer comme lui, que « les nombres premiers sont plus nombreux que toute multitude de nombres premiers proposée », c'est-à-dire que pour tout ensemble fini de nombres premiers, il y a un nombre premier qu'il n'est pas compris en cet ensemble. La preuve d'Euclide est simple et élégante et mérite d'être exposée. Soit $\{p_0, p_1, \ldots p_n\}$ un ensemble fini quelconque de nombres premiers. Il est certainement possible de multiplier entre eux les éléments de cet ensemble. Soit $P$ le produit obtenu de cette manière. Comme chaque nombre premier est un nombre naturel, $P$ sera lui aussi un nombre naturel. Considérons alors l'autre nombre naturel $P+1$. Si $P+1$ était à son tour premier, alors il serait certain qu'il y ait un nombre premier qui n'est pas compris en $\{p_0, p_1, \ldots, p_n\}$, car $P+1$ est certainement plus grand que le plus grand des nombres compris en cet ensemble. Si $P+1$ n'était pas premier à son tour, alors il serait divisible par un nombre premier, disons $p$. Si l'ensemble $\{p_0, p_1, \ldots, p_n\}$ comprenait tous les nombres premiers, alors $p$ devrait être un des ses éléments et il serait donc un facteur de $P$. Donc $p$ devrait diviser en même temps $P$ et $P+1$, et il devrait donc diviser aussi la différence $P-(P-1) = 1$. Mais aucun nombre premier ne peut diviser 1. Donc, si $P+1$ n'était pas premier, $p$ ne serait pas compris en $\{p_0, p_1, \ldots, p_n\}$, et il y aurait donc, à nouveau, un nombre premier qui n'est pas compris dans cet ensemble. Donc, que $P+1$ soit premier ou qu'il ne soit pas premier, il y a un nombre premier qui n'est pas compris dans l'ensemble $\{p_0, p_1, \ldots, p_n\}$. Qu'on observe que si l'on suppose, comme l'on a l'habitude de le faire, que cet ensemble comprenne la totalité des nombres premiers plus petits au égaux à $p_n$ (ou à n'importe quel autre de ses éléments), de là il s'ensuit immédiatement qu'il y a un nombre premier plus grand que $p_n$.

Après Euclide, de nombreux mathématiciens ont donné des preuves différentes de ce théorème. Le but de ces preuves n'était pas de corriger ou perfectionner la preuve précédente dont la correction et l'élégance sont indiscutables. Le but essentiel de ces nouvelles démonstrations était plutôt de montrer des connexions entre le théorème

d'Euclide et d'autres résultats mathématiques, aptes à suggérer une manière pour déterminer la fonction $\pi(i)$ de $\mathbb{N}$ sur $\mathbb{N}$, associant à chaque nombre naturel $i$ l'$i$-ième nombre premier. L'intérêt de la détermination de cette fonction ne réside pas, à son tour, dans le fait que la connaissance de cette fonction permettrait de calculer autant de nombres premiers qu'on veuille (aujourd'hui le nombre de nombres premiers connus est assez remarquable, le plus grand parmi ceux-ci étant égal à $2^{20\,996\,011} - 1$ et comporte, en numérotation décimale, 6 320 430 chiffres). Ce qui fait l'intérêt de la fonction $\pi(i)$ est le fait que si elle était connue, elle exprimerait la distribution des nombres premiers sur l'ensemble des nombres naturels.

Parmi les différentes démonstrations du théorème d'Euclide affirmant l'existence d'une infinité de nombres premiers, une place particulière est occupée par celle donnée par Euler en 1737. Il n'est pas possible ici, en ne se fondant que sur les notions mathématiques introduites ci-dessous, de donner une idée ne fût-ce que très vague de la preuve d'Euler. On dira seulement qu'elle fait intervenir une série à partir de laquelle Euler définit une fonction sur l'ensemble des nombres réels (cf. le chapitre 6), qui deviendra ensuite célèbre sous le nom de « fonction zêta ». Un siècle plus tard, Bernhard Riemann eut l'idée d'étendre cette fonction au corps des nombres complexes (pour la notion de corps, cf. le chapitre 5 ; pour éclairer la notion de nombre complexe, le lecteur devra en revanche s'adresser à d'autres textes moins élémentaires) en montrant que la détermination de certaines des valeurs qui annulent cette fonction ainsi étendue (les zéros non banals de la fonction zêta de Riemann) fournirait une connaissance de la distribution des nombres premiers sur l'ensemble des nombres naturels.

Bien qu'on dispose aujourd'hui d'approximations apparemment assez précises de la fonction $\pi(i)$, et que l'on connaisse plusieurs de ses propriétés, la détermination de cette fonction est un but qu'on n'a pas encore atteint. Les recherches les plus prometteuses dans cette direction se réclament de l'étude de la fonction zêta de Riemann. Pour essayer de résoudre un problème qui apparemment ne relève que des nombres naturels, les mathématiciens contemporains mobilisent ainsi des notions relevant de théories, telles que l'analyse complexe, apparemment très éloignées de la simplicité originaire de la notion de nombre naturel. C'est un exemple des relations très profondes qui lient les différents domaines des mathématiques modernes,

**Lectures possibles** : P. Ribenboim, *Nombres premiers : mystères et records*, PUF, Paris, 1994.

* * *

Né à Breselenz en Allemagne en 1826, deuxième fils d'un pasteur de l'église protestante, et mort à Selasca en Italie, en 1866, Bernhard Riemann fut sans doute un des mathématiciens les plus novateurs de tous les temps. Non seulement ses travaux et ses idées ouvrirent des horizons nouveaux dans plusieurs domaines des recherches mathématiques ; ils montrèrent surtout que des théories, jusqu'alors considérées comme distinctes, pouvaient collaborer à la détermination de notions nouvelles définissant de nouvelles directions dans l'évolution des mathématiques. Encore maintenant les idées de Riemann sont des sources d'inspiration fondamentales pour les recherches de plusieurs mathématiciens. Bien que dans sa courte vie, il travaillât sur un nombre très grand de problèmes mathématiques et physico-mathématiques, son nom est particulièrement lié à la théorie de l'intégration, au développement de l'analyse complexe

et à la naissance de la géométrie moderne, en particulier à l'élaboration d'une conception nouvelle de l'espace.

**Lectures possibles** : D. Laugwitz, *Bernhard Riemann,* 1826-1866 *: Wendenpunkte in der Auffassung des Mathematik*, Birkhaüser, Basel, Boston, Berlin, 1996.

* * *

L'histoire du grand théorème de Fermat commence au troisième siècle de notre ère quand Diophante — le mathématicien alexandrin auteur des *Arithmétiques*, le traité qui constitue le point culminant de l'arithmétique grecque et marque l'origine de l'algèbre et de la théorie des équations (encore aujourd'hui on appelle « diophantiennes » les équations à coefficients entiers, dont on cherche les solutions entières) — posa, justement dans les *Arithmétiques*, le problème consistant à diviser un carré en deux autres carrés. Déjà les pytaghoriciens connaissaient certains nombres entiers positifs carrés qui résultent de la somme des deux autres nombres positifs carrés, par exemple 25, le carré de 5, qui résulte de la somme de 16 et 9, respectivement les carrés de 4 et de 3. Diophante cherchait une méthode pour trouver, s'ils existent, les deux nombres dont la somme des carrés est égale au carré d'un nombre donné. Si on invertit le problème, il n'est pas difficile d'en trouver une solution, car, quels que soient les nombres naturels distincts $p$ et $q$, différents de zéro, le produit $2pq$, la différence $p^2 - q^2$ et la somme $p^2 + q^2$ sont tous des nombres naturels différents de zéro, et, comme

$$\begin{aligned}(p^2 - q^2)^2 &= p^4 - 2p^2q^2 + q^4\\ (p^2 + q^2)^2 &= p^4 + 2p^2q^2 + q^4\end{aligned}$$

il suffit de poser

$$x = 2pq\ ; \qquad y = (p^2 - q^2)\ ; \qquad z = (p^2 + q^2)$$

pour avoir

$$x^2 + y^2 = z^2$$

Fermat lut le traité de Diophante, quatorze cents ans plus tard. Parvenu au point où Diophante pose ce problème, il ecrivit en latin, en marge de sa copie du texte, la note suivante : « Décomposer un cube en deux autres cubes, une quatrième puissance, et généralement une puissance quelconque en deux puissances de même nom, au dessus de la seconde puissance, est une chose impossible et j'en ai assurément trouvé l'admirable démonstration. La marge trop exiguë ne la contiendrait pas ».

Depuis que cette remarque de Fermat a été rendue publique, le rêve de tout historien des mathématiques a été de retrouver une note de Fermat donnant sa démonstration présumée. Personne n'a pourtant rien trouvé de plus, parmi les papiers de Fermat, qu'une preuve, en vérité assez simple, dérivant de la solution qu'on vient de donner du problème original de Diophante, de l'affirmation de Fermat pour $n = 4$. En 1753, Euler démontra cette affirmation pour $n = 3$ et en 1847 Kummer la prouva, à condition que l'exposant $n$ appartienne à une large classe de nombres premiers.

Les recherches des mathématiciens ont en outre mis en lumière un fait qui semble rendre hautement improbable l'hypothèse que Fermat possédât effectivement une preuve correcte de son affirmation. En effet, les procédures algébriques dont se servait Fermat sont toutes applicables, non seulement aux nombres naturels, mais aussi à d'autres structures distinctes de $\mathbb{N}$, bien que construites à partir de $\mathbb{N}$ ; et il n'est pas difficile de construire des structures de cette sorte, dans lesquelles l'affirmation de

Fermat admet des contre-exemples. De là, il s'ensuit qu'aucune preuve élémentaire n'est possible pour cette affirmation.

Le rêve des historiens ayant été brisé, il en restait un autre, qui a été pendant longtemps le rêve de tout mathématicien : trouver une preuve correcte de l'affirmation de Fermat. Les recherches dans cette direction ont été innombrables et il n'est pas possible ici d'en donner un aperçu. On se limitera à conclure l'histoire en répétant que ce rêve a été finalement réalisé en 1994 par Andrew Wiles.

**Lectures possibles** : Yves Hellegouarch, *Invitation aux mathématiques de Fermat-Wiles*, Masson, Paris, 1997 ; S. Singh, *Le dernier théorème de Fermat*, J.-C. Lattès, s.l., 1998 ; W. et F. Ellison, « Théorie des nombres », J. Dieudonné, d., *Abrégé d'histoire des mathématiques,* 1700-1900, nouv. éd., Hermann, Paris, 1986, pp. 151-236.

* * *

Né à Beaumont de Lomagne en 1601 et mort à Castres en 1665, Pierre de Fermat passa la grande majorité de sa vie à Toulouse, où il fut parlementaire et homme de loi. Les mathématiques ne furent pour lui qu'un loisir qui pourtant l'accompagna tout au cours de sa vie. Bien qu'aucun de ses écrits ne fît destiné à la publication, il acquit une importante réputation parmi les mathématiciens de son époque, grâce à une assez large correspondance. Ses lettres et ses papiers furent publiés pour la première fois après sa mort, en 1679, et sont aujourd'hui disponibles grâce aux quatre volumes des *Œuvres de Fermat* (éd. par C. Henry et P. Tannery). Ses recherches en géométrie visèrent en particulier les problèmes de la recherche des tangentes et du calcul des aires : sa méthode pour la détermination des *maximus* et des *minimus* d'une courbe constitua l'une des acquisitions fondamentales qui amenèrent à l'invention du calcul différentiel et fut l'une des sources d'inspiration fondamentales de Newton. Au contraire, ses idées et conjectures en théorie des nombres restèrent pratiquement inconnues ou sans aucune influence jusqu'au XVIII$^{\text{ème}}$ siècle. Euler fut le premier à se rendre compte de l'intérêt des suggestions de Fermat dans ce domaine.

**Lectures possibles** : M. Mahoney, *The Mathematical Career of Pierre de Fermat,* 1601-1665, 2$^{\text{nd}}$ ed., Princeton Univ. Press, Princeton, 1994.

### 4. Le développement binomial pour un exposant naturel quelconque

Les précédentes preuves par récurrence sont toutes assez simples. On ne doit pas pour autant croire qu'il est toujours facile de démontrer un théorème par récurrence. Quand on conduit une telle preuve, on doit surtout prendre garde au fait que la démonstration de l'implication qui va de $n = s$ à $n = s'$ soit valide pour toute valeur de $s$ plus grande ou égale à la valeur choisie comme base de l'induction.

REMARQUE 3.7. Un exemple amusant d'un argument récursif erroné parce que cette clause essentielle n'est pas observée est le suivant.

On veut démontrer que si dans une assemblée il y a au moins une femme, alors tous les membres de l'assemblée sont des femmes. On procède par induction complète sur le nombre $n$ des membres de l'assemblée. Si on pose $n = 1$, la conjecture est banalement vérifiée, car si l'assemblée n'est composée que par un membre et qu'il y a parmi ses membres au moins une femme, alors le seul membre de l'assemblée est une femme, et donc tous les membres de l'assemblée sont des femmes. Imaginons maintenant que la conjecture soit vérifiée pour $n = s$, c'est-à-dire que si dans toute assemblée de $s$ membres il y a au moins une femme,

alors tous les membres d'une telle assemblée sont des femmes. Ce qu'on doit alors prouver est que si ceci est le cas, alors c'est aussi le cas que si dans une assemblée de $s' = s + 1$ membres il y a une femme, alors tous les membres de cette assemblée sont des femmes. Prenons une assemblée, disons $\mathfrak{A}$, de $s + 1$ membres, parmi lesquels il y a au moins une femme, disons Elisabeth. Choisissons un membre de cette assemblée autre que Elisabeth, disons $\mathfrak{a}$, et éliminons-le. On retourne ainsi à une assemblée à $s$ membres où il y a au moins une femme, justement Elisabeth. L'hypothèse qu'on a posée nous assure ainsi que tous les membres de cette assemblée sont des femmes. Si on replace dans cette assemblée le membre $\mathfrak{a}$ de $\mathfrak{A}$ qu'on avait d'abord éliminé, on obtient à nouveau l'assemblée $\mathfrak{A}$ de départ. Parmi ses $s + 1$ membres il y en aura donc $s$ qui sont sans doute des femmes et un, $\mathfrak{a}$, dont on ne sait pas encore s'il est une femme ou non. Il s'agit justement de montrer que c'est, lui aussi, une femme. Pour faire ceci, prenons à nouveau un membre de $\mathfrak{A}$, cette fois différent de $\mathfrak{a}$, et éliminons-le. On retrouvera une assemblée de $s$ membres, où il y a au moins une femme. De l'hypothèse qu'on a posée il suit que cette assemblée ne contient que des femmes. Comme $\mathfrak{a}$ est bien un membre de cette assemblée, il est aussi une femme, donc tous les éléments de $\mathfrak{A}$ sont des femmes, ce qu'il s'agissait de démontrer.

Le lecteur est invité à trouver par lui-même l'erreur de ce raisonnement, ou, à défaut, à se rallier à l'idée que la présence au monde de la reine d'Angleterre confère à tous les humains la condition de femme.

On va considérer ici l'exemple d'un théorème démontrable par récurrence, dont la preuve est un peu plus difficile que celles données ci-dessus. Bien que sa preuve soit encore fort accessible à des non mathématiciens, ce théorème appartient à des mathématiques un peu moins élémentaires que celles considérées jusqu'à présent.

Soient $a$ et $b$ deux quantités quelconques, c'est-à-dire deux éléments d'un ensemble $E$ qui respecte les conditions qu'on a indiquées ci-dessus relativement à l'addition et à la multiplication. On pourra alors les additionner. Leur somme étant une nouvelle quantité de la même sorte, disons $c$, il sera possible de multiplier $c$ avec elle-même autant de fois qu'on le voudra, disons $n$ fois ($n$ étant un nombre naturel quelconque). Le résultat d'une telle opération sera dit, comme tout à l'heure, « puissance $n$ -ième » de $c$, ou, plus généralement, « puissance $n$-ième du binôme $a + b$ », le nombre $n$ étant dit « exposant » de la puissance en question. Comme $a$ et $b$ sont deux quantités quelconques, ce binôme sera aussi quelconque. Si on sait écrire la puissance $n$ -ième du binôme $a + b$ sous la forme d'une somme de produits où n'interviennent que les quantités $a$ et $b$, accompagnées éventuellement d'un nombre naturel, on dira qu'on sait *développer* une telle puissance, c'est-à-dire une puissance quelconque à exposant naturel d'un binôme quelconque. Cette somme sera appelée « développement binomial pour un exposant naturel quelconque ». Le nouveau problème qu'on se pose est justement de déterminer un tel développement, les quantités $a$ et $b$ et le nombre naturel $n$ étant donnés.

Remarque 3.8. Lorsqu'on travaille sur des éléments indéterminés d'un ensemble $E$ sur lequel sont définies une addition et une multiplication, on appelle généralement « monôme » un produit de plusieurs éléments de $E$, dénotés chacun par un symbole élémentaire. Dans l'écriture dénotant un monôme ne comparaîtront donc pas de signes d'addition. Quant au signe « $\cdot$ », indiquant une multiplication, il est généralement omis, car on suppose que deux symboles indiquant des éléments de $E$, posés l'un à côté de l'autre, sans aucun symbole intercalé, dénotent le produit de ces termes. Si $x$ et $y$ appartiennent à $E$, et $n$ et $m$ sont des nombres naturels, les écritures « $xy$ », « $x^n y$ », « $x^n y^m$ » indiquent ainsi (ou, si on préfère, sont) des monômes. On appelle « binôme » l'addition de deux monômes et « polynôme » l'addition de plusieurs monômes. Comme « plusieurs » peut aussi signifier « deux » ou même « un », à la rigueur tout monôme et tout binôme sont des polynômes. On peut supposer

que $\mathbb{N}$ soit un sous-ensemble de $E$, ou qu'on ait défini une multiplication entre les éléments de $E$ et les nombres naturels. Si $n$ est un nombre naturel et $\mathfrak{m}$ un monôme en $E$, alors $n\mathfrak{m}$ est aussi un monôme en $E$. En particulier, si $a, b \in E$, les produits $1a = a$ et $1b = b$ seront des monômes et la somme $a+b$ un binôme. En général, on réserve par contre le terme « polynôme » pour indiquer une somme de monômes dans chacun desquels interviennent des puissances à exposant naturel, d'un ou plusieurs éléments de $E$. Ainsi si $x$, $y$, $a_i$, $a_{i-j,j}$ sont des éléments de $E$ et $p$ un nombre naturel,

$$\sum_{i=0}^{p} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_p x^p$$

$$\sum_{i=0}^{p} \left( \sum_{j=0}^{i} a_{i-j,j} x^{i-j} y^j \right) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + \ldots + a_{0,p}x^p$$

sont des polynômes. Le premier est généralement dit « polynôme en $x$ de degré $p$ » (car $p$ est l'exposant le plus grand parmi les exposants des puissances de $x$ intervenant dans ce polynôme) le deuxième « polynôme en $x$ et $y$ de degré $p$ » (car $p$ est la somme la plus grande parmi les sommes des exposants des puissances de $x$ et $y$ intervenant dans ce polynôme).

Revenons à notre problème. On note d'abord que, quel que soit $c$, si $p$ et $q$ sont deux nombres naturels plus grands que 1, on aura :

$$\begin{aligned} c^p \cdot c^q &= (\underbrace{c \cdot c \cdot \ldots \cdot c}_{p \text{ fois}}) \cdot (\underbrace{c \cdot c \cdot \ldots \cdot c}_{q \text{ fois}}) \\ &= \underbrace{c \cdot c \cdot \ldots \cdot c}_{p+q \text{ fois}} = c^{p+q} \end{aligned}$$

Ainsi, puisque pour tout nombre naturel $n$, $n = n + 0$, si on veut que la règle précédente vaille pour tout couple de nombres naturels $p$ et $q$, on devra poser :

$$c^0 = 1 \qquad \text{et} \qquad c^1 = c$$

ce qui donnera exactement

$$c^n = c^{n+0} = c^n \cdot c^0 \qquad \text{et} \qquad c^{n+1} = c^n \cdot c^1$$

Grâce à la distributivité de la multiplication sur l'addition, on aura alors la table récursive suivante :

| | | |
|---|---|---|
| $(a+b)^0 =$ | ..... | $1$ |
| $(a+b)^1 =$ | $(a+b)^{1+0} = (a+b) \cdot 1 =$ ..... | $a+b$ |
| $(a+b)^2 =$ | $(a+b)^{1+1} = (a+b) \cdot (a+b) =$ ..... | $(a+b)a + (a+b)b$ |
| $(a+b)^3 =$ | $(a+b)^{2+1} = (a+b)^2 \cdot (a+b) =$ ..... | $(a+b)^2 a + (a+b)^2 b$ |
| ... | ... | ... |
| $(a+b)^n =$ | $(a+b)^{(n-1)+1} = (a+b)^{n-1} \cdot (a+b) =$ | $(a+b)^{n-1}a + (a+b)^{n-1}b$ |

Quel que soit $n$, il est donc possible, en $n+1$ étapes, de calculer le développement de la puissance $n$-ième d'un binôme quelconque $a+b$. Pour cela, il faudra calculer, l'un après l'autre, tous les développements des puissances $j$-ièmes de ce même binôme pour $j = 0, 1, 2, ..., n-1$. Imaginons par exemple qu'on veuille calculer le développement de la puissance 4-ième d'un tel binôme.

On aura, comme ci-dessus :

$$\begin{array}{lll}(a+b)^0 = & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & 1\\ (a+b)^1 = & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & a+b\\ (a+b)^2 = & (a+b)a+(a+b)b = \ldots & a^2+2ab+b^2\\ (a+b)^3 = & (a+b)^2a+(a+b)^2b = & a^3+3a^2b+3ab^2+b^3\\ (a+b)^4 = & (a+b)^3a+(a+b)^3b = & a^4+4a^3b+6a^2b^2+4ab^3+b^4\end{array}$$

Bien que ce procédé par récurrence résolve en principe le problème pour tout nombre naturel $n$, il demande des calculs de plus en plus longs, à mesure que la valeur de $n$ croît. Ce n'est pourtant pas le défaut majeur de cette solution ; plus important encore est le fait qu'en suivant cette méthode, on ne parvient pas à déterminer la forme commune à tous les développements de n'importe quelle puissance naturelle d'un binôme quelconque ; autrement dit, on ne trouve pas la formule qui exprime d'emblée et en toute généralité le développement de $(a+b)^n$ quel que soit le nombre naturel $n$. La recherche de cette formule est le but de l'argument qui occupe le présent paragraphe.

REMARQUE 3.9. Il ne faut pas confondre une preuve par récurrence avec une méthode par récurrence conduisant à la détermination, quel que soit le nombre naturel $i$, de l'$i$-ème terme d'une certaine suite de termes. Dans le premier cas, il s'agit d'un argument démonstratif fondé sur le cinquième axiome de Peano, fournissant la preuve d'un théorème portant sur tous les éléments d'une progression. Dans le deuxième cas il s'agit d'une procédure qui permet de déterminer (ou calculer) le terme cherché à partir de la détermination d'un ou plusieurs termes de rang inférieur. Comme, quel que soit $i$, il faut, pour déterminer de cette manière $(i-1)$-ème terme de notre suite, avoir déjà déterminé au moins son $(i-1)$-ième terme, il est clair que, à la différence d'une preuve par récurrence, une méthode par récurrence ne conduit pas en général (ou du moins ne conduit pas directement) à la détermination d'une formule valable pour tout élément d'une progression.

Considérons d'abord le développement de $(a+b)^4$. Il est facile de voir que tous les termes qui entrent dans la somme exprimant ce développement sont des monômes de la forme « $\nu a^p b^q$ », où $\nu$, $p$ et $q$ sont des nombres naturels et $p+q=4$. Il est facile de voir que cela vaut également pour les puissances moindres que la quatrième, la somme des nombres $p$ et $q$ (dite « ordre du terme $\nu a^p b^q$ » ) étant à chaque fois égale à l'exposant de la puissance considérée. Il est facile de démontrer par récurrence que cela doit être aussi le cas pour le développement d'une puissance quelconque du binôme $a+b$. En fait, c'est le cas du développement de $(a+b)^0$, car $(a+b)^0 = 1 = 1a^0b^0$, et $0+0=0$, et il est facile de voir que si c'est le cas du développement de $(a+b)^s$, $s$ étant un nombre naturel quelconque, alors c'est aussi le cas du développement de $(a+b)^{s'} = (a+b)^{s+1} = [(a+b)^s a] + [(a+b)^s b]$, car en multipliant le développement de $(a+b)^s$ d'abord par $a$ et ensuite par $b$, on ne fait qu'augmenter l'ordre de tout terme de 1. Le résultat de cette double multiplication sera alors une somme, où n'interviennent que des termes de la forme $\nu a^p b^q$, avec $p+q = s+1 = s'$. Parmi ces termes, certains seront similaires entre eux, c'est-à-dire qu'ils ne différeront, éventuellement, que pour la valeur du nombre naturel $\nu$, qui est dit « coefficient » du terme en question. Ces termes pourront alors être additionnés, leur somme étant naturellement un nouveau terme de la forme $\nu a^p b^q$, avec $p+q = s+1 = s'$.

Ce n'est pas tout. Il est aussi facile de voir que, abstraction faite du nombre naturel $\nu$, les termes qui composent le développement de $(a+b)^4$ sont tous ceux qu'on peut construire en choisissant les nombres naturels $p$ et $q$ de manière à ce que leur somme soit égale à 4. Ces

termes sont en fait donnés par tous les couples ordonnés

$$\begin{aligned} p &= 4 \qquad q = 0 \\ p &= 3 \qquad q = 1 \\ p &= 2 \qquad q = 2 \\ p &= 1 \qquad q = 3 \\ p &= 0 \qquad q = 4 \end{aligned}$$

Il est également facile de vérifier que cela est vrai également pour le développement de toutes les puissances qui précèdent la quatrième et, en général, pour le développement de tout binôme $(a+b)^n$ : les monômes qui interviennent dans ce développement sont tous les termes de la forme « $\nu a^p b^q$ » qu'on peut construire en choisissant les nombres naturels $p$ et $q$ de sorte que $p+q=n$, $\nu$ étant un coefficient quelconque. Il est facile de le prouver, en utilisant un argument récursif similaire au précédent. En fait, les couples ordonnés des nombres naturels $p$ et $q$ dont la somme est égale à $s$ sont

$$\begin{aligned} &p = s && q = 0 \\ &p = s-1 && q = 1 \\ &p = s-2 && q = 2 \\ &... && ... \\ &p = 1 && q = s-1 \\ &p = 0 && q = s \end{aligned}$$

et les multiplications successives par $a$ et par $b$, en augmentant de 1 respectivement les valeurs de $p$ et de $q$, donnent les couples

$$\begin{aligned} &p = s+1 && q = 0 \\ &p = s && q = 1 \\ &p = s-1 && q = 2 \\ &... && ... \\ &p = 1 && q = s \\ &p = 0 && q = s+1 \end{aligned}$$

qui sont justement tous les couples de nombres naturels dont la somme est égale à $s' = s+1$.

On a ainsi démontré que, pour tout nombre naturel $n$ et tout couple de quantités $a$ et $b$, on a :

$$(a+b)^n = \sum_{i=0}^{n} \nu_i a^{n-i} b^i \tag{17}$$

où les $\nu_i$ $(i = 0, 1, ..., n)$ sont des nombres naturels qu'il s'agit maintenant de déterminer. La difficulté de la preuve de notre théorème consiste justement en la détermination de ces nombres.

Commençons en fixant une notation convenable. En suivant la convention habituelle, on notera par « $\binom{n}{i}$ » le coefficient $\nu_i$ intervenant dans le terme $\nu_i a^{n-i} b^i$ du développement de $(a+b)^n$. La (17) s'écrira alors sous la forme :

$$\begin{aligned} (a+b)^n &= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots \\ &\qquad \dots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n \end{aligned}$$

Il sera ensuite facile de vérifier que, quel que soit $s$ (pourvu qu'il soit différent de zéro), chacun des coefficients $\binom{s+1}{1}$, $\binom{s+1}{2}$,..., $\binom{s+1}{s}$ intervenant dans le développement de $(a+b)^{s+1}$ résulte de l'addition de deux coefficients intervenant dans le développement de $(a+b)^s$. En effet, comme

$$(a+b)^{s+1} = (a+b)^s(a+b) = a(a+b)^s + b(a+b)^s$$

on aura

$$\begin{aligned}(a+b)^{s+1} &= a\sum_{i=0}^{s}\binom{s}{i}a^{s-i}b^i + b\sum_{i=0}^{s}\binom{s}{i}a^{s-i}b^i \\ &= \sum_{i=0}^{s}\binom{s}{i}a^{s-i+1}b^i + \sum_{i=0}^{s}\binom{s}{i}a^{s-i}b^{i+1}\end{aligned}$$

Mais si $t$ est un nombre naturel quelconque plus grand que 0 et plus petit que $s$, alors :

$$\begin{aligned}\sum_{i=0}^{s}\binom{s}{i}a^{s-i+1}b^i &= \binom{s}{0}a^{s+1} + \binom{s}{1}a^s b + \ldots + \\ &\quad + \binom{s}{t}a^{s-t+1}b^t + \binom{s}{t+1}a^{s-t}b^{t+1} + \ldots + \\ &\quad + \binom{s}{s-1}a^2 b^{s-1} + \binom{s}{s}ab^s\end{aligned}$$

et

$$\begin{aligned}\sum_{i=0}^{s}\binom{s}{i}a^{s-i}b^{i+1} &= \binom{s}{0}a^s b + \binom{s}{1}a^{s-1}b^2 + \ldots + \\ &\quad + \binom{s}{t-1}a^{s-t+1}b^t + \binom{s}{t}a^{s-t}b^{t+1} + \ldots + \\ &\quad + \binom{s}{s-1}ab^s + \binom{s}{s}b^{s+1}\end{aligned}$$

et donc :

$$\begin{aligned}(a+b)^{s+1} &= \binom{s}{0}a^{s+1} + \left[\binom{s}{1} + \binom{s}{0}\right]a^s b + \ldots + \\ &\quad + \left[\binom{s}{t} + \binom{s}{t-1}\right]a^{s-t+1}b^t + \left[\binom{s}{t+1} + \binom{s}{t}\right]a^{s-t}b^{t+1} + \ldots \\ &\quad \ldots + \left[\binom{s}{s} + \binom{s}{s-1}\right]ab^s + \binom{s}{s}b^{s+1}\end{aligned}$$

Or, selon la convention précédente, on aura aussi

$$\begin{aligned}(a+b)^{s+1} &= \sum_{i=0}^{s+1}\binom{s+1}{i}a^{s-i+1}b^i \\ &= \binom{s+1}{0}a^{s+1} + \binom{s+1}{1}a^s b + \ldots + \\ &\quad + \binom{s+1}{t}a^{s-t+1}b^t + \binom{s+1}{t+1}a^{s-t}b^{t+1} + \ldots + \\ &\quad + \binom{s+1}{s}ab^s + \binom{s+1}{s+1}b^{s+1}\end{aligned}$$

et il sera donc facile de tirer, par comparaison, les égalités suivantes :

$$\begin{aligned}
\binom{s+1}{0} &= \binom{s}{0} \\
\binom{s+1}{1} &= \binom{s}{1} + \binom{s}{0} \\
&\cdots \\
\binom{s+1}{t} &= \binom{s}{t} + \binom{s}{t-1} \\
\binom{s+1}{t+1} &= \binom{s}{t+1} + \binom{s}{t} \\
&\cdots \\
\binom{s+1}{s} &= \binom{s}{s} + \binom{s}{s-1} \\
\binom{s+1}{s+1} &= \binom{s}{s}
\end{aligned}$$

D'ici, comme $s$ et $t$ sont quelconques, on passe sans difficulté aux égalités générales :

$$\begin{aligned}
&\binom{s+1}{0} = \binom{s}{0} = ... = \binom{1}{0} = \binom{0}{0} = 1 \\
&... \\
&\binom{s+1}{i} = \binom{s}{i} + \binom{s}{i-1} \\
&... \\
&\binom{s+1}{s+1} = \binom{s}{s} = ... = \binom{1}{1} = \binom{0}{0} = 1
\end{aligned}$$

où $s$ et $t$ sont des nombres naturels quelconques, et $1 \leq i \leq s$. Les nombres naturels intervenant en tant que coefficients numériques dans les développements successifs des puissances $j = 0, 1, 2, ...$ pourront alors être rangés dans la table suivante, dite « triangle de Pascal (ou de Tartaglia) », dans laquelle chaque entrée des lignes suivant la première est la somme des deux entrées de la ligne précédente, celle qui est positionnée au-dessus d'elle et celle qui est immédiatement à gauche de cette dernière :

| | $\binom{n}{0}$ | $\binom{n}{1}$ | $\binom{n}{2}$ | $\binom{n}{3}$ | $\binom{n}{4}$ | $\binom{n}{5}$ | $\binom{n}{6}$ | ... | ... |
|---|---|---|---|---|---|---|---|---|---|
| $(a+b)^0$ : | 1 | 0 | 0 | 0 | 0 | 0 | 0 | ... | $\rightarrow n = 0$ |
| $(a+b)^1$ : | 1 | 1 | 0 | 0 | 0 | 0 | 0 | ... | $\rightarrow n = 1$ |
| $(a+b)^2$ : | 1 | 2 | 1 | 0 | 0 | 0 | 0 | ... | $\rightarrow n = 2$ |
| $(a+b)^3$ : | 1 | 3 | 3 | 1 | 0 | 0 | 0 | ... | $\rightarrow n = 3$ |
| $(a+b)^4$ : | 1 | 4 | 6 | 4 | 1 | 0 | 0 | ... | $\rightarrow n = 4$ |
| $(a+b)^5$ : | 1 | 5 | 10 | 10 | 5 | 1 | 0 | ... | $\rightarrow n = 5$ |
| $(a+b)^6$ : | 1 | 6 | 15 | 20 | 15 | 6 | 1 | ... | $\rightarrow n = 6$ |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Le théorème suivant a été alors démontré :

THÉORÈME 4.1. *Si $n$ est un nombre naturel quelconque et $a$ et $b$ deux quantités quelconques, alors*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

*où les facteurs* $\binom{n}{i}$ *(*$i = 0, 1, ...$*) sont des nombres naturels (dits « coefficients binomiaux » ), respectant les conditions suivantes :*

**(*i*):** $\binom{n}{n} = \binom{n}{0} = 1$

**(*ii*):** *si* $i > n$, *alors* $\binom{n}{i} = 0$

**(*iiii*):** *si* $1 \leq i \leq n$, *alors* $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$

NOTE HISTORIQUE 3.5. L'argument qui nous a porté au théorème précédent ne dépend d'aucune manière de la nature des quantités $a$ et $b$ ; en particulier rien n'empêche que ces quantités soient considérées, au cours de ce raisonnement, comme des nombres entiers positifs. Le lecteur ne sera donc pas surpris d'apprendre que cet argument était déjà connu, pour l'essentiel, par les mathématiciens arabes auxquels on doit d'avoir poursuivi les recherches arithmétiques d'Euclide, d'Archimède et, surtout, de Diophante. Il semble en particulier que déjà Al-Khwārizmī, qui vécut a Baghdad au IX$^{\text{ème}}$ siècle (du nom duquel vient le terme « algorithme » ), possèdât une règle permettant le calcul (évidemment par reccurence) d'une puissance entière positive quelconque d'un binôme. Un énoncé explicite de cette règle (pour $n < 13$) se trouve d'ailleurs dans le *Recueil de mathématiques à l'aide du tableau et de la poussière* de Al-Tūsī, datant de 1265, où on trouve aussi un tableau qui ressemble au triangle de Pascal.

Un tableau analogue apparaît dans l'*Arithmética integra* de Stifel en 1544. Quelques années plus tard, c'est Niccolò Tartaglia (né à Brescia en 1499 ou 1500, et mort à Venise en 1557) qui, dans le chapitre XX du II$^{\text{ème}}$ livre de la *Seconda parte del general trattato di numeri et mesure*, publié en 1556, donne le triangle de Pascal dans sa forme actuelle. Tartaglia n'indique pourtant que la possibilité d'employer ce tableau numérique pour extraire des racines des nombres entiers et positifs. C'est en revanche Pascal qui fit de ce tableau une étude approfondie, en lui consacrant son *Traité du triangle arithmétique*, un ouvrage composite, d'abord écrit en latin, puis rémanié et partiellement traduit en français, imprimé en 1654, mais distribué au public après la mort de son auteur, en 1665. Après avoir énoncé différentes propriétés de son triangle et l'avoir employé pour classifier les nombres entiers positifs en différents « ordres » (selon la ligne du triangle dans laquelle ils se trouvent), Pascal indique de possibles applications de ceci à la combinatoire, à la probabilité et au calcul des puissances d'un binôme.

**Lectures possible** : B : Pascal, *Traité du triangle arithmétique et traités connexes*, B. Pascal, *Œuvres Complètes*, texte établi, présenté et annoté par J. Mesnard, Desclée de Bouwer, s.l., 1964-1992 (trois volumes en quatre tomes), vol. I, t. 2, pp. 1166-1332 ; A. W. F. Edwards, *Pascal's Arithmetical Triangle*, Charles Griffin & Co., London et Oxford Univ. Press, New York, 1987.

Il est alors clair que, quel que soit $n$, il suffira de consulter le triangle de Pascal pour connaître tous les coefficients numériques du développement de $(a + b)^n$. Ceci n'est pourtant pas encore le résultat cherché, car si on procède de cette manière, la détermination des coefficients du développement de $(a + b)^n$ dépend de la détermination préalable des coefficients du développement de $(a+b)^{n-1}$ ; la détermination des coefficients du développement de $(a+b)^{n-1}$ dépende de la détermination préalable des coefficients du développement de $(a + b)^{n-2}$ ; et ainsi de suite. On ne pourra donc pas écrire directement, quel que soit $n$, le développement de $(a + b)^n$. Dit autrement : il reste à chercher à exprimer les coefficients binomiaux de manière non récursive, c'est-à-dire à trouver une formule qui exprime chaque coefficient $\binom{n}{i}$ en termes

de nombres naturels $n$ et $i$ et de manière indépendante de tout autre coefficient binomial. Le théorème 4.1 nous permet de poser, quel que soit le nombre naturel $n$,

$$\binom{n}{0} = 1$$

tandis que la considération des cas donnés par les plus petites valeurs de $n$ permet d'avancer la conjecture suivante :

$$\text{si } 1 \leq i \leq n \text{ alors } \binom{n}{i} = \frac{n(n-1)(n-2)...[n-(i-1)]}{1 \cdot 2 \cdot ... \cdot i}$$

Pour démontrer que c'est bien le cas, on peut procéder de deux manières. On peut s'appuyer sur les conditions (*i*)-(*iii*) énoncées par le théorème 4.1 et montrer qu'elles impliquent cette conjecture (c'est-à-dire que si elles sont posées, les nombres naturels $\binom{n}{i}$ ne peuvent être que ceux que cette conjecture établit). Dans ce cas, on abandonne le développement binomial et on ne s'occupe que des coefficients $\binom{n}{i}$, en conduisant une démonstration qui reste, en tant que telle, totalement indépendante de la considération de ce développement. Mais on peut aussi laisser les conditions (*i*)-(*iii*) énoncées par le théorème 4.1 de côté et travailler directement sur le développement binomial. Naturellement les deux démonstrations aboutissent finalement au même résultat, et procèdent l'une et l'autre par récurrence, mais tandis que dans le premier cas on n'a le résultat cherché qu'en couplant le nouveau théorème et le théorème 4.1, dans le deuxième cas, le résultat cherché est directement exprimé par le nouveau théorème et est donné indépendamment du théorème 4.1.

Pour des raisons de clarté, je montre d'abord comment raisonner si on choisit la deuxième possibilité. Il s'agit d'énoncer puis de démontrer le théorème suivant :

THÉORÈME 4.2. *Si $n$ est un nombre naturel quelconque et $a$ et $b$ deux quantités quelconques, alors*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

*où les facteurs $\binom{n}{i}$ $(i = 1, ..., n)$ sont des nombres naturels donnés par la formule suivante :*

$$\binom{n}{i} = \frac{n(n-1)(n-2)...[n-(i-1)]}{1 \cdot 2 \cdot ... \cdot i}$$

*et $\binom{n}{0} = 1$.*

Avant de présenter la preuve de ce théorème, il convient d'introduire de nouvelles notations : si $p$ est un nombre naturel quelconque plus grand que 0, alors on indique le produit $1 \cdot 2 \cdot ... \cdot p$ par le symbole « $p!$ », qu'on lit habituellement « $p$ factoriel » ou « factoriel $p$ » (si $p = 0$, on suppose, par convention notationnelle, que $p! = 0! = 1$) ; si $p$ et $q$ sont des nombres naturels quelconques, tels que $p \leq q$ , et $u_p, u_{p+1}, ..., u_q$ des éléments d'un ensemble quelconque sur lequel on a défini une addition et une multiplication associatives, alors on note le produit $u_p \cdot u_{p+1} \cdot ... \cdot u_q$ par le symbole « $\prod_{k=p}^{q} u_k$ ». La deuxième partie du théorème 4.2 affirmera alors que, si $i = 0$, le coefficient binomial $\binom{n}{i} = \binom{n}{0}$ est, quel que soit $n$, égal à 1, et si $1 \leq i \leq n$, le coefficient binomial $\binom{n}{i}$ est donné, quel que soit $n$, par la formule suivante :

$$\binom{n}{i} = \frac{\prod_{k=0}^{i-1} (n-k)}{i!} \tag{18}$$

La preuve peut être donnée par récurrence sur la valeur de $n$. En conduisant cette preuve, il faut pourtant faire attention à ne pas tomber dans l'erreur qu'on a dénoncée au début du présent paragraphe. En effet la loi qui détermine le coefficient $\binom{n}{i}$ d'après le théorème 4.2 change en passant de $i = 0$ à $i = 1$. Ainsi, si on exploite la condition $\binom{n}{0} = 1$ pour prouver que $(a+b)^0 = \sum_{i=0}^{0} \binom{0}{i} a^{0-i} b^i$, et ensuite on exploite la condition 18 pour prouver que si $(a+b)^s = a^s + \sum_{i=1}^{s} \binom{s}{i} a^{s-i} b^i$, alors $(a+b)^{s'} = a^{s'} + \sum_{i=1}^{s'} \binom{s'}{i} a^{s'-i} b^i$, on n'aura pas démontré correctement le théorème, car cette dernière implication ne concerne pas le passage du cas $n = 0$ au cas $n = 1$, à cause du fait que la 18 n'intervient pas dans le développement de $(a+b)^0$. La manière la plus simple d'éviter cet erreur est de démontrer le théorème pour $n = 0$, naturellement sans utiliser la 18 ; de prouver ensuite que si $n = 1$, alors

$$(a+b)^n = a^n + \sum_{i=1}^{n} \binom{n}{i} a^{n-i} b^i$$

en exploitant autant la condition $\binom{n}{0} = 1$ que la (18) ; et d'employer cette dernière preuve comme base d'une récurrence, en prouvant ensuite que si $s$ est un nombre naturel quelconque différent de zéro et

$$(a+b)^s = a^s + \sum_{i=1}^{s} \binom{s}{i} a^{s-i} b^i$$

alors

$$(a+b)^{s'} = a^{s'} + \sum_{i=1}^{s'} \binom{s'}{i} a^{s'-i} b^i$$

La preuve du théorème 4.2 consiste alors en trois parties distinctes. La voici.

**Preuve du théorème 4.2** ($a$) Si $n = 0$, on aura

$$(a+b)^n = (a+b)^0 = 1$$

et, si quel que soit $n$, $\binom{n}{0} = 1$,

$$\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i = \sum_{i=0}^{0} \binom{0}{i} a^{0-i} b^i = \binom{0}{0} a^0 b^0 = 1$$

et donc la condition énoncée par le théorème est vérifiée dans ce cas.

($b$) Si $n = 1$, on aura ensuite

$$(a+b)^n = a + b$$

et, d'après la (18),

$$\sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i = \sum_{i=0}^{1} \binom{1}{i} a^{1-i} b^i = \binom{1}{0} a + \binom{1}{1} b = a + b$$

et la condition énoncée par le théorème est aussi vérifiée.

($c$) Il ne reste donc qu'à prouver que

$$\left[(a+b)^s = a^s + \sum_{i=1}^{s} \frac{\prod_{k=0}^{i-1}(s-k)}{i!} a^{s-i}b^i\right] \quad \Rightarrow$$

$$\Rightarrow \quad \left[(a+b)^{s'} = a^{s'} + \sum_{i=1}^{s'} \frac{\prod_{k=0}^{i-1}(s'-k)}{i!} a^{s'-i}b^i\right]$$

quel que soit le nombre naturel $s$ différent de 0. Or, si

$$(a+b)^s = a^s + \sum_{i=1}^{s} \frac{\prod_{k=0}^{i-1}(s-k)}{i!} a^{s-i}b^i$$

alors :

$$\begin{aligned}
(a+b)^{s'} &= (a+b)^{s+1} = (a+b)^s(a+b) = \\
&= \left[a^s + \sum_{i=1}^{s} \frac{\prod_{k=0}^{i-1}(s-k)}{i!} a^{s-i}b^i\right](a+b) = \\
&= a^{s+1} + a^s b + a\left[\sum_{i=1}^{s} \frac{\prod_{k=0}^{i-1}(s-k)}{i!} a^{s-i}b^i\right] + \\
&\quad + b\left[\sum_{i=1}^{s} \frac{\prod_{k=0}^{i-1}(s-k)}{i!} a^{s-i}b^i\right] = \\
&= a^{s+1} + a^s b + \\
&\quad + \left[s\cdot a^s b + ... + \frac{\prod_{k=0}^{h-1}(s-k)}{h!} a^{s-h+1}b^h + ... + ab^s\right] + \\
&\quad + \left[s\cdot a^{s-1}b^2 + ... + \frac{\prod_{k=0}^{h-2}(s-k)}{(h-1)!} a^{s-h+1}b^h + ... + b^{s+1}\right]
\end{aligned}$$

$h$ étant un nombre naturel quelconque compris entre 1 et $s$. En exécutant les additions des termes semblables, on aura alors :

$$\begin{aligned}
(a+b)^{s'} &= a^{s+1} + (s+1)a^s b + ... + \\
&\quad + \left(\frac{\prod_{k=0}^{h-1}(s-k)}{h!} + \frac{\prod_{k=0}^{h-2}(s-k)}{(h-1)!}\right) a^{s-h+1}b^h + ... + b^{s+1}
\end{aligned}$$

Or, il est clair que si les choses sont telles que l'affirme le théorème 4.2, c'est-à-dire que, au-delà du premier, les coefficients du développement de $(a+b)^n$ sont donnés, pour tout nombre naturel $n \neq 0$, par les fractions

$$\frac{\prod_{k=0}^{i-1}(n-k)}{i!} \qquad (i = 1, 2, ..., n) \tag{19}$$

alors ces fractions ne peuvent qu'exprimer des nombres naturels. En fait si ce n'était pas le cas, le théorème 4.1 serait contredit. Il est pourtant également clair que, si on n'a pas démontré auparavant le théoème 4.1, la preuve du théorème 4.2 ne peut pas se fonder sur cette conclusion qui dérive, justement, du fait qu'on a supposé la validité d'une partie de ce même théorème. De surcroît, même si on suppose que les coefficients binomiaux sont des nombres naturels, on ne pourra les sommer en général, c'est-à-dire indépendamment de leur détermination particulière, qu'en les exprimant sous la forme (19) et en appliquant, comme tout à l'heure, l'algorithme d'addition des nombres fractionnaires. Or, l'application de cet algorithme nous donne, quel que soit le nombre naturel $h \neq 0$, les égalités suivantes :

$$\begin{aligned}
\left( \frac{\prod_{k=0}^{h-1}(s-k)}{h!} + \frac{\prod_{k=0}^{h-2}(s-k)}{(h-1)!} \right) &= \left( \frac{\left[\prod_{k=0}^{h-1}(s-k)\right] + \left[h \cdot \prod_{k=0}^{h-2}(s-k)\right]}{h!} \right) \\
&= \frac{\left[\prod_{k=0}^{h-2}(s-k)\right] \cdot [(s-h+1)+h]}{h!} \\
&= \frac{\left[\prod_{k=0}^{h-2}(s-k)\right] \cdot [s+1]}{h!} \\
&= \frac{\left[\prod_{k=0}^{h-1}[(s+1)-k]\right]}{h!} = \frac{\left[\prod_{k=0}^{h-1}(s'-k)\right]}{h!}
\end{aligned}$$

d'où il est facile de conclure que :

$$\begin{aligned}
(a+b)^{s'} &= a^{s+1} + (s+1)a^s b + ... + \\
&\quad + \frac{\left[\prod_{k=0}^{h-1}(s'-k)\right]}{h!} a^{s-h+1} b^h + ... + b^{s+1} \\
&= a^{s'} + \sum_{i=1}^{s'} \frac{\left[\prod_{k=0}^{i-1}(s'-k)\right]}{i!} a^{s'-i} b^i
\end{aligned}$$

ce qu'il fallait démontrer. □

Il est clair que, si on établit le développement du binôme de degré $n$, en se fondant sur le théorème précédent, démontré de cette manière, le long argument qui précède l'énoncé de ce théorème est strictement inutile pour la solution de notre problème, car la récurrence qui dans cette preuve assure que la nature des coefficients binomiaux est celle indiquée nous assure aussi que ces coefficients sont les entrées successives du triangle de Pascal et que le développement cherché a la forme indiquée par la (17). Pourtant, cet argument, qui porte au théorème 4.1, est indispensable d'un point de vue heuristique, pour parvenir à avancer la conjecture que la preuve précédente transforme en théorème. L'énoncé du théorème 4.2 serait inimaginable sans la suggestion préalable dérivant de cet argument. De surcroît, comme je l'ai dit, on peut parvenir à un résultat analogue par une autre voie, en employant le théorème 4.1 comme un lemme essentiel. Il s'agira pour cela d'énoncer, puis de démontrer, le théorème suivant :

THÉORÈME 4.3. *Si* $\binom{n}{i}$ *est un nombre naturel, dont la valeur dépend des valeurs de deux autres nombres naturels* $n$ *et* $i$*, et qui satisfait aux conditions (i) et (iii) énoncées par le théorème 4.1, alors, quel que soit* $n$*, si* $1 \leq i \leq n$ *, on a nécessairement :*

$$\binom{n}{i} = \frac{n(n-1)(n-2)...[n-(i-1)]}{1 \cdot 2 \cdot ... \cdot i} = \frac{\prod_{k=0}^{i-1}(n-k)}{i!} \tag{20}$$

*(pour ce qui est de la condition (ii) énoncée par le même théorème, on note que si* $i > n$*, alors*

$$\frac{\prod_{k=0}^{i-1}(n-k)}{i!} = \frac{n \cdot (n-1) \cdot ... \cdot (n-n) \cdot ...}{i!} = \frac{n \cdot (n-1) \cdot ... \cdot 0 \cdot ...}{i!} = \frac{0}{i!} = 0$$

*de sorte que cette condition est aussi respectée lorsqu'on suppose que la (20) vaut pour tout nombre naturel* $i \neq 0$*).*

**Preuve** La preuve se fait par le biais de deux inductions complètes emboîtées l'une dans l'autre.

($a$) On considère d'abord le cas $n = 1$. Comme, d'après la condition ($i$) — ou les conditions ($i$) et ($iii$), qui sont naturellement compatibles — on a

$$\binom{1}{1} = \binom{0}{0} + \binom{0}{1} = 1 + 0 = 1.$$

il suffira de vérifier que :

$$\frac{\prod_{k=0}^{0}(1-k)}{1!} = 1$$

Ce qui est très facile, car

$$\frac{\prod_{k=0}^{0}(1-k)}{1!} = \frac{1-0}{1} = 1$$

($b$) Après quoi il s'agit de vérifier que : si $1 \leq i \leq s$, les conditions *(i)* et *(iii)* énoncées par le théorème 4.1 sont respectées, et

$$\binom{s}{i} = \frac{\prod_{k=0}^{i-1}(s-k)}{i!}$$

alors, si $1 \leq i \leq s'$ :

$$\binom{s'}{i} = \frac{\prod_{k=0}^{i-1}(s'-k)}{i!}$$

On suppose donc que $1 \leq s$, et on considère d'abord le cas $i = 1$. On aura alors la première étape de la deuxième induction :

($b_\alpha$) Comme il est alors certain que $i < s'$, car $i = 1 \leq s < s + 1 = s'$, il faut démontrer que : si $s$ est un nombre naturel plus grand ou égal à 1, si les conditions *(i)* et *(iii)* énoncées

par le théorème 4.1 sont respectées, alors :

$$\left[\binom{s}{1} = \frac{\prod_{k=0}^{0}(s-k)}{1!}\right] \Rightarrow \left[\binom{s'}{1} = \frac{\prod_{k=0}^{0}(s'-k)}{1!}\right]$$

Cette preuve est également très simple, car

$$\frac{\prod_{k=0}^{0}(s'-k)}{1!} = \frac{s'}{1} = s' = s+1$$

et donc, si

$$\binom{s}{1} = \frac{\prod_{k=0}^{0}(s-k)}{1!}$$

les conditions $(i)$ et $(iii)$ énoncées par le théorème 4.1 nous permettent de conclure que :

$$\binom{s'}{1} = \binom{s+1}{1} = \binom{s}{1} + \binom{s}{0} = \frac{\prod_{k=0}^{0}(s-k)}{1!} + 1 = \frac{s}{1} + 1 = s+1 = \frac{\prod_{k=0}^{0}(s'-k)}{1!}$$

$(b_\beta)$ Il reste à franchir la deuxième étape de la deuxième induction : pour cela il faudra démontrer que si l'implication énoncée ci-dessus est satisfaite pour $i = t$, $t$ étant un nombre naturel quelconque compris entre 1 et $s$, alors cette même implication est aussi satisfaite pour $i = t'$. En d'autres termes, il faut prouver que, quel que soit $t$, si

$$(21) \qquad \left(\begin{array}{c}[1 \leq t \leq s] \wedge \\ [(i) \wedge (iii)] \wedge \\ \binom{s}{t} = \frac{\prod_{k=0}^{t-1}(s-k)}{t!}\end{array}\right) \Rightarrow \left([1 \leq t \leq s'] \Rightarrow \binom{s'}{t} = \frac{\prod_{k=0}^{t-1}(s'-k)}{t!}\right)$$

alors

$$\left(\begin{array}{c}[1 \leq t' \leq s] \wedge \\ [(i) \wedge (iii)] \wedge \\ \binom{s}{t'} = \frac{\prod_{k=0}^{t'-1}(s-k)}{t'!}\end{array}\right) \Rightarrow \left([1 \leq t' \leq s'] \Rightarrow \binom{s'}{t'} = \frac{\prod_{k=0}^{t'-1}(s'-k)}{t'!}\right)$$

Or, si $1 \leq t' \leq s'$ de la $(iii)$ il suit que

$$\binom{s'}{t'} = \binom{s}{t'} + \binom{s}{t}$$

et, si $\binom{s}{t'} = \frac{\prod_{k=0}^{t'-1}(s-k)}{t'!}$, alors

$$\binom{s'}{t'} = \frac{\prod_{k=0}^{t'-1}(s-k)}{t'!} + \binom{s}{t}$$

Mais, de la 21 et de l'égalité

$$\binom{1}{1} = \frac{\prod_{k=0}^{0}(1-k)}{1!}$$

qu'on a déjà démontrée, il suit, par induction complète, que, pour tout $i$, si $1 \leq i \leq s$, alors $\binom{s}{i} = \frac{\prod_{k=0}^{i-1}(s-k)}{i!}$ et donc

$$\binom{s}{t} = \frac{\prod_{k=0}^{t-1}(s-k)}{t!}$$

et de là

$$\begin{aligned}
\binom{s'}{t'} &= \frac{\prod_{k=0}^{t'-1}(s-k)}{t'!} + \frac{\prod_{k=0}^{t-1}(s-k)}{t!} \\
&= \frac{\prod_{k=0}^{t}(s-k) + (t+1)\prod_{k=0}^{t-1}(s-k)}{t'!} \\
&= \frac{\left[\prod_{k=0}^{t-1}(s-k)\right][(s-t)+(t+1)]}{t'!} = \frac{\left[\prod_{k=0}^{t-1}(s-k)\right][s+1]}{t'!} \\
&= \frac{\prod_{k=0}^{t}[(s+1)-k]}{t'!} = \frac{\prod_{k=0}^{t'-1}[s'-k]}{t'!}
\end{aligned}$$

ce qui clôture la démonstration. □

Remarque 3.10. Comme la démonstration précédente nous permet de le supposer, le nombre naturel $\binom{n}{i}$ recouvre en mathématiques une fonction plus large que celle de simple coefficient binomial. Il ne serait, par exemple, pas trop difficile de démontrer qu'il indique le nombre des sous-ensembles contenant $i$ éléments (distincts) d'un ensemble donné quelconque contenant $n$ éléments, ce qu'on appelle en général des « combinaisons de $i$ éléments d'un ensemble à $n$ éléments ».

Ainsi, si on veut savoir, par exemple, combien de jeux distincts peut recevoir un joueur de belote, il suffit de calculer le nombre

$$\binom{32}{8} = \frac{\prod_{k=0}^{8-1}(32-k)}{8!}$$

ce qui donne le nombre considérable de

$$\frac{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} = 1 \cdot 31 \cdot 5 \cdot 29 \cdot 4 \cdot 9 \cdot 13 \cdot 5 = 10.518.300$$

Cette observation montre une des raisons pour lesquelles le développement binomial apparaît comme le point d'intersection de nombreuses théories mathématiques, ce qui confère au résultat précédemment démontré un rôle important dans l'édifice des mathématiques.

Note Historique 3.6. L'effort de distinguer entre elles différentes sortes de nombres entiers positifs, et donc de classifier ces dernières en accord avec quelques critères, remonte à l'aube des mathématiques. La classification apparemment la plus naturelle, et sans doute la plus connue, celle entre nombres pairs et impairs, était certainement déjà connue par les pythagoriciens, comme il est attesté par quelques

fragments et différents témoignages. Celle-ci n'était pourtant pas la seule classification dont les pythagoriciens se servaient. Une autre — qui, bien que moins connue par les non-mathématiciens, ne fut non plus jamais abandonnée ensuite, et constitue encore aujourd'hui un élément primordial de la théorie des nombres — relève, au moins pour son origine, du pouvoir de représentation des nombres.

Si on représente une unité par un point, et, au lieu de représenter des nombres entiers par une simple succession linéaire de points, on les représente par des configurations bi-dimensionnelles, on se rend compte assez facilement que les nombres 3, 6, 10, ... peuvent être représentés par des triangles emboîtés, et représenter donc, à leur tour, des triangles :

## Première Figure p. 187

Les pythagoriciens appelaient ces nombres « triangulaires » .

Il suffit de disposer les points de façon à former des triangles rectangles, pour se rendre compte qu'en additionnant deux nombres triangulaires successifs, on obtient des nombres « carrés », 4, 9, 16, ..., c'est-à-dire des nombres qui peuvent être représentés par des carrés emboîtés, et représenter donc ces carrés :

## Seconde Figure p. 187

Comme les nombres triangulaires correspondent aux sommes successives de l'addition réitérée $1+2+3+4+\ldots$ et les nombres carrés ne sont que carrés des nombres entiers positifs, il s'ensuit que, pour tout nombre entier positif $n$, on a

$$[1+2+...+n+(n+1)]+(1+2+...+n)=(n+1)\times(n+1)$$

et donc

$$(1+2+...+n)+(1+2+...+n)=(n+1)\times n$$

d'où on tire sur le champ la formule du chapitre 3 :

$$1+2+...+n=\frac{n(n+1)}{2}$$

On comprendra alors que la preuve de cette formule, qu'on a présentée dans le paragraphe 1 n'est rien qu'une version arithmétique d'une preuve bien plus ancienne et primordiale, fondée sur la théorie des nombres triangulaires et des nombres carrés.

Il semble que des techniques démonstratives de telle sorte, fondées sur le pouvoir représentatif des nombres, étaient très répandues dans les mathématiques préeuclidiennes ; aujourd'hui on les qualifie généralement de « techniques arithmo-géométriques ».

Une fois qu'on a compris l'esprit de la distinction entre nombres triangulaires et nombres carrés, il n'est pas difficile de continuer, en passant successivement aux nombres pentagonaux, hexagonaux, etc., respectivement : 5, 12, 22,... ; 6, 15, 28,... ; etc. Les représentations de ces nombres sont les suivantes :

## Figure p. 188

## Première Figure p. 189

Il est facile de voir que ces nombres sont donnés respectivement par les sommes successives des additions réitérées :

$$1+4+7+10+... \qquad \text{et} \qquad 1+5+9+13+...$$

qui donnent en même temps la loi de leur formation et le principe de généralisation de la classification précédente.

Pris dans leur ensemble, les nombres triangulaires, carrés, pentagonaux, hexagonaux, etc. sont dits, pour une raison qu'il est facile de comprendre, « nombres figurés plans ».

Il y a pourtant une autre manière de continuer la classification commencée par la caractérisation des nombres triangulaires. Il s'agit d'abord d'imaginer que différents nombres triangulaires se disposent dans l'espace sur des plans différents, de manière à donner lieu à des pyramides emboîtées :

Seconde Figure p. 189

On aura ainsi les nombres dits « pyramidaux », qu'on pourra penser comme une espèce particulière de nombres figurés solides.

Il est clair que les nombres pyramidaux successifs, 4, 10, 20,... sont les sommes successives de l'addition réitérée des nombres triangulaires, 1+3+6+10+... En continuant de cette manière, en imaginant des configurations de points dans des espaces de 4, 5, 6,... dimensions, on construira des nombres triangulaires d'ordre 4, 5, 6,... Les nombres triangulaires d'ordre 4, c'est-à-dire 5, 15, 35,..., seront évidemment les sommes successives de l'addition réitérée des nombres pyramidaux, 1+4+10+20+... ; les nombres triangulaires d'ordre 5, c'est-à-dire 6, 21, 56,... seront ensuite les sommes successives de l'addition réitérée des nombres triangulaires d'ordre 4, $1 + 5 + 15 + 35 + ...$ ; et ainsi de suite. Il est facile de constater que de cette manière on retrouve les coefficients binomiaux, c'est-à-dire les entrées du triangle de Pascal, dont les colonnes peuvent ainsi être pensées comme les successions des nombres triangulaires des différents ordres. On n'aura plus de difficultés alors à comprendre que les nombres qui apparaissent dans le triangle de Pascal jouent, dans la théorie des nombres, un rôle essentiel, bien plus large que celui de simples coefficients du développement binomial.

**Lectures possibles** : T. Heath, *A History of Greek Mathematics*, Clarendon Press, Oxford, 1921 (réédition : Dover, New York, 1981 (2 vols.)).

Remarque 3.11. Ci-dessus, nous avons laissé en suspens le problème de la détermination de la somme de l'addition $\sum_{i=0}^{n} i^m$, quels que soient les nombres naturels $n$ et $m$. La connaissance du développement binomial pour un exposant naturel quelconque nous permet de calculer cette somme par une méthode récursive très astucieuse remontant pour l'essentiel à Pascal (qui l'exposa en un court traité annexé au *Traité du triangle arithmétique* cf. la note 3.5). Il s'agit d'abord d'employer la formule qui donne le développement binomial pour l'exposant $m+1$, pour calculer successivement les termes $0^{m+1}, 1^{m+1}, 2^{m+1}, ..., n^{m+1}, (n+1)^{m+1}$

de la somme $\sum_{i=0}^{n+1} i^{m+1}$ :

$$\begin{aligned}
0^{m+1} &= 0^{m+1} \\
1^{m+1} &= 1^{m+1} \\
2^{m+1} &= (1+1)^{m+1} = \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} 1^j \\
3^{m+1} &= (1+2)^{m+1} = \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} 2^j \\
4^{m+1} &= (1+3)^{m+1} = \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} 3^j \\
&\ldots \\
n^{m+1} &= [1+(n-1)]^{m+1} = \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} (n-1)^j \\
(n+1)^{m+1} &= (1+n)^{m+1} = \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} n^j
\end{aligned}$$

En additionnant membre à membre (et en observant que $0^0 = 1$), on aura :

$$\begin{aligned}
\sum_{i=0}^{n+1} i^{m+1} &= \sum_{i=0}^{n} \left[ \sum_{j=0}^{m+1} \binom{m+1}{j} 1^{m+1-j} i^j \right] \\
&= \sum_{i=0}^{n} \binom{m+1}{0} 1^{m+1} i^0 + \sum_{i=0}^{n} \binom{m+1}{1} 1^m i^1 + \\
&\quad + \sum_{i=0}^{n} \binom{m+1}{2} 1^{m-1} i^2 + \ldots + \sum_{i=0}^{n} \binom{m+1}{m-1} 1^2 i^{m-1} + \\
&\quad + \sum_{i=0}^{n} \binom{m+1}{m} 1^1 i^m + \sum_{i=0}^{n} \binom{m+1}{m+1} 1^0 i^{m+1} \\
&= \binom{m+1}{0} \sum_{i=0}^{n} i^0 + \binom{m+1}{1} \sum_{i=0}^{n} i^1 + \\
&\quad + \binom{m+1}{2} \sum_{i=0}^{n} i^2 + \ldots + \binom{m+1}{m-1} \sum_{i=0}^{n} i^{m-1} + \\
&\quad + \binom{m+1}{m} \sum_{i=0}^{n} i^m + \binom{m+1}{m+1} \sum_{i=0}^{n} i^{m+1}
\end{aligned}$$

Et comme

$$\binom{m+1}{m+1} = 1$$

et

$$\sum_{i=0}^{n} i^{m+1} = \left( \sum_{i=0}^{n+1} i^{m+1} \right) - (n+1)^{m+1}$$

de là, il sera très facile de tirer :

$$\sum_{i=0}^{n} i^m = \frac{1}{\binom{m+1}{m}} \left[ (n+1)^{m+1} - \left( \begin{array}{c} \binom{m+1}{0} \sum_{i=0}^{n} i^0 + \binom{m+1}{1} \sum_{i=0}^{n} i^1 + \\ + \binom{m+1}{2} \sum_{i=0}^{n} i^2 + \dots \\ \dots + \binom{m+1}{m-1} \sum_{i=0}^{n} i^{m-1} \end{array} \right) \right] \tag{22}$$

Comme les coefficients binomiaux qui entrent dans cette égalité sont tous connus, grâce à la (20), il suffit de connaître les sommes des additions $\sum_{i=0}^{n} i^0 = \sum_{i=0}^{n} 1 = n+1$, $\sum_{i=0}^{n} i^1 = \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$,...,$\sum_{i=0}^{n} i^{m-1}$ pour en tirer la somme de l'addition $\sum_{i=0}^{n} i^m$.

Pour ne faire qu'un exemple, si on pose $m = 4$, on aura, d'après la (22) :

$$\begin{aligned} \sum_{i=0}^{n} i^4 &= \frac{1}{\binom{5}{4}} \left[ (n+1)^5 - \left( \begin{array}{c} \binom{5}{0} \sum_{i=0}^{n} i^0 + \binom{5}{1} \sum_{i=0}^{n} i^1 + \\ + \binom{5}{2} \sum_{i=0}^{n} i^2 + \binom{5}{3} \sum_{i=0}^{n} i^3 \end{array} \right) \right] \\ &= \frac{1}{5} \left[ (n+1)^5 - \left( \begin{array}{c} (n+1) + 5\frac{n(n+1)}{2} + \\ +10\frac{n(n+1)(2n+1)}{6} + 10\frac{[n(n+1)]^2}{4} \end{array} \right) \right] \\ &= \frac{n+1}{5} \left[ (n+1)^4 - 1 - \frac{5}{2}n - \frac{10}{6}n(2n+1) - \frac{10}{4}n^2(n+1) \right] \\ &= \frac{n\,(n+1)}{5} \left[ n^3 + \frac{3}{2}n^2 + \frac{1}{6}n - \frac{1}{6} \right] \end{aligned}$$

Le lecteur pourra considérer des valeurs petites de $n$ et vérifier que ce produit est un nombre naturel (montrer que ceci est le cas pour tout $n$, indépendamment de la considération de la (22), n'est pas facile, même si ceci est évidemment le cas) et qu'il est en particulier la somme de l'addition $\sum_{i=0}^{n} i^4$.

En se fondant sur la (22) et en employant des méthodes fondamentales en algèbre linéaire (la théorie des systèmes d'équations du premier degré), on arrive ensuite à démontrer une formule qui donne directement la somme de $\sum_{i=0}^{n} i^m$ pour tout $m$ naturel. Il est pourtant impossible de donner ici ne serait-ce qu'une esquisse de ces méthodes et même d'énoncer cette formule sous forme compacte, sans employer des notations et des notions qu'il serait trop long et difficile d'introduire.

CHAPITRE 4

# Nombres rationnels

Dans le chapitre précédent, on a plusieurs fois utilisé des nombres fractionnaires, en supposant connues les règles fondamentales par lesquelles on opère sur ces nombres. Le moment est maintenant venu de justifier cette pratique et de définir précisément une classe de nombres plus large que la classe des nombres entiers positifs ou naturels, et qui contient justement des objets qu'on peut reconnaître comme des nombres fractionnaires. Ceci peut être fait de différentes manières : autant par le biais de l'identification des nombres fractionnaires avec des objets d'une nature déterminée (comme on l'a fait dans le chapitre 1, pour les nombres entiers positifs), que de manière purement formelle (comme on l'a en revanche fait dans le chapitre 2, pour les nombres naturels), ne se fondant que sur un système d'axiomes qui fournit une définition implicite de ces derniers nombres. La première stratégie correspond à l'exigence de nous doter d'outils aussi efficaces et commodes que les nombres entiers positifs pour faire face aux besoins de la mesure. La deuxième correspond à l'exigence de disposer d'objets identifiables comme le résultat de n'importe quelle division réalisable sur les nombres naturels (et ensuite, réitérativement, sur les nombres qu'on atteint par des extensions successives de $\mathbb{N}$). La première est une exigence pratique, les mathématiques étant pensées comme un outil ; la seconde est une exigence théorique et ne répond qu'à une recherche d'équilibre et d'élégance de nos systèmes formels. On peut penser qu'historiquement cette dernière a été ressentie de manière d'autant plus pressante qu'elle concordait manifestement avec la première. Bien que la deuxième exigence n'ait pas attendu l'axiomatique de Peano (ou de Dedekind) pour se manifester, nous pouvons identifier, dans le cadre de notre exposé, la première exigence avec une exigence d'extension de la classe des nombres entiers positifs, ainsi qu'ils ont été définis dans le chapitre 1, et la deuxième avec une exigence d'extension de la classe des nombres naturels, ainsi qu'ils ont été définis dans le chapitre 2. Encore une fois, on suivra d'abord la première stratégie et on partira des résultats atteints de cette manière pour justifier la mise en place d'une axiomatique.

REMARQUE 4.1. On cherchera ainsi à montrer, sur un nouvel exemple, comment, en mathématiques, la construction d'un système formel est toujours redevable d'un but — celui de caractériser formellement une structure relationnelle qui a déjà été, d'une manière ou d'une autre, identifiée —, de sorte que les axiomes (et les définitions) d'un tel système ne fonctionnent jamais comme des prémisses arbitraires, mais visent plutôt à exprimer des conditions propres à cette structure relationnelle.

## 1. Les nombres fractionnaires strictement positifs en tant que corrélats de l'acte de partager

Bien que dans les mathématiques modernes, la notion de mesure ait pris une connotation technique fort précise — qui dérive de la généralisation de la théorie de l'intégration, proposée au tout début du XX$^{e}$ siècle par le mathématicien français Henri L. Lebesgue — sa présence dans l'édifice des mathématiques remonte à l'Antiquité. La notion moderne de mesure formalise

une pratique courante dans les mathématiques qui précède largement son introduction : cette pratique consistait dans le simple fait d'associer un nombre (ou un élément d'un ensemble convenablement choisi) à un objet donné, de manière à exprimer par le biais de ce nombre (ou de cet élément) des propriétés relationnelles de l'objet en question. C'est par exemple ce qu'on fait tous les jours quand on parle de longueur (et même, plus généralement de mesure) : en disant que ma salle à manger fait cinq mètres de long (ou mesure cinq mètres), j'associe le nombre cinq à ma salle à manger, par l'intermédiaire de l'unité, dite justement « de mesure », que constitue le mètre.

NOTE HISTORIQUE 4.1. Dans le *Discours préliminaire de l'Encyclopédie*, d'Alembert définit la quantité comme « tout ce qui est susceptible d'augmentation ou de diminution ». Cette définition célèbre ne serait certes pas convenable aujourd'hui, mais il reste utile de s'y rapporter pour comprendre ce que les mathématiciens ont, pendant plus de deux mille ans, considéré comme leur objet d'étude. Bien que cela ne fut jamais rendu explicite, il semble possible de dire que, avant l'aube des mathématiques modernes, les mathématiciens pensaient comme quantités des objets qu'on pouvait sommer et comparer entre eux selon une relation d'ordre strict, ou, le cas échéant, déclarer égaux. Naturellement, ceci ne signifie pas que toute quantité devait pouvoir être sommée, ou comparée à n'importe quelle autre quantité. Les quantités étaient plutôt pensées comme distinctes en différents domaines : les nombres, les segments, les polygones, etc. Les premiers étaient conçus comme des quantités discrètes, toutes les autres comme des quantités continues, ou, comme il était usuel de dire, des grandeurs. Les conditions de sommabilité et de comparabilité n'étaient évidemment satisfaites qu'à l'intérieur de ces différents domaines : pour ne prendre qu'un exemple, les segments étaient conçus comme des quantités, en particulier des grandeurs, parce qu'on savait sommer deux segments, les comparer entre eux, en disant lequel était le plus grand et lequel était le plus petit, ou, éventuellement, s'assurer du fait qu'ils étaient égaux.

Il est important d'observer qu'en disant de deux segments qu'on savait les sommer ou les comparer, on ne veut pas dire qu'on savait sommer ou comparer leurs longueurs. Ce qu'on veut dire est justement qu'on savait sommer ou comparer ces segments. La somme ou la comparaison de deux grandeurs ne faisait pas intervenir des entités étrangères, telles que des nombres d'une certaine nature, associés à ces grandeurs, sur lesquels on opérait, à défaut d'opérer sur les grandeurs elles-mêmes. Sommer deux segments signifiait par exemple en déplacer un à côté de l'autre, de manière à former, à partir de ces segments, un nouveau segment, résultant de la composition des segments donnés. En parlant de longueurs ou d'aires, les mathématiciens ne voulaient parler que d'un attribut des grandeurs, l'attribut qui était invariable sous un changement de position.

Les choses commencèrent à changer à partir de la deuxième moitié du XVI$^{\text{ème}}$ siècle, avec la naissance de ce que nous appelons aujourd'hui « théorie de l'intégration ». Le but de cette théorie était, à l'origine, d'évaluer l'espace renfermé par une courbe. On voulait d'abord réduire cet espace à un carré : construire un carré égal à la figure dont la courbe était la frontière. On se rendit pourtant compte assez vite, qu'on pouvait exprimer une courbe (ceci était du moins vrai pour certaines courbes, les seules qu'il parût intéressant d'étudier) par une équation portant sur des segments.

Naturellement, ceci n'eut lieu qu'après que Descartes ait donné un sens à la notion de produit de deux ou plusieurs segments (cf. la note historique 3.6). Descartes fut aussi le premier à se rendre compte qu'il était possible d'exprimer une courbe

par une équation portant sur des segments. Son idée était simple et géniale, et les mathématiciens ne l'abandonnèrent jamais plus. Juste un peu simplifiée, cette idée était la suivante. Qu'on prenne deux droites $r$ et $s$ qui se coupent selon un angle donné (pour rendre les choses plus simples, on peut supposer, sans aucune perte de généralité, que cet angle est droit). Ces droites définiront un plan. Un point $A$ étant pris sur ce plan, on trace de ce point deux droites, $r_A$ et $s_A$, respectivement parallèles aux droites données. Chacune de ces droites coupera celle, parmi les droites données, à laquelle elle n'est pas parallèle. Qu'on considère alors les deux segments pris sur les droites $r_A$ et $s_A$ et compris entre le point donné et les deux droites $r$ et $s$. Appelons-les « $x_A$ » et « $y_A$ ». Il est clair que ces segments, pris ensemble, caractérisent la position du point $A$, c'est-à-dire que dans le même plan, il n'y a aucun point $B$ non coïncidant avec $A$ , pour lequel, en faisant la même opération, on trouve deux segments, $x_B$ et $y_B$, respectivement égaux à $x_A$ et $y_A$. Les deux droites fixes $r$ et $s$ sont alors dites « axes cartésiens » et les deux segments $x_A$ et $y_A$ sont dits « coordonnées cartésiennes » du point $A$. Imaginons maintenant qu'une courbe soit tracée sur le plan dont il est question, et qu'elle soit telle que, quel que soit le point $Z$ qu'on prenne sur cette courbe, les deux coordonnées cartésiennes de $Z$, $x_Z$ et $y_Z$ satisfassent à une certaine équation, qu'on pourra noter par le symbole générique « $F(x_Z, y_Z) = 0$ ». On dira alors que cette équation exprime la courbe donnée.

La théorie de l'intégration naquit lorsque Newton, vers les années 1664-1666, se rendit compte du fait qu'il était possible d'opérer sur l'équation exprimant une certaine courbe, de manière à obtenir une écriture —Êqui indiquait des opérations possibles à accomplir sur un segment $x$, pris sur l'axe $r$ et conçu comme variable sur cet axe, entre deux points fixes quelconques— et qui pouvait à son tour être conçue comme une expression de l'espace compris entre la courbe donnée, l'axe $r$ et les parallèles à l'axe $s$ tirées vers la courbe, à partir des points limites de l'intervalle de variation de $x$ sur $r$. C'est la première forme de ce qu'on appelle aujourd'hui une « intégrale ».

Ce qui est intéressant, pour notre histoire, est que, en associant à un espace délimité par une courbe une écriture en $x$, ou, comme on le dira un peu plus tard, une fonction de $x$, Newton avait indiqué la possibilité de déterminer des propriétés relationnelles de cet espace, en opérant sur cette fonction. En particulier, il avait indiqué la possibilité de sommer et comparer deux espaces de telle nature en sommant et comparant les fonctions correspondantes.

Après Newton, les mathématiques continuèrent à évoluer fort rapidement. Si les mathématiciens n'oublièrent pas la grande leçon du jeune anglais (à l'époque de sa découverte, Newton avait moins de 25 ans), ils commencèrent à comprendre que, au lieu de travailler sur les segments, on pouvait opérer sur des nombres, dit réels (cf. le chapitre 6), exprimant les longueurs de ces segments. Du coup, ils commencèrent à comprendre qu'une intégrale pouvait être conçue comme un nombre réel caractérisant une certaine région du plan délimitée par une courbe. D'abord Cauchy, au début des années 1820, puis Riemann, une trentaine d'années plus tard, montrèrent comment on pouvait définir plus proprement une intégrale, pensée justement comme un nombre réel associé à une région du plan.

C'est ainsi que naquit l'idée moderne d'aire d'une surface : l'aire d'une surface est un nombre réel positif qui est associé à cette surface de manière à respecter certaines conditions. La plus fondamentale de ces conditions peut être exprimée ainsi : une surface étant donnée, coupons-la en deux ; si $X$ est l'aire de la surface donnée et

$X_1$ et $X_2$ sont les aires des deux surfaces résultant de cette coupure, il faut que $X_1 + X_2 = X$. Cette condition est dite « additivité de l'aireadditivité ».

La théorie de l'intégration de Riemann est une théorie puissante et magnifique, mais elle souffre de beaucoup de limitations, dont les mathématiciens se rendirent bientôt compte. Ils commencèrent alors à essayer de généraliser cette théorie, c'est-à-dire à la modifier de manière à pouvoir calculer l'intégrale référée à des courbes de plus en plus particulières et même à la rendre applicable non plus seulement aux surfaces délimitées, d'une manière ou d'une autre, par une de ces courbes, mais aussi à des ensembles de plus en plus abstraits. La notion moderne de mesure est un des résultats de ces efforts, dans lesquels s'illustrèrent entre autres, deux mathématiciens français : Émile Borel et Henri Lebesgue . Lebesgue fut probablement le premier à poser le problème à rebours : au lieu de se demander comment on pouvait mesurer un ensemble donné, il se demanda comment devait être fait un ensemble pour pouvoir être mesuré. Pour ce faire, il construisit d'abord une notion de mesure fort générale, en généralisant la notion d'aire associée à l'intégrale de Riemann, et, à partir de ceci, il se pencha sur la recherche des conditions de mesurabilité d'un ensemble.

La théorie issue de cet effort est une des plus belles théories des mathématiques, mais aussi une des plus sophistiquées et difficiles. On ne pourra certes pas en résumer ici les lignes fondamentales. On peut pourtant citer ce que Lebesgue lui-même écrivit dans un texte, *La mesure des grandeurs*, dans lequel il raisonnait sur la manière dont sa théorie aurait pu être enseignée à des jeunes élèves (on note qu'ici Lebesgue ne distingue pas entre une grandeur et sa mesure et appelle « grandeur d'un corps » ce que nous appellerions « mesure » d'une grandeur). Lebesgue note d'abord (on est au chapitre 6 de son texte, intitulé « Grandeurs mesurables » ) que : « La longueur d'un segment ou d'un arc de cercle, l'aire d'un polygone ou d'un domaine découpé dans une surface, le volume d'un polyèdre ou d'un corps ont été définis comme des nombres positifs attachés à des êtres géométriques et parfaitement définis par ces êtres au choix de l'unité près ». Il cherche alors à comprendre ce qui est commun à ces exemples et peut ainsi être généralisé. Cela l'amène à poser deux conditions qu'il énonce ainsi : « a) Une famille de corps étant donnée, on dit qu'on a défini pour ces corps une grandeur $G$, si, à chacun d'eux et à chaque partie de chacun d'eux, on a attaché un nombre positif déterminé. [...] b) Si l'on divise un corps $C$ en un certain nombre de corps partiels $C_1, C_2, \ldots, C_p$, et si la grandeur G est, pour ces corps, $g$ d'une part, $g_1, g_2, \ldots, g_p$, d'autre part, on doit avoir : $g = g_1 + g_2 + \ldots + g_p$ ». Il note ensuite que pour tirer des théorèmes généraux, à partir de ces conditions, il faut faire une « hypothèse supplémentaire », qu'il suggère pourtant de ne pas expliciter dans un cours d'introduction. Je n'accepterai pas ici cette suggestion ; voici comment Lebesgue formule cette hypothèse : « c) La famille des corps pour lesquels est définie une grandeur doit être assez riche pour que tout corps de la famille puisse être réduit à un point par diminutions successives, sans sortir de la famille et de manière qu'au cours de ces diminutions la grandeur décroisse continuement de sa valeur primitive à zéro ». Lebesgue continue naturellement son exposition ; je m'arrête par contre ici.

**Lectures possibles** : H. Lebesgue , *La mesure des grandeurs*, tomes XXXI (1931) à XXXIV (1935) de *L'Enseignement mathématique* ; A. Michel, *Histoire de la théorie de l'intégration*, Vrin, Paris, 1992 ; J.-P. Pier, *Histoire de l'intégration*, Masson, Paris, Milano, Barcellona, 1996.

* * *

Henri Lebesgue naquit à Beauvais, le 28 juin 1875, et mourut à Paris, le 26 juillet 1941. Après avoir étudié les mathématiques à l'École Normale Supérieure, et avoir enseigné deux ans au lycée central de Nancy, il enseigna aux universités de Rennes (entre 1902 et 1906) et de Poitiers (entre 1906 et 1910). En 1910, il fut nommé maître de conférence à la Sorbonne, où il devint professeur en 1919, deux ans avant d'être nommé au Collège de France. En 1922, il fut enfin nommé à l'Académie des Sciences. Il posa les bases de sa théorie de la mesure et de l'intégration pendant les années passées à Nancy, au tout début de sa carrière, qu'il consacra ensuite à développer et affiner ces idées. Vers la fin de sa vie, il consacra de nombreuses études et plusieurs écrits à la didactique des mathématiques et, en partie, à leur histoire.

**Lectures possibles** : L. Félix, *Message d'un mathématicien : Henri Lebesgue*, Blanchard, Paris, 1974.

Dans les mathématiques classiques, par exemple chez Euclide, on parle néanmoins de mesure dans un sens encore plus originel, dont plus tard découlera l'idée d'association : la mesure est conçue comme une relation entre deux objets de même nature, dépendant de la position respective de ces deux objets dans une hiérarchie fixée par une relation d'ordre et une opération d'addition, et correspondant à la possibilité de concevoir le premier de ces objets comme le résultat exact de l'opération qui ajoute le second objet à lui-même un certain nombre de fois. Naturellement ici le terme « nombre » renvoie aux nombres entiers positifs, ou, pour être encore plus précis, aux nombres entiers strictement positifs.

REMARQUE 4.2. Comme le lecteur l'aura aisément remarqué, l'expression « nombres entiers positifs » a été jusqu'ici utilisée pour se référer aux nombres entiers plus grands ou égaux à zéro : $0, 1, 2, \ldots$ Cependant, tout ce qu'on a dit généralement à propos de ces nombres aurait pu être dit aussi des nombres entiers plus grands que zéro : $1, 2, 3, \ldots$ Tout au plus, en voulant se référer seulement à ces derniers nombres, on aurait dû modifier convenablement, d'une manière tout à fait facile à imaginer, quelques-unes de nos formulations. La raison en est qu'on a traité jusqu'ici des nombres entiers positifs, pris dans leur ensemble, essentiellement comme des éléments d'une progression. Lorsqu'il a été nécessaire d'exclure le nombre zéro des nombres (naturels ou entiers positifs) auxquels on se référait, on l'a fait, de surcroît, de manière explicite. Pour des raisons que le lecteur comprendra facilement par la suite, il sera dorénavant plus avantageux d'introduire une nouvelle expression et de se référer aux nombres entiers plus grands que zéro par le terme « nombres entiers strictement positifs ». Cette expression est d'un usage courant en français et on ne fait ici que l'adopter (de même, on parlera plus tard des nombres fractionnaires strictement positifs pour se référer aux nombres fractionnaires plus grands que zéro et des nombres rationnels positifs pour se référer aux nombres rationnels plus grands ou égaux à zéro, mais comme ces termes feront l'objet de définitions explicites, il n'est pas nécessaire d'y insister ici).

Par exemple, de deux segments (non nuls) $a$ et $b$, on peut dire, selon le sens classique du terme « mesure » adopté par Euclide, que le premier mesure le deuxième si et seulement s'il existe un nombre entier strictement positif $n$, tel que $na = \underbrace{a + a + \ldots + a}_{n \text{ fois}} = b$ ; de même pour deux nombres entiers strictement positifs $p$ et $q$ : $p$ mesure $q$ si et seulement s'il existe un nombre entier strictement positif $n$, tel que $np = q$. Si c'est le cas, on dira alors, toujours dans ce sens classique du terme « mesure » (qui, je le répète, n'est pas celui qui est aujourd'hui habituel en mathématiques), que le segment $a$ et le nombre $p$ sont des mesures, respectivement, du segment $b$ et du nombre $q$.

Il est clair que tout couple de nombres entiers strictement positifs ne respecte pas cette condition : ce n'est pas le cas que, quels que soient les nombres entiers strictement positifs $p$ et $q$, ou bien $p$ mesure $q$, ou bien $q$ mesure $p$. Pourtant, si on appelle « mesure commune » de deux objets un troisième objet qui est (au sens précédent de ce terme) autant une mesure du premier que du deuxième objet, on peut démontrer facilement le théorème suivant :

THÉORÈME 1.1. *Pour tout couple de nombres entiers strictement positifs, $p$ et $q$, il existe un nombre entier positif $m$ qui est une mesure commune de $p$ et $q$.*

**Preuve** Pour conduire cette démonstration célèbre, Euclide s'est servi d'un algorithme qui aujourd'hui porte justement le nom d' « algorithme d'Euclide », et qu'on peut convenablement utiliser ici, en répétant, en substance, la même démonstration qu'Euclide lui-même. D'abord, si $p = q$, alors il suffit de montrer que, quel que soit le nombre entier strictement positif $p$, il existe deux nombres entiers strictement positifs $s$ et $n$ tels que $ns = p = q$. Or, si $n = 1$ et $s = p = q$, ceci est toujours le cas, donc : si $p = q$, alors $p$ et $q$ ont au moins deux mesures communes parmi les nombres entiers strictement positifs. Cela montre, en passant, que pour chaque nombre entier strictement positif $p$, il y a au moins deux nombres entiers strictement positifs qui sont mesures de $p$ : 1 et $p$ lui-même. Imaginons maintenant que $p \neq q$ et supposons que $p < q$. Il y aura sûrement un nombre entier strictement positif $n_1$ tel que

$$q - n_1 p = r_1 \qquad \text{et} \qquad 0 \leq r_1 < p$$

Si $r_1 = 0$, alors $q = n_1 p$ et $p$ mesure $q$, donc $p$ est une mesure commune à $p$ et à $q$. Si $0 < r_1 < p$, alors il y aura sûrement un nombre entier strictement positif $n_2$ tel que

$$p - n_2 r_1 = r_2 \qquad \text{et} \qquad 0 \leq r_2 < r_1$$

Si $r_2 = 0$, alors $p = n_2 r_1$ et $q = r_1 + n_1 p = (n_1 n_2 + 1) r_1$, donc $r_1$ mesure autant $p$ que $q$. Si $0 < r_2 < r_1$, alors il y aura sûrement un nombre entier strictement positif $n_3$ tel que

$$r_1 - n_3 r_2 = r_3 \qquad \text{et} \qquad 0 \leq r_3 < r_2$$

Si $r_3 = 0$, alors $r_1 = n_3 r_2$ c'est-à-dire $p = (n_2 n_3 + 1) r_2$ et $q = r_1 + n_1 p = n_3 r_2 + n_1 (n_2 n_3 + 1) r_2 = (n_3 + n_1 n_2 n_3 + n_1) r_2$, donc $r_2$ mesure autant $p$ que $q$. Si $0 < r_3 < r_2$, on raisonne comme avant, et ainsi de suite. Il est clair que, comme les restes $r_i$ $(i = 1, 2, \ldots)$ sont des nombres entiers positifs, de plus en plus petits, et qu'il n'existe pas de tels nombres plus petits que 0, on arrivera, au bout d'un nombre fini $m$ d'étapes, à l'égalité $r_m = 0$, qui nous permettra de conclure que $r_{m-1}$ est une mesure commune à $p$ et $q$. □

Si $r_{m-1} = 1$ est la seule mesure commune de $p$ et $q$, c'est-à-dire que, pour aucun nombre entier strictement positif $t$ plus petit que $m - 1$ on a $r_t = 0$, et qu'on a en revanche $r_{m-1} = 1$ (et donc $r_m = 0$) alors les deux nombres $p$ et $q$ seront dits « premiers entre eux », un nombre entier strictement positif, ou si on préfère naturel, étant dit « premier », comme on l'a déjà observé dans le chapitre 3, s'il est mesuré — ou, comme on le dit aujourd'hui, divisible — seulement par 1 et par lui-même.

NOTE HISTORIQUE 4.2. Formulées en termes modernes, les trois premières propositions du livre VII des *Éléments* énoncent, respectivement, un critère pour déterminer si deux nombres entiers positifs donnés sont ou non premiers entre eux et une procédure pour calculer le plus grand commun diviseur entre deux ou trois nombres non premiers entre eux. Pour illustrer la manière dont l'algorithme d'Euclide intervient dans les preuves de ces propositions, considérons d'abord la proposition VII.1.

Euclide y affirme que si deux nombres (entiers positifs) différents entre eux, disons, pour plus de clarté, $n$ et $m$, sont donnés et que le plus petit, disons $m$, est retranché du plus grand, autant de fois qu'il faut pour que le reste de soustraction,

disons $r_1$, soit plus petit que $m$ lui-même (sans être pour autant nul), et que $r_1$ est à son tour retranché de $m$, autant de fois qu'il faut pour que le reste de cette soustraction, disons $r_2$, soit plus petit que $r_1$ (sans être pour autant nul), et que $r_2$ est de nouveau retranché de $r_1$, autant de fois qu'il faut pour que le reste de cette soustraction, disons $r_3$, soit plus petit que $r_2$ (sans être pour autant nul), et ainsi de suite, jusqu'à trouver un reste égal à l'unité, alors les deux nombres donnés sont premiers entre eux, c'est-à-dire, en accord avec la définition VII.12, que leur seule mesure commune est l'unité. La preuve d'Euclide est naturellement une preuve par l'absurde. Celui-ci suppose que les deux nombres donnés, qu'il représente, comme d'habitude, par deux segments, AB et CD, ont une mesure commune différente de l'unité, disons $E$, et il montre que, si ces nombres se comportent l'un relativement à l'autre comme l'on vient de dire, alors $E$ doit mesurer l'unité, bien qu'il soit forcément plus grand que celle-ci, ce qui est évidemment impossible.

Dans la proposition VII.2, il s'agit, en revanche, dans le langage d'Euclide, de trouver la plus grande mesure commune entre deux nombres donnés, supposant que ces nombres ne sont pas premiers entre eux. Euclide suppose que les deux nombres sont AB et CD et que AB est plus grand que CD (si les deux nombres sont égaux, le problème est résolu d'emblée, car ils sont eux-mêmes la commune mesure cherchée). Si CD mesure AB, alors il est la mesure commune cherchée, et le problème est résolu. Si CD ne mesure pas AB, alors en appliquant l'algorithme d'Euclide, on devra nécessairement trouver, au bout d'un certain nombre d'étapes, un reste différent de l'unité qui mesure le reste précédent, car autrement les deux nombres donnés sont premiers entre eux, contrairement à l'hypothèse. Euclide démontre alors, sans aucune difficulté, que ce reste est une mesure commune aux deux nombres donnés, et qu'elle est nécessairement la plus grande. La solution du problème posé par la proposition VII.3, la recherche de la plus grande mesure commune entre trois nombres donnés non premiers entre eux, suit enfin comme un simple corollaire de la proposition VII.2, puisqu'il est suffisant, pour parvenir au but, de considérer les trois nombres donnés deux à deux.

Après avoir été appliqué aux nombres, l'algorithme d'Euclide réapparaît, appliqué aux grandeurs, au tout début du livre X, dont les propositions X.2-X.5 font le pendant des propositions VII.1 - VII.3, car elles fournissent respectivement : un critère pour déterminer si deux grandeurs données sont ou non commensurables entre elles, et une procédure pour calculer le plus grand commun diviseur entre deux ou trois grandeurs commensurables plus grand commun diviseur !entre deux ou trois grandeurs commensurables entre elles.

La proposition X.2 nous dit en particulier que si deux grandeurs sont telles que les restes successifs qui dérivent de l'application à ces grandeurs de l'algorithme d'Euclide ne sont jamais tels qu'un de ces restes mesure le précédent, alors ces grandeurs sont incommensurables entre elles, c'est-à-dire qu'elles n'ont pas de mesure commune. Supposons que deux grandeurs, $a$ et $b$, par exemple deux segments, soient données et que $a$ soit plus grand que $b$. On retranche alors $b$ de $a$ autant de fois qu'il faut pour que le reste de cette soustraction, disons $r_1$, soit plus petit que $b$ lui-même. Si ce reste est nul, alors $b$ mesure $a$, et comme on peut penser $b$ comme le reste d'ordre zéro résultant de l'application aux grandeurs données de l'algorithme d'Euclide, il s'ensuit que les grandeurs $a$ et $b$ ne se comportent pas l'une par rapport à l'autre comme le veut l'hypothèse de la proposition. Imaginons alors que $r_1$ soit différent de zéro et retranchons-le, à son tour de $b$, autant de fois qu'il faut pour que le reste

de cette soustraction, disons $r_2$, soit plus petit que $r_1$. Si ce reste est nul, alors $r_1$ mesure $b$, contrairement à l'hypothèse. S'il n'est pas nul, retranchons-le de $r_1$, autant de fois qu'il faut pour que le reste de cette soustraction, disons $r_3$, soit plus petit que $r_2$. Si ce reste est nul, alors $r_2$ mesure $r_1$, contrairement à l'hypothèse. S'il n'est pas nul, retranchons-le de $r_2$, autant de fois qu'il faut pour que le reste de cette soustraction, disons $r_4$, soit plus petit que $r_3$. Et ainsi de suite. Comme, parmi les segments (non nuls), de même que parmi toutes sortes de grandeurs, il n'y en a pas un qui soit plus petit que tous les autres, il est clair qu'il n'y a aucune raison de principe qui puisse nous assurer que les deux segments donnés ne soient pas tels que cette procédure puisse continuer à l'infini, sans qu'on ne rencontre jamais de reste nul, et donc un reste qui mesure le précédent. Dans le chapitre 6, on verra même qu'il est assez facile de choisir deux segments qui vérifient cette possibilité. La proposition X.2 revient ainsi à affirmer que si les grandeurs données sont telles que cette procédure peut continuer à l'infini, sans qu'on ne rencontre jamais de reste nul, alors ces deux grandeurs sont incommensurables. Pour le prouver, Euclide admet (sans vraiment l'avoir prouvé) que les restes $r_i$ $(i = 1, 2, 3, \ldots)$ non seulement diminuent progressivement, mais qu'il est toujours possible, une grandeur quelconque étant fixée, d'en prendre un qui soit plus petit que cette grandeur. Il imagine alors que les deux grandeurs données sont commensurables, c'est-à-dire qu'elles admettent une mesure commune $c$, et il considère un reste $r_h$ plus petit que $c$. Si la procédure indiquée peut continuer à l'infini, sans qu'on rencontre jamais un reste nul, alors il y aura une infinité de nombres entiers, positifs « $n_i$ » $(i = 0, 1, 2, 3, \ldots)$ tels que

$$\begin{array}{rcl} a & = & n_0 b + r_1 \\ b & = & n_1 r_1 + r_2 \\ r_1 & = & n_2 r_2 + r_3 \\ & \ldots & \\ r_{h-1} & = & n_h r_h + r_{h+1} \\ & \ldots & \end{array}$$

les restes $r_i$ $(i = 1, 2, 3, \ldots)$ étant tels qu'on les a supposés ci-dessus. Et, il est clair que $c$, en mesurant $b$, mesure aussi $n_0 b$ et donc, en mesurant $a$, mesure aussi la différence $r_1$ de $a$ et $n_0 b$. Mais comme $c$ mesure $r_1$ et $b$, il mesure aussi $r_2$, et comme il mesure $r_1$ et $r_2$, il mesure aussi $r_3$, et ainsi de suite. Donc $c$ mesure $r_h$, bien qu'on vienne de supposer que $r_h$ est plus petit que $c$, ce qui est absurde. Donc il ne peut pas y avoir de mesure commune $c$ de $a$ et $b$, comme il s'agissait justement de démontrer.

On observe que, quelles que soient les grandeurs données $a$ et $b$, l'algorithme d'Euclide associe à ces grandeurs une suite de nombres entiers positifs $n_0, n_1, n_2, ...$ qui est finie si les grandeurs $a$ et $b$ sont commensurables entre elles, et infinie si elles ne sont pas commensurables. On peut imaginer donc que cette suite caractérise les relations entre $a$ et $b$ qui dépendent de la dimension respective de ces grandeurs. Comme les Grecs appelaient « antiphérèse » l'algorithme d'Euclide, certains commentateurs d'Aristote ont cru pouvoir lire dans un célèbre passage des *Topiques* [158b, 33-34], où Aristote dit que l'expression « avoir le même rapport » signifie « avoir la même antanarèse », une indication du fait qu'Aristote pensait pouvoir définir le rapport de deux grandeurs comme la succession de nombres entiers positifs $n_0, n_1, n_2, \ldots$ associée par l'algorithme d'Euclide à ces grandeurs. Après avoir lu les deux notes historiques 4.4 et 4.5, le lecteur n'aura pas de difficulté à comprendre la fascination que cette hypothèse a provoquée chez beaucoup d'historiens. Il reste le fait que, même si cette

hypothèse était exacte, Aristote ne nous aurait pas encore dit comment on peut opérer sur les rapports ainsi définis : il nous a peut être donné une définition du rapport entre deux grandeurs, mais non pas une arithmétique, même élémentaire, des rapports entre deux grandeurs.

**Lectures possibles** : J. Itard, *Les livres arithmétiques d'Euclide*, Hermann, Paris, 1961.

Le théorème 1.1 étant établi, il est naturel de penser que si deux nombres entiers strictement positifs $p$ et $q$ donnés sont tels qu'aucun des deux ne mesure l'autre, alors les deux égalités $p = ns$ et $q = ms$ qu'on peut sûrement déterminer ($n, m$ et $s$ étant des nombres entiers strictement positifs, et $s$ étant la mesure commune de $p$ et $q$) nous informent sur la relation qu'entretiennent les nombres $p$ et $q$, quant à la mesure. Ceci est la base de la théorie euclidienne des proportions entre nombres (entiers strictement positifs). Si on en reste à la mesure des nombres entiers strictement positifs, cette théorie est tout à fait satisfaisante. On peut pourtant avoir une visée plus large : celle de mesurer des objets autres que les nombres entiers strictement positifs. Cette exigence n'était nullement étrangère à Euclide qui cherchait en particulier à mesurer les grandeurs propres à sa géométrie. C'est à cette fin que, dans le livre V des *Éléments*, il reprend la théorie des proportions entre grandeurs quelconques, vraisemblablement due à Eudoxe de Cnide, mathématicien de l'école platonicienne. Malgré la puissance et l'élégance de cette théorie — qui n'emploie, outre les grandeurs à mesurer, rien d'autre que des nombres entiers positifs — l'évolution des mathématiques a conduit, à partir du XVII$^{e}$ siècle à l'abandonner. Nous n'exposerons pas ici la théorie d'Eudoxe, et montrerons tout de suite comment une stratégie différente (qui ne touchera au but qu'après la construction de l'ensemble des nombres réels, donnée au chapitre 6) peut fonctionner.

NOTE HISTORIQUE 4.3. La définition 21 du livre VII des *Éléments* d'Euclide est la suivante : « Des nombres sont en proportion quand le premier, du deuxième, et le troisième du quatrième, sont équimultiples, ou la même partie, ou les mêmes parties ». Pour rendre cette définition compréhensible au lecteur qui ne connaît pas la terminologie d'Euclide, il faudrait remonter tout au long des définitions du livre VII, au moins jusqu'à la définition 1.3. Pour éviter ce trop long détour, je traduirai d'emblée la définition précédente dans un langage plus accessible pour des lecteurs modernes : « On dit que les nombres entiers strictement positifs $a$ , $b$, $A$ et $B$ sont en proportion si parmi les mesures communes de $a$ et de $b$ il y en a (au moins) une qui mesure ces nombres selon les mêmes facteurs selon lesquels une des mesures communes de $A$ et de $B$ mesure ces autres nombres. Si on introduit le symbole moderne « $a : b = A : B$ » pour indiquer que les nombres $a$, $b$, $A$ et $B$ sont en proportion, on aura, en symboles, la traduction suivante :

$$[a : b = A : B] =_{df} \exists h \left[ \left( \begin{array}{c} a = nh \\ b = mh \end{array} \right) \Rightarrow \exists H \left( \begin{array}{c} A = nH \\ B = mH \end{array} \right) \right]$$

où $n$, $m$, $h$ et $H$ sont des nombres naturels strictement positifs.

C'est clair que la légitimité de cette définition dépend du fait que, quels que soient les nombres entiers strictement positifs $x$ et $y$, il existe, au sens d'Euclide, une mesure commune à $x$ et $y$, c'est-à-dire un nombre entier strictement positif $z$ tel que, pour quelques nombres entiers strictement positifs $n$ et $m$, on a $: x = nz$ et $y = mz$. En effet, si on imaginait que les nombres $a$ et $b$ sont tels qu'il n'y a pas de nombres entiers strictement positifs $h$, $n$, $m$, tels que $a = nh$ et $b = mh$, alors l'antécédent de l'implication qui entre dans le membre de droite de la définition précédente serait

certainement faux, et l'implication serait donc vraie (du fait de la table de vérité de l'implication ; le lecteur est invité pour cela à se reporter à un cours de logique élémentaire). Les nombres $a$ et $b$ seraient alors en proportion avec n'importe quels nombres $A$ et $B$, et la définition d'Euclide perdrait tout son sens.

Supposons maintenant que $a$ et $b$ soient deux nombres entiers strictement positifs quelconques. Ils auront au moins une mesure commune, et s'ils ont plus d'une mesure commune, ils n'auront, de toute façon, qu'un nombre fini de mesures communes. Soient $h_1$, $h_2$, ..., $h_k$ ($k$ étant un nombre entier strictement positif) ces mesures communes et soient à leur tour $n_1, n_2, \ldots, n_k$ et $m_1, m_2, \ldots, m_k$ les nombres entiers strictement positifs tels que

$$\begin{array}{lll} a = n_1 h_1 & \text{et} & b = m_1 h_1 \\ a = n_2 h_2 & \text{et} & b = m_2 h_2 \\ & \ldots & \\ a = n_k h_k & \text{et} & b = m_k h_k \end{array}$$

On aura alors qu'à considérer tous les couples $< n_i, m_i >$ ($i = 1, 2, \ldots, k$) et à vérifier, pour chacun de ces couples, l'existence d'un nombre entier positifs $H_i$ tel que

$$A = n_i H_i \qquad \text{et} \qquad B = m_i H_i$$

Si un tel nombre existe pour au moins un parmi les couples $< n_i, m_i >$ ($i = 1, 2, \ldots, k$), alors les nombres $a, b, A$ et $B$ seront en proportion, autrement ils ne le seront pas. La définition VII.21 d'Euclide admet donc une procédure finie de vérification, c'est-à-dire qu'il y a une procédure finie qui permet d'établir, pour chaque quadruplet $< a, b, A, B >$ de nombres entiers strictement positifs, si ces nombres sont ou non en proportion.

Imaginons maintenant que $a$, $b$, $A$ et $B$ ne soient pas des nombres entiers strictement positifs, mais des quantités d'une autre nature qui n'admettent pas forcément une mesure commune, par exemple des segments (dans le chapitre 6, on prouvera en effet que deux segments $\nu$ et $\mu$ quelconques n'admettent pas forcément une mesure commune, c'est-à-dire un segment $\zeta$ tel que, pour quelques nombres entiers strictement positifs $n$ et $m$, on ait : $\nu = n\zeta$ et $\mu = m\zeta$). Il est clair, d'après ce qu'on vient de dire, que la définition VII.21 ne permet pas de définir convenablement la proportionnalité entre ces quantités. Donc, ou bien on renonce à caractériser la relation à quatre places 'être en proportion', relativement à ces quantités, en se limitant à comparer celles-ci deux à deux, relativement à une relation d'ordre, ou bien on cherche une définition de proportionnalité essentiellement différente de la VII.21. C'est ainsi que, lorsque, dans le livre V des *Éléments*, Euclide veut donner une théorie des proportions applicable à des grandeurs (c'est-à-dire des quantités continues, telles que des segments, des polygones, des angles, etc.), il est obligé de se fonder sur une définition autre que la VII.21.

Voici, l'une après l'autre, les définitions 5 et 6 du livre V : « Des grandeurs sont dites *être dans le même rapport*, une première relativement à une deuxième et une troisième relativement à une quatrième quand les équimultiples de la première et de la troisième ou simultanément dépassent, ou sont simultanément égaux ou simultanément inférieurs à des équimultiples de la deuxième et de la quatrième, selon n'importe quelle multiplication, chacun à chacun, et pris de manière correspondante » ;

« Et que les grandeurs qui ont le même rapport soient dites *en proportion* ». En traduisant ces définitions dans un langage plus accessible et en les fusionnant l'une avec l'autre, on aura la définition suivante : On dit que les grandeurs $a$, $b$, $A$ et $B$ sont en proportion si, quels que soient les nombres entiers strictement positifs $n$, $m$ : si $na > nb$ alors $nA > nB$ ; si $na = nb$ alors $nA = nB$ ; et si $na < nb$ alors $nA < nB$. En symboles :

$$[a : b = A : B] =_{df} \left\{ (n, m \in \mathbb{N}^+) \Rightarrow \left[ \begin{array}{l} (na > mb) \Rightarrow (nA > mB) \\ (na = mb) \Rightarrow (nA = mB) \\ (na < mb) \Rightarrow (nA < mB) \end{array} \right] \right\}$$

Bien que cette définition puisse, à première vue, apparaître plus simple que la précédente, il n'est pas difficile de se rendre compte qu'elle n'admet pas une procédure finie et générale qui permette de décider si quatre grandeurs quelconques données $a$, $b$, $A$ et $B$ sont en proportion : s'il suffit de montrer que pour un certain couple de nombres entiers strictement positifs $n$ et $m$, une des implications qui constituent le conséquent du membre de droite de cette définition n'est pas vérifiée, pour en conclure que ces grandeurs ne sont pas en proportion, la considération de n'importe quel nombre de couples de nombres entiers strictement positifs $n$ et $m$ qui vérifient ces implications ne pourra suffire à conclure que ces grandeurs sont en proportion. La définition V.5 est donc essentiellement infinitaire. C'est la raison profonde d'innombrables discussions qui ont accompagné, des siècles durant, l'évolution de la théorie des proportions.

Qu'on remarque pourtant que cela ne signifie guère qu'on ne puisse jamais établir (par le biais d'une procédure finie) si quatre grandeurs particulières données, $a$, $b$, $A$ et $B$ sont ou pas en proportion. Pour que cela soit possible, il faut cependant que ces grandeurs aient entre elles des relations telles qu'il suffise que $na > mb$, $na = mb$, ou $na < mb$, $n$ et $m$ étant des nombres entiers strictement positifs, pour qu'on ait respectivement $nA > mB$, $nA = mB$, ou $na < mB$. Imaginons par exemple que $A$ et $B$ soient des côtés d'un triangle quelconque, que $b$ soit une corde de ce triangle parallèle à $B$ et $a$ la partie de $A$ retranchée par cette corde du côté de l'angle opposé à $B$. On aura alors deux triangles dont l'un est contenu dans l'autre, $a$ et $b$ seront deux côté du premier, et $A$ et $B$ seront les côtés respectivement homologues à ceux du second. Il serait alors aisé de montrer, par des moyens géométriques spécifiques à cette situation particulière, qu'en multipliant $a$ et $A$ par un un nombre entier positif $n$, et $b$ et $B$ pour un nombre entier positif $m$, on obtient quatre nouveaux segments $na$, $mb$, $nA$ et $mB$ tels que $na$ et $nA$ respectent les mêmes égalités et inégalités que $mb$ et $mB$. On en conclut alors que $a : b = A : B$. C'est le contenu d'un des théorèmes les plus fondamentaux de la géométrie euclidienne, le théorème dit de Thales qui constitue la proposition VI.2 des *Éléments*. Ce devrait pourtant être clair que la preuve de ce théorème ne tient pas à une procédure générale qu'on pourrait appliquer à n'importe quel quadruple de grandeurs pour décider si elles sont ou pas en proportion. Elle relève plutôt de la situation particulière dont il est question dans ce théorème.

De même que la théorie des proportions exposée dans le livre VII des *Éléments*, et en général toute l'arithmétique d'Euclide sont probablement dues à Thééthète, la théorie exposée dans le livre V est due à Eudoxe de Cnide. Même si formellement la définition VII.21 est une conséquence de la définition V.5, pourvu qu'on réfère cette dernière définition à des nombres entiers positifs, l'opposition de ces deux théories

est radicale et marque une séparation entre la théorie mathématique des nombres et celle des grandeurs, qui a marqué les mathématiques classiques à partir d'Euclide jusqu'au début du XVII$^{\text{ème}}$ siècle. Si on regarde les choses de près, on se rend compte pourtant que l'opposition entre les deux théories des proportions d'Euclide n'est qu'une conséquence d'un fait encore plus profond, qu'on a déjà observé dans la note historique 3.3 : si sur les nombres entiers positifs, il est possible de définir une multiplication interne (une opération de multiplication dont les deux facteurs sont des éléments d'un même ensemble, ici l'ensemble des nombres entiers positifs), ceci n'est pas possible sur les grandeurs, qui, dans le cadre des mathématiques classiques, n'admettent qu'une multiplication externe (une opération de multiplication dont les deux facteurs sont l'un, un élément d'un certain ensemble, ici une grandeur et l'autre un nombre entier positif). C'est ainsi que l'opposition entre théorie des nombres et théorie des grandeurs ne sera résorbée, comme on l'a observé dans la note historique 3.3, que lorsque Descartes parviendra, dans sa *Géométrie*, en 1637, à formuler un cadre théorique permettant de définir aussi sur les grandeurs une multiplication interne : c'est la première préfiguration de celle qui, deux siècles et demi plus tard, deviendra la théorie des nombres réels.

**Lectures possibles** : J.-L. Gardies, *L'héritage épistémologique d'Eudoxe de Cnide*, Vrin, Paris, 1988.

La première étape de notre stratégie consiste à évaluer la possibilité de formuler la théorie des proportions entre nombres entiers strictement positifs comme une théorie propre à une classe d'objets nouveaux qui constitue une extension de la classe des nombres entiers strictement positifs : de nouveaux « nombres » qui peuvent servir à mesurer des grandeurs (c'est-à-dire des quantités continues et donc autres que les nombres entiers strictement positifs), dont on suppose qu'elles possèdent une mesure commune.

REMARQUE 4.3. Bien qu'on n'ait pas jusqu'ici éclairci ce qu'on entend par quantité continue (on le fera, d'ailleurs assez rapidement, dans le chapitre 6), il est clair que, selon la convention terminologique qu'on vient d'introduire, toute grandeur est une quantité. D'autre part, on utilise ici le terme « quantité » comme on l'a fait dans le chapitre 3, pour nous référer aux éléments d'un ensemble sur lequel on a défini une addition associative et commutative. Naturellement (comme on l'a remarqué dans la note historique 4.1), cela n'implique pas que toute quantité ou plus précisément toute grandeur, est additionnable avec une autre grandeur, car deux grandeurs distinctes peuvent appartenir à deux ensembles distincts, sur lesquels on a séparément défini une addition associative et commutative. Par exemple, il est clair que si, en géométrie euclidienne, deux segments sont toujours additionnables entre eux, ceci n'est pas le cas d'un segment et d'un angle, bien qu'autant les segments que les angles soient, en géométrie euclidienne, des grandeurs. Cependant, il est certain, selon la définition précédente, que si $a$ est une grandeur, alors $a + a + \ldots + a$ est une grandeur, et que si $a$ et $b$ sont deux grandeurs qu'on peut additionner entre elles, alors

$$\begin{aligned}(a+b)+(a+b)+\ldots+(a+b) &= [(a+b)+a]+b+\ldots+a+b\\ &= [(a+a)+b]+b+\ldots+a+b\\ &= (a+a)+(b+b)+\ldots+a+b\\ &= (a+a+\ldots+a)+(b+b+\ldots+b)\end{aligned}$$

de sorte que si on utilise la notation multiplicative « $n\cdot x$ », où $n$ est un nombre entier positif et $x$ une grandeur, pour indiquer, comme ci-dessus, l'addition réitérée $\underbrace{x+x+...+x}_{n \text{ fois}}$, on

aura, pour tout nombre entier positif $n$,

$$n(a+b) = na + nb$$

et la multiplication entre grandeurs et nombres entiers positifs est donc distributive distributivité !de la multiplication !entre nombres entiers positifs sur l'addition entre grandeurs sur l'addition (entre grandeurs).

NOTE HISTORIQUE 4.4. Si la définition VII.21 des *Éléments* s'applique, sans aucune restriction, à n'importe quel quadruplet $< a, b, A, B >$ de nombres entiers strictement positifs, la définition V.5 des mêmes *Éléments* ne s'applique pas à n'importe quel quadruplet $< a, b, A, B >$ de grandeurs. Pour que cela ait un sens de dire que quatre grandeurs $a$, $b$, $A$ et $B$ sont ou ne sont pas en proportion d'après cette définition, il faut en effet qu'il soit possible de comparer entre eux, relativement à la relation d'ordre strict $<$, d'un côté, les produits $na$ et $mb$ et, de l'autre côté, les produits $nA$ et $mB$. Or, comme $n$ et $m$ sont des nombres entiers strictement positifs, ces produits ne sont, à leur tour, que des grandeurs de même nature que les grandeurs $a$, $b$, $A$ et $B$. Ils sont donc comparables entre eux, relativement à la relation d'ordre strict $<$ si et seulement si les grandeurs $a$, $b$, $A$ et $B$ le sont. La définition V.5 des Éléments ne s'applique donc à quatre grandeurs quelconques $a$, $b$, $A$ et $B$ qu'à condition que ces grandeurs soient comparables entre elles deux à deux, relativement à la relation d'ordre strict $<$, la première avec la deuxième et la troisième avec la quatrième.

Or, si on accepte l'idée, propre aux mathématiques classiques, d'après laquelle la notion de grandeur, et, plus généralement, celle de quantité, ne sont pas définies de manière abstraite, en qualifiant de grandeur ou de quantité tout objet qui satisfait à certaines conditions formelles, mais se réfèrent plutôt à des domaines d'objets déjà constitués, qui sont définis séparément les uns des autres (même si pas nécessairement de manière indépendante, car, pour ne prendre qu'un exemple, la définition du domaine des polygones n'est pas indépendante de celle du domaine des segments), en définissant pour chacun de ces domaines, une relation d'égalité, une relation d'ordre strict et (au moins) une loi de composition interne (généralement une addition), il s'ensuit, comme on l'a déjà observé dans la note historique 4.1, que dire de deux objets $\nu$ et $\mu$ qu'ils sont des grandeurs, ou plus en général des quantités, n'est pas la même chose que de dire que ces objets sont comparables entre eux relativement à une relation d'ordre strict. Il est en effet possible que ces objets appartiennent à de domaines de quantités séparés et qu'on ne dispose donc d'aucune relation d'ordre strict qui s'applique aux deux en même temps.

Toutes les fois qu'en mathématiques classiques on voulait comparer des grandeurs, ou plus généralement des quantités, relativement à une relation d'ordre, ou même les additionner ou les égaliser, il fallait s'assurer qu'elles appartenaient au même domaine de grandeurs, ou, plus généralement, de quantités. C'est un problème que les historiens des mathématiques connaissent bien, celui de l'homogénéité (deux quantités appartenant au même domaine de quantités étant généralement dites « homogènes » ).

L'exemple de la relation de proportionnalité entre quatre grandeurs illustre ce problème : pour que cela ait un sens de déclarer quatre grandeurs $a$, $b$, $A$ et $B$ en proportion (ou non en proportion) entre elles, en accord avec la définition V.5, il faut s'assurer d'abord que ces grandeurs sont homogènes deux à deux. Rien pourtant n'oblige à ce que ces grandeurs soient toutes homogènes entre elles, les grandeurs $a$ et $b$ pouvant bien être non homogènes avec les grandeurs $A$ et $B$. Comme, d'un point de vue formel, la définition V.5 s'applique à toutes sortes de quantités, homogènes

deux à deux, si $a$ et $b$ sont des grandeurs homogènes, on peut même appliquer cette définition pour affirmer que ces grandeurs sont (ou ne sont pas) en proportion avec deux nombres entiers strictement positifs quelconques. On pourra dire par exemple que les segments $a$ et $b$ et les nombres 1 et 2 sont en proportion, ou, plus simplement (et cette plus grande simplicité linguistique explique en partie le dédoublement de la définition euclidienne de proportionnalité entre grandeurs, qui occupe à la rigueur, comme on l'a vu, les définitions V.5 et V.6 des *Éléments*) que $a$ et $b$ sont dans le même rapport que 1 et 2, c'est-à-dire que $b$ est le double de $a$.

On dit souvent que le problème de l'homogénéité ne se présente plus dans les mathématiques modernes. Il faut pourtant bien comprendre le sens dans lequel cette affirmation doit être interprétée. Lorsqu'on dit que dans les mathématiques modernes, le problème de l'homogénéité n'a plus lieu de subsister, on ne veut pas affirmer que les mathématiciens modernes savent comparer ou additionner entre elles des grandeurs de toutes sortes. Ce qu'on veut dire est plutôt qu'ils travaillent, explicitement ou implicitement, à l'intérieur de certaines structures qui, par définition, sont telles que leurs éléments sont tous comparables et composables entre eux. Dans le chapitre 5, on définira certaines de ces structures et on parviendra, en particulier, à définir la structure de corps commutatif totalement ordonné , en reconnaissant cette structure comme le contexte où, pour ainsi dire, les opérations algébriques subissent le moins de restrictions. Dans le chapitre 6, on montrera ensuite que les segments, ainsi que toutes sortes de grandeurs propres aux mathématiques classiques, peuvent être traités comme (ou du moins représentés par) des nombres réels, et on comprendra que l'ensemble des nombres réels est un corps commutatif totalement ordonné. Lorsque les mathématiciens modernes semblent, par exemple, additionner un segment et un carré, ou comparer un angle avec un arc de cercle ou un segment, ils sont en fait en train d'additionner ou de comparer des nombres réels.

**Lectures possibles** : B. Vitrac, « Introduction », *in* Euclide, *Les Éléments*, vol. 2 (livre V à IX), PUF, Paris, 1994, pp. 13-32.

On imagine avoir affaire à une certaine classe $\mathfrak{A}$ de grandeurs, disons des segments, qu'on suppose être telle que, quel que soit le couple $a$ et $b$ de grandeurs de cette classe, alors $a$ et $b$ possèdent une mesure commune sous la forme d'une grandeur de la même espèce, dans notre cas un segment. Dit en d'autres termes : on imagine travailler sur une sous-classe $\mathfrak{A}$ de la classe des segments, telle que si $a$ et $b$ sont deux éléments de $\mathfrak{A}$, alors il y a un autre élément $c$ de $\mathfrak{A}$ et deux nombres entiers strictement positifs $n$ et $m$, tels que $a = nc$ et $b = mc$. Il s'agit de savoir si pour tout couple $a$ et $b$ de grandeurs de $\mathfrak{A}$, tels que $a \leq b$, on peut donner un sens à l'écriture « $b = \mathfrak{q}a$ », $\mathfrak{q}$ étant un objet qui se comporte comme les nombres entiers strictement positifs (c'est-à-dire qu'il appartient à une classe d'objets qui admet une addition, une multiplication et une relation d'ordre qui satisfont aux mêmes conditions que l'addition, la multiplication et la relation d'ordre entre nombres entiers strictement positifs) et peut être défini à partir de ces nombres, de telle sorte que la seule écriture « $b = \mathfrak{q}a$ » nous donne, pour ainsi dire, la même information que les deux écritures « $a = nc$ » et « $b = mc$ ». Voici comment on raisonne.

Soit $\gamma$ une grandeur quelconque (qu'on imagine non nulle) de la classe considérée, disons donc un segment. On note par le symbole « $\frac{1}{m}\gamma$ » le segment qui mesure $\gamma$ selon le facteur $m$, c'est-à-dire le segment qui entre exactement $m$ fois en $\gamma$ ($m$ étant un nombre entier strictement positif) ; on note d'autre part par le symbole « $\frac{n}{m}\gamma$ » le segment qui résulte en additionnant $\frac{1}{m}\gamma$ à lui-même $n$ fois ($n$ étant un nombre entier strictement positif) ; on note enfin l'addition réitérée $\underbrace{a + a + ... + a}_{s \text{ fois}}$ ($s$ étant un nombre entier strictement positif et $a$ une grandeur) par le

symbole multiplicatif « $s \cdot a$ ». De ces conventions on tire les égalités suivantes :

$$m \cdot \frac{1}{m}\gamma = \gamma \tag{23}$$

$$n \cdot \frac{1}{m}\gamma = \frac{n}{m}\gamma \tag{24}$$

En partant de la deuxième de ces égalités, il sera facile de démontrer que, pour tout triplet de nombres entiers strictement positifs $n, m$ et $p$,

$$\frac{n}{m}\gamma + \frac{p}{m}\gamma = \frac{n+p}{m}\gamma \tag{25}$$

En fait, conformément à (24), on aura

$$\frac{n}{m}\gamma + \frac{p}{m}\gamma = n \cdot \frac{1}{m}\gamma + p \cdot \frac{1}{m}\gamma$$

mais, comme pour tout nombre entier strictement positif $s$, « $s \cdot \frac{1}{m}\gamma$ » n'est qu'une notation pour une addition entre segments, de là il suit

$$\frac{n}{m}\gamma + \frac{p}{m}\gamma = (n+p) \cdot \frac{1}{m}\gamma$$

d'où (25) dérive encore en vertu de (24).

On cherche maintenant à comprendre quel doit être le résultat de l'addition de deux segments $\frac{p}{m}\gamma$ et $\frac{q}{n}\gamma$, les nombres entiers strictement positifs $m$ et $n$ étant différents. En vertu de (24) on aura

$$\frac{p}{m}\gamma + \frac{q}{n}\gamma = p \cdot \frac{1}{m}\gamma + q \cdot \frac{1}{n}\gamma$$

Supposons d'abord que l'un des deux nombres entiers strictement positifs $m$ et $n$ mesure l'autre. En imaginant que $m > n$, on pourra alors poser l'égalité $m = kn$, $k$ étant un nombre entier strictement positif. Or, conformément à (23), on aura

$$m \cdot \frac{1}{m}\gamma = n \cdot \frac{1}{n}\gamma$$

et puisque $m = kn = nk$ :

$$nk \cdot \frac{1}{m}\gamma = n \cdot \frac{1}{n}\gamma \tag{26}$$

Mais, conformément à la définition ci-dessus de la multiplication entre un nombre entier strictement positif et une grandeur quelconque, il est facile de prouver que pour toute grandeur $a$ et pour tout couple de nombres entiers strictement positifs $s$ et $t$, $(s \cdot t) \cdot a = s \cdot (t \cdot a)$ . D'autre part, si $a$ et $b$ sont des segments et $n$ un nombre entier strictement positif, il est facile de prouver que si $n \cdot a = n \cdot b$, alors $a = b$. En effet, si $a \neq b$, et on imagine que $a < b$, alors, il y aura un segment $c$, tel que $b = a + c$. De l'hypothèse $n \cdot a = n \cdot b$ il suit alors $n \cdot a = n \cdot (a + c) = (n \cdot a) + (n \cdot c)$. Mais, comme cette égalité ne dépend pas de la nature particulière du segment $a$, il s'ensuit que le segment $n \cdot c$ doit être tel que, pour tout segment $x$, $x + (n \cdot c) = x$, c'est-à-dire que, selon la terminologie qu'on introduira explicitement dans le chapitre 5, $n \cdot c$ est un élément neutre de l'addition élément !neutre !de l'addition parmi les segments. Mais $x + (n \cdot c) = x + \underbrace{c + c + ... + c}_{n \text{ fois}}$, donc $c$ aussi est un élément neutre de l'addition parmi les segments, et donc $b = a + c = a$. De l'hypothèse que $b$ soit différent de $a$, il suit alors que $b$ est égal à $a$, donc, selon la tautologie $(\neg A \Rightarrow A) \Rightarrow A$, $b$ est égal à $a$, comme on voulait le démontrer.

De (26) on tire, donc :

$$k \cdot \frac{1}{m}\gamma = \frac{1}{n}\gamma$$

c'est-à-dire :

$$\frac{p}{m}\gamma + \frac{q}{n}\gamma = p \cdot \frac{1}{m}\gamma + q \cdot \left(k \cdot \frac{1}{m}\gamma\right)$$

et donc, encore grâce à l'égalité $(s \cdot t) \cdot a = s \cdot (t \cdot a)$,

$$\frac{p}{m}\gamma + \frac{q}{n}\gamma = p \cdot \frac{1}{m}\gamma + qk \cdot \frac{1}{m}\gamma = \frac{p+qk}{m}\gamma$$

Pour généraliser ce résultat, imaginons maintenant qu'aucun des nombres entiers strictement positifs $m$ et $n$ ne mesure l'autre. Il suffit de poser $h = mn$ et de raisonner comme tout à l'heure pour tirer les égalités

$$\begin{aligned} \frac{1}{n}\gamma &= m \cdot \frac{1}{h}\gamma \\ \frac{1}{m}\gamma &= n \cdot \frac{1}{h}\gamma \end{aligned}$$

d'où il suit sans difficulté que :

$$\begin{aligned} \frac{p}{m}\gamma + \frac{q}{n}\gamma &= p \cdot \left(n \cdot \frac{1}{h}\gamma\right) + q \cdot \left(m \cdot \frac{1}{h}\gamma\right) \\ &= pn \cdot \frac{1}{h}\gamma + qm \cdot \frac{1}{h}\gamma \\ &= \frac{pn+qm}{h}\gamma \end{aligned}$$

On a alors démontré que pour tout quadruplet de nombres entiers strictement positifs $n, m, p, q$ on a :

$$\frac{p}{m}\gamma + \frac{q}{n}\gamma = \frac{pn+qm}{mn}\gamma \tag{27}$$

Dans l'argument précédent, on a, en passant, démontré que pour tout triplet de nombres entiers strictement positifs $n, m, p$, on a :

$$p \cdot \frac{n}{m}\gamma = \frac{pn}{m}\gamma$$

car $p \cdot \frac{n}{m}\gamma = p \cdot \left(n \cdot \frac{1}{m}\gamma\right) = pn \cdot \frac{1}{m}\gamma = \frac{pn}{m}\gamma$. Il s'agit maintenant de comprendre ce qu'on peut entendre par une multiplication telle que $\left(\frac{p}{m}\gamma\right)$ et $\left(\frac{q}{n}\gamma\right)$ entre deux segments.

Imaginons d'abord que les nombres entiers strictement positifs $p$ et $m$ soient tels que l'un d'eux mesure l'autre. En supposant que $m \leq p$, on pourra alors conclure qu'il y a un nombre entier strictement positif $k$ tel que $p = km$. De là il suivra alors que $\frac{1}{m}\gamma = k \cdot \frac{1}{p}\gamma$, et donc :

$$\begin{aligned} \left(\frac{p}{m}\gamma\right) &= \left(p \cdot \frac{1}{m}\gamma\right) = \left[p \cdot \left(k \cdot \frac{1}{p}\gamma\right)\right] \\ &= pk \cdot \frac{1}{p}\gamma = kp \cdot \frac{1}{p}\gamma = k \cdot \left(p \cdot \frac{1}{p}\gamma\right) = k \cdot \gamma \end{aligned}$$

Il sera alors facile de tirer, quels que soient les nombres entiers strictement positifs $p, q, k, m$ et $n$ :

$$\left(\frac{p}{m}\gamma\right) \cdot \left(\frac{q}{n}\gamma\right) = (k \cdot \gamma) \cdot \left(\frac{q}{n}\gamma\right)$$

Pourtant, ceci ne résout pas encore la question, car on ne sait toujours pas ce que signifie une multiplication entre deux segments tels que $k \cdot \gamma$ et $\frac{q}{n}\gamma$. À ce point, il faut raisonner par analogie.

Si $a, b, c$ et $d$ sont quatre segments quelconques, tels que $a = nc$ et $b = md$ ($m$ et $n$ étant deux nombres entiers strictement positifs), alors le rectangle construit sur les segments $a$ et $b$ contient $n \cdot m$ rectangles égaux, tous correspondants au rectangle construit sur $c$ et $d$. On peut alors imaginer que la multiplication de deux segments de la classe $\mathfrak{A}$ est analogue à la construction d'un rectangle dont ces segments sont les côtés. Cela signifie que cette multiplication a comme résultat un objet différent des objets de départ. En supposant que ce soit le cas pour toutes les grandeurs additionnables, on peut poser les conventions suivantes :

$$\begin{array}{rcl} \gamma \cdot \gamma & = & \gamma^2 \\ \left(p \cdot \frac{1}{n}\gamma\right) \cdot \left(q \cdot \frac{1}{n}\gamma\right) & = & pq \cdot \frac{1}{n^2}\gamma^2 \end{array} \tag{28}$$

$n, p$ et $q$ étant des nombres entiers strictement positifs quelconques et $\gamma^2$ un carré de côté $\gamma$, ou, plus généralement, un objet appartenant à une classe d'objets, autre que celle à laquelle appartient $\gamma$, qui se comporte relativement aux autres objets de la classe à laquelle il appartient comme $\gamma$ se comporte face aux autres objets de la classe $\mathfrak{A}$ (en effet, quel que soit le nombre naturel $s$, le carré construit sur la $s$-ième partie d'un segment est la $s^2$-ième partie du carré construit sur ce même segment).

Cela permet de résoudre en général le problème posé, c'est-à-dire indépendamment de la position $p = km$. En fait, si on pose, comme tout à l'heure, $h = mn$, on peut conclure, en exploitant les égalités déjà démontrées,

$$\begin{array}{rcl} \left(\frac{p}{m}\gamma\right) \cdot \left(\frac{q}{n}\gamma\right) & = & \left(pn \cdot \frac{1}{h}\gamma\right) \cdot \left(qm \cdot \frac{1}{h}\gamma\right) \\ & = & (pn \cdot qm) \cdot \frac{1}{h^2}\gamma^2 \\ & = & \frac{pn \cdot qm}{mn \cdot mn}\gamma^2 \end{array}$$

et donc :

$$\left(\frac{p}{m}\gamma\right) \cdot \left(\frac{q}{n}\gamma\right) = \frac{mn \cdot pq}{mn \cdot mn}\gamma^2$$

Jusqu'ici les termes de la forme « $\frac{p}{m}\gamma$ » ou « $\frac{p}{m}\gamma^2$ », $p$ et $m$ étant des nombres entiers strictement positifs, ne sont entrés que dans des égalités où le membre de gauche exprime une opération d'addition ou de multiplication entre deux termes de la forme « $\frac{p}{m}\gamma$ », ou entre un terme de cette même forme et un nombre entier strictement positif, tandis que le terme de droite exprime le résultat de ces opérations par le biais d'un terme de la forme « $\frac{p}{m}\gamma$ », ou de la forme « $\frac{p}{m}\gamma^2$ ». On n'a pourtant pas raisonné sur la signification possible d'égalités telles que

$$\frac{p}{m}\gamma = \frac{q}{n}\gamma \qquad \text{et} \qquad \frac{p}{m}\gamma^2 = \frac{q}{n}\gamma^2$$

où $p, q, m$ et $n$ sont des nombres entiers strictement positifs. Pour comprendre ce que ces égalités peuvent signifier, il suffit pourtant d'observer que les termes « $\frac{p}{m}\gamma$ » et « $\frac{q}{n}\gamma$ » et les termes « $\frac{p}{m}\gamma^2$ » et « $\frac{q}{n}\gamma^2$ » ne désignent que des grandeurs respectivement de la même nature que $\gamma$ et $\gamma^2$. En particulier, si $\chi$ est une grandeur, soit de la nature de $\gamma$, soit de la nature de $\gamma^2$, un terme tel que « $\frac{s}{t}\chi$ » (où $s$ et $t$ sont des nombres entiers strictement positifs) indique le résultat de l'addition $\underbrace{\frac{1}{t}\chi + \frac{1}{t}\chi + ... + \frac{1}{t}\chi}_{s \text{ fois}}$, où $\frac{1}{t}\chi$ est la $t$-ième partie de $\chi$. Ainsi une égalité telle que

$$\frac{p}{m}\chi = \frac{q}{n}\chi$$

ne saurait être satisfaite qu'à condition que la grandeur indiquée par le terme « $\frac{p}{m}\chi$ » soit égale (selon la relation d'égalité qui est propre aux grandeurs de la nature de $\chi$) à la grandeur indiquée par le terme « $\frac{q}{n}\chi$ » et *vice versa*. Des considérations analogues s'appliquent aussi à des égalités telles que

$$p \cdot \chi = \frac{q}{n}\chi$$

car $p \cdot \chi$ est aussi une grandeur de même nature que $\chi$.

Cela nous convainc de la légitimité de deux suppositions telles que les suivantes, qui, comme on le comprendra par la suite, sont compatibles avec les suppositions précédentes :

$$\begin{aligned} \frac{p}{m}\chi &= \frac{q}{n}\chi \qquad \text{si et seulement si} \qquad s \cdot \frac{p}{m}\chi = s \cdot \frac{q}{n}\chi \\ p\chi &= \frac{q}{n}\chi \qquad \text{si et seulement si} \qquad s \cdot p\chi = s \cdot \frac{q}{n}\chi \end{aligned}$$

où $s, p, m, q$, et $n$ sont des nombres entiers strictement positifs quelconques et le symbole « $\chi$ » indique soit $\gamma$, soit $\gamma^2$.

Arrivé à ce point, il suffit d'observer que le segment $\gamma$ et le carré $\gamma^2$ interviennent dans les déductions précédentes comme des facteurs invariables, qui ne dépendent que d'un choix initial qui n'a aucune influence sur le succès des déductions. On peut donc éliminer ces facteurs et définir ainsi les nombres fractionnaires strictement positifs et les opérations d'addition et de multiplication portant sur ces nombres :

Définition 1.1. *On appelle « nombre fractionnaire strictement positif », un couple ordonné de nombres entiers strictement positifs quelconques $p$ et $m$, qu'on note « $\frac{p}{m}$ ».*

Définition 1.2. *On appelle « addition sur les nombres fractionnaires strictement positifs », l'opération, notée « $+$ », qui conduit des nombres fractionnaires strictement positifs $\frac{p}{m}$ et $\frac{q}{n}$ au nombre fractionnaire strictement positif $\frac{pn+qm}{mn}$, qu'on appelle « somme » des deux nombres fractionnaires strictement positifs donnés.*

Définition 1.3. *On appelle « multiplication sur les nombres fractionnaires strictement positifs », l'opération, notée « $\cdot$ » (ou simplement, s'il n'y a pas risque d'ambiguïté, par une juxtaposition), qui conduit des nombres fractionnaires strictement positifs $\frac{p}{m}$ et $\frac{q}{n}$, au nombre fractionnaire strictement positif $\frac{mn \cdot pq}{mn \cdot mn}$, qu'on appelle « produit » des deux nombres fractionnaires positifs donnés.*

Outre ces définitions, les axiomes suivants sont nécessaires pour régler les relations multiplicatives entre nombres fractionnaires strictement positifs et nombres entiers strictement positifs, et introduire la relation d'égalité entre nombres fractionnaires strictement positifs.

Si $s, p, m, q$ et $n$ sont des nombres entiers strictement positifs quelconques, alors :

Axiome 1.

$$\frac{pq}{m} = pq \cdot \frac{1}{m} = p \cdot \frac{q}{m}$$

Axiome 2.

$$m \cdot \frac{1}{m} = 1$$

Axiome 3.

$$\begin{aligned} i)\ \left(\frac{p}{m} = \frac{q}{n}\right) &\Leftrightarrow \left(s \cdot \frac{p}{m} = s \cdot \frac{q}{n}\right) \\ ii)\ \left(p = \frac{q}{n}\right) &\Leftrightarrow \left(s \cdot p = s \cdot \frac{q}{n}\right) \end{aligned}$$

Remarque 4.4. Il devrait apparaître clairement, de la manière dont on y est parvenu, que les définitions 1.1-1.3 et les axiomes 1-3 expriment des propriétés de l'opération de partager un segment (non nul), ou plus généralement une grandeur (non nulle), en un nombre quelconque de parties égales, et des segments (ou grandeurs) qui résultent de cette opération. Ces propriétés ont été ci-dessus tirées, par déduction et, dans un cas, par analogie, des propriétés des segments (ou grandeurs) et des nombres entiers strictement positifs. L'idée sous-jacente à ces définitions et axiomes est de définir une classe d'objets qui se comportent entre eux comme se comportent entre eux les résultats de cette opération. Or, si deux segments (ou grandeurs) $\gamma$ et $\delta$ possèdent une mesure commune, on peut toujours prendre un de ces segments (ou une de ces grandeurs), disons $\gamma$, comme le segment (ou la grandeur) de départ, et exprimer l'autre comme le résultat d'une addition réitérée (ou multiplication) de la mesure commune, de sorte qu'il y aura toujours un nombre fractionnaire strictement positif $\frac{p}{q}$ tel que

$$\delta = \frac{p}{q}\gamma$$

$\frac{1}{q}\gamma$ étant justement la mesure commune de $\gamma$ et $\delta$. Si l'on définit les nombres fractionnaires strictement positifs comme ci-dessus, et $a$ et $b$ sont des grandeurs qui possèdent une mesure commune, alors l'écriture « $a = \mathfrak{q}b$ » a toujours un sens, pourvu que $\mathfrak{q}$ soit justement un nombre fractionnaire strictement positif. La définition précédente résout ainsi le problème qu'on s'était posé au départ.

On observe pourtant que cette définition ne consiste pas uniquement dans la définition 1.1. Cette seule définition, indépendamment des deux définitions qui la suivent et des axiomes successifs, est vide, en se réduisant à une pure convention terminologique et notationnelle. À bien regarder les choses de près, ceci est pourtant aussi le cas de la définition des nombres entiers positifs donnée dans le chapitre 1. Si l'on fait abstraction des clauses opérationnelles qui fixent les opérations légitimes sur les collections de traits verticaux prises comme nombres entiers positifs, la définition 1.5 est également vide. Bien que ces deux définitions doivent ainsi se qualifier de constructives et explicites, elles ne peuvent pas être prises indépendamment d'un cadre opérationnel qui est fixé, soit explicitement par d'autres définitions corrélées à celles-ci, soit implicitement. Bien que les mathématiques emploient souvent, comme toute autre discipline rigoureuse, des définitions purement terminologiques ou notationnelles, pour introduire des termes ou symboles qui sont, à la suite de ces définitions, employés comme des abréviations d'autres termes ou symboles, elles ne peuvent pas se limiter à des définitions de ce type. Si on appelle « proprement mathématiques » les définitions non purement terminologiques ou notationnelles qui interviennent dans une théorie mathématique, alors la caractéristique qu'on vient d'observer pour les définitions des nombres entiers positifs et des nombres fractionnaires strictement positifs est commune aux définitions proprement mathématiques : elles ne sauraient se réduire à de simples propositions de la forme « on appelle « $x$ » ceci ou cela ». Elles sont plutôt le résultat d'un réseau de définitions de cette sorte qui participent ensemble à spécifier le « ceci ou cela » et à le caractériser comme un pôle d'une structure opérationnelle.

Ceci étant dit, revenons plus spécifiquement aux définitions 1.1-1.3 et aux axiomes 1-3. Il est certain (et peut être aisément démontré, en se réclamant du théorème 1.1) que, quelles que soient les mesures $\frac{1}{q}\gamma$ et $\frac{1}{n}\gamma$ d'un segment (ou d'une grandeur) quelconque $\gamma$, ces mesures possèdent, à leur tour, une mesure commune. Cependant, cela ne signifie guère que toutes les mesures d'un segment (ou d'une grandeur) $\gamma$ donné(e) possèdent une mesure

commune, c'est-à-dire qu'il existe une mesure de $\gamma$ qui soit en même temps une mesure commune à toutes les mesures de $\gamma$. Cela distingue les parties exactes d'une grandeur (ou mesures de cette grandeur), et donc les nombres fractionnaires strictement positifs, des nombres entiers strictement positifs (ou, même, tout simplement positifs). Il est en fait aisé de montrer que ces derniers ne sont pas seulement tels qu'ils satisfont au théorème 1.1, mais qu'ils sont aussi tels qu'il existe un nombre entier strictement positif (naturellement 1) qui est la mesure commune de tous les nombres entiers strictement positifs, (ou, même, tout simplement positifs). Cela dépend du fait qu'il existe un nombre entier strictement positif qui est le plus petit des nombres entiers strictement positifs, et que l'ensemble des nombres entiers strictement positifs plus petits que n'importe quel nombre entier strictement positif est fini (et que tout nombre entier positif est une mesure de 0). Comme on le verra, si on définit sur les nombres fractionnaires strictement positifs une relation d'ordre compatible avec la relation $\leq$ définie sur les nombres entiers positifs, cela n'est en revanche pas le cas des nombres fractionnaires strictement positifs. De là, il s'ensuit qu'il n'y a aucun nombre fractionnaire strictement positif qui soit la mesure commune de tous les nombres fractionnaires strictements positifs. On verra plus tard que cela n'est qu'un aspect de la propriété dite de « densité (relativement à $\leq$) » de l'ensemble de ces nombres, et, en partant de cela, on introduira de nouvelles réflexions connectées avec cette différence entre nombres entiers (strictement) positifs et nombres fractionnaires strictement positifs. Pour l'instant, on en reste à cette simple observation.

## 2. Nombres fractionnaires strictement positifs et division

Les considérations précédentes ne font aucune référence explicite à la relation entre les nombres fractionnaires strictement positifs et la division entre nombres entiers strictement positifs. Dans le chapitre 1, on a défini la division entre nombres entiers positifs comme l'opération inverse de la multiplication, et on a vu que la classe des nombres entiers positifs est ouverte par rapport à la division. On montrera ici qu'un nombre fractionnaire strictement positif quelconque $\frac{p}{q}$ peut être pris comme le résultat de la division du nombre entier strictement positif $p$ par le nombre entier strictement positif $q$. On définira ensuite la division sur les nombres fractionnaires strictement positifs et on montrera que la classe de ces nombres est fermée par rapport à cette opération.

Donnons d'abord le théorème suivant :

THÉORÈME 2.1. *Si $\frac{p}{q}$ est un nombre fractionnaire strictement positif, alors*

$$p = q \cdot \frac{p}{q}$$

*et le nombre $\frac{p}{q}$ peut donc être pris comme le résultat de la division du nombre entier positif $p$ par le nombre entier positif $q$.*

**Preuve** Suivant les axiomes 1 et 2, on aura :

$$\begin{aligned} q \cdot \frac{p}{q} &= \frac{qp}{q} = qp \cdot \frac{1}{q} \\ &= pq \cdot \frac{1}{q} = p \cdot \left( q \cdot \frac{1}{q} \right) \\ &= p \cdot 1 = p \end{aligned}$$

□

Une conséquence de ce théorème est la règle bien connue de simplification des nombres fractionnaires strictement positifs. Elle est énoncée par le théorème suivant :

THÉORÈME 2.2. *Si* $\frac{p}{q}$ *et* $\frac{n}{m}$ *sont deux nombres fractionnaires strictement positifs quelconques, alors*

$$\frac{p}{q} = \frac{n}{m} \quad \textit{si et seulement si} \quad pm = nq$$

**Preuve** Si $\frac{p}{q} = \frac{n}{m}$, alors, selon l'axiome 3($i$),

$$q \cdot \frac{p}{q} = q \cdot \frac{n}{m}$$

et donc, suivant le théorème 2.1 et l'axiome 1,

$$p = q \cdot \frac{n}{m} = \frac{qn}{m}$$

Ainsi, selon les axiomes 1, 2 et 3($ii$),

$$\begin{aligned} pm &= mp = m \cdot \frac{qn}{m} \\ &= qn \cdot m \cdot \frac{1}{m} = qn = nq \end{aligned}$$

D'autre part, suivant l'axiome 2, $m \cdot \frac{1}{m} = 1 = q \cdot \frac{1}{q}$ , donc, selon l'axiome 3($i$),

$$npm \cdot \frac{1}{m} = npq \cdot \frac{1}{q} = nq \cdot p \cdot \frac{1}{q}$$

Mais, si $pm = nq$, alors

$$npm \cdot \frac{1}{m} = nnq \cdot \frac{1}{m} = nq \cdot n \cdot \frac{1}{m}$$

et donc, en comparant,

$$nq \cdot \left( n \cdot \frac{1}{m} \right) = nq \cdot \left( p \cdot \frac{1}{q} \right)$$

et, d'ici, selon l'axiome 3($i$),

$$n \cdot \frac{1}{m} = p \cdot \frac{1}{q}$$

et, selon l'axiome 1,

$$n \cdot \frac{1}{m} = \frac{n}{m} = p \cdot \frac{1}{q} = \frac{p}{q}$$

ce qui clôt la démonstration. □

Or, comme, pour tout triplet $n$, $m$ et $p$ de nombres entiers strictement positifs, $(pn)m = n(pm)$, du théorème 2.2, il s'ensuit que pour tout triplet $n$, $m$ et $p$ de nombres entiers strictement positifs :

$$\frac{pn}{pm} = \frac{n}{m} \tag{29}$$

La définition 1.3 revient donc à poser que si $\frac{p}{m}$ et $\frac{q}{n}$ sont deux nombres fractionnaires strictement positifs quelconques, alors :

$$\frac{p}{m} \cdot \frac{q}{n} = \frac{pq}{mn} \tag{30}$$

(ce qui est une égalité bien connue).

Voici, maintenant, la plus naturelle des définitions de la division sur les nombres fractionnaires strictement positifs :

Définition 2.1. *On appelle « division sur les nombres fractionnaires strictement positifs », l'opération, notée « : », qui conduit des nombres fractionnaires strictement positifs $\frac{p}{m}$ et $\frac{q}{n}$ au nombre fractionnaire strictement positif $\frac{h}{k}$ (qu'on appelle « quotient », des nombres donnés), si et seulement si $\frac{h}{k} \cdot \frac{q}{n} = \frac{p}{m}$.*

De cette définition, il suit le théorème suivant :

Théorème 2.3. *La classe des nombres fractionnaires strictement positifs est fermée par rapport à la division, et si $\frac{p}{m}$ et $\frac{q}{n}$ sont deux nombres fractionnaires strictement positifs quelconques, alors $\frac{p}{m} : \frac{q}{n} = \frac{pn}{mq}$*

**Preuve** Si $\frac{p}{m}$ et $\frac{q}{n}$ sont deux nombres fractionnaires strictement positifs, alors $p$, $m$, $q$ et $n$ sont des nombres entiers strictement positifs, donc $\frac{pn}{mq}$ est un nombre fractionnaire strictement positif. Mais de (29) et (30), que

$$\frac{pn}{mq} \cdot \frac{q}{n} = \frac{pnq}{mqn} = \frac{(nq)p}{(nq)m} = \frac{p}{m}$$

et donc $\frac{pn}{mq}$ est le quotient de $\frac{p}{m}$ et $\frac{q}{n}$, et ce quotient est un nombre fractionnaire strictement positif. □

Il ne sera en outre pas difficile de démontrer le théorème suivant :

Théorème 2.4. *Si $\frac{p}{m}$ et $\frac{q}{n}$ sont deux nombres fractionnaires strictement positifs, alors*

$$\frac{p}{m} : \frac{q}{n} = \frac{p}{m} \cdot \frac{n}{q}$$

**Preuve** Selon la définition 2.2, on a

$$\left(\frac{p}{m} : \frac{q}{n}\right) \cdot \frac{q}{n} = \frac{p}{m}$$

et donc

$$\left[\left(\frac{p}{m} : \frac{q}{n}\right) \cdot \frac{q}{n}\right] \cdot \frac{n}{q} = \frac{p}{m} \cdot \frac{n}{q}$$

Mais, on aura aussi

$$\begin{aligned} \left[\left(\frac{p}{m} : \frac{q}{n}\right) \cdot \frac{q}{n}\right] \cdot \frac{n}{q} &= \left(\frac{p}{m} : \frac{q}{n}\right) \cdot \left(\frac{q}{n} \cdot \frac{n}{q}\right) = \\ &= \left(\frac{p}{m} : \frac{q}{n}\right) \cdot 1 = \frac{p}{m} : \frac{q}{n} \end{aligned}$$

et donc, en comparant,

$$\frac{p}{m} : \frac{q}{n} = \frac{p}{m} \cdot \frac{n}{q}$$

□

Il sera dès lors naturel de se demander si l'addition et la multiplication sur les nombres fractionnaires strictement positifs respectent ou non les propriétés d'associativité, de commutativité, et de distributivité de la multiplication sur l'addition. En réalité, l'axiome 1 contient une version affaiblie de l'associativité de la multiplication. Du reste, toutes les démonstrations et les arguments précédents n'emploient ces propriétés que par rapport aux nombres entiers positifs. Comme les définitions 1.2 et 1.3 s'accordent avec les règles établies pour l'addition et la multiplication des nombres entiers positifs (comme le montre l'argument avancé dans le paragraphe précédent), le lecteur ne sera pas surpris du théorème suivant :

THÉORÈME 2.5. *L'addition et la multiplication sur les nombres fractionnaires strictement positifs respectent les propriétés d'associativité, de commutativité, et de distributivité de la multiplication sur l'addition.*

**Preuve** La preuve de ce théorème ne présente aucune difficulté. Il suffit d'exécuter les opérations selon leur définition et de constater que, puisque l'addition et la multiplication sur les nombres entiers positifs satisfont aux propriétés d'associativité, de commutativité, et de distributivité de la multiplication sur l'addition, il s'ensuit que ces mêmes propriétés sont satisfaites par l'addition et la multiplication sur les nombres fractionnaires strictement positifs. Je vais prouver, à titre d'exemple, que l'addition et la multiplication sur les nombres fractionnaires strictement positifs satisfont à la propriété de distribution de la multiplication sur l'addition. Soient $\frac{p}{m}$, $\frac{q}{n}$ et $\frac{h}{k}$ trois nombres fractionnaires strictement positifs. On aura, alors, d'après les définitions 1.2 et 1.3 et la (30) :

$$\begin{aligned} \frac{h}{k}\left(\frac{p}{m}+\frac{q}{n}\right) &= \frac{h}{k}\left(\frac{pn+qm}{mn}\right) \\ &= \frac{h\,(pn+qm)}{kmn} \end{aligned}$$

et

$$\begin{aligned} \frac{h}{k}\cdot\frac{p}{m}+\frac{h}{k}\cdot\frac{q}{n} &= \frac{hp}{km}+\frac{hq}{kn} \\ &= \frac{hp\cdot kn+hq\cdot km}{km\cdot kn} \\ &= \frac{h\,(pn+qm)}{kmn} \end{aligned}$$

donc

$$\frac{h}{k}\left(\frac{p}{m}+\frac{q}{n}\right)=\frac{h}{k}\cdot\frac{p}{m}+\frac{h}{k}\cdot\frac{q}{n}$$

Les démonstrations des autres parties du théorème sont parfaitement analogues et ne comportent aucune difficulté. Elles peuvent donc être laissées au lecteur à titre d'exercice. □

Une question semble à ce stade se poser de manière spontanée : la classe des nombres fractionnaires strictement positifs ne contiendrait-elle pas les nombres entiers strictement positifsê En d'autres termes, les nombres entiers strictement positifs ne seraient-ils pas des nombres fractionnaires strictement positifs dotés d'une nature particulièreê

Comme il est facile de le constater, les axiomes 1 et 2 établissent des liens multiplicatifs entre nombres entiers strictement positifs et nombres fractionnaires strictement positifs qui permettent, en certains cas, d'établir une égalité entre un nombre de la première sorte et un nombre de la deuxième. On a par exemple, grâce à ces axiomes, au théorème 2.1 qui en dérive, et à la (29) :

$$p\cdot\frac{1}{p}=\frac{p}{p}=\frac{1}{1}=1 \tag{31}$$

$$q\cdot\frac{p}{q}=\frac{qp}{q}=\frac{p}{1}=p \tag{32}$$

$$\frac{p}{p}\cdot\frac{q}{m}=1\cdot\frac{q}{m}=\frac{q}{m} \tag{33}$$

quels que soient les nombres entiers strictement positifs $p$, $q$ et $m$.

Pourtant, ces égalités ne répondent pas tout à fait à la question précédente. En effet, prise à la lettre, cette question est mal posée. La question intéressante, et même la seule sensée

est la suivante : y a-t-il des nombres fractionnaires strictement positifs qui se comportent, relativement les uns aux autres par rapport aux opérations d'addition et de multiplication, exactement comme les nombres entiers strictement positifs se comportent, relativement les uns aux autres, par rapport aux opérations d'addition et de multiplicationê Formulée de cette manière, la question admet la réponse claire que tout le monde attend : oui, il y a de tels nombres fractionnaires strictement positifs. Les égalités (31) et (32) sont justement là pour nous dire quels sont ces nombres : elles nous disent que, quel que soit le nombre entier strictement positif $p$, les nombres fractionnaires strictement positifs $\frac{p}{p}$ et $\frac{p}{1}$ peuvent être pris respectivement pour les nombres entiers positifs 1 et $p$.

Pour mieux comprendre cette réponse et apprendre à travailler avec les nombres fractionnaires strictement positifs, il faut observer que, suivant le théorème (2.2), deux nombres fractionnaires $\frac{p}{m}$ et $\frac{q}{n}$ peuvent être en même temps distincts et égaux : ils sont distincts (conformément à la définition 1.1), si $p \neq q$ ou $m \neq n$, mais il peuvent être en même temps égaux si $pn = mq$. Ainsi l'égalité parmi les nombres fractionnaires strictement positifs ne coïncide pas avec l'identité, comme c'est le cas en revanche pour les nombres entiers positifs. C'est un cas fréquent en mathématiques, même si dans la pratique opérationnelle il est souvent possible (et même quelquefois nécessaire) de confondre identité et égalité, ou du moins de passer de l'une à l'autre sans restrictions.

Une manière simple de justifier cette pratique, sans contrevenir aux exigences abstraites de rigueur logique, est de penser les objets mathématiques comme des classes d'équivalence sous la relation d'égalité. Ainsi, pour en rester à l'exemple des nombres fractionnaires positifs, on pourra reformuler la définition 1.1 comme suit :

Définition 2.2. *On appelle « nombre fractionnaire strictement positif » une classe d'équivalence de couples ordonnés de nombres entiers strictement positifs quelconques notés « $\frac{p}{m}$ » (p et m étant des nombres entiers strictement positifs), telle que, si n, m, p et q sont des nombres entiers strictement positifs, alors les couples $\frac{p}{m}$ et $\frac{q}{n}$ appartiennent à la même classe si et seulement si $pn = mq$ ; si ceci est le cas, la même classe d'équivalence de couples ordonnés de nombres entiers strictement positif, et donc le même nombre fractionnaire strictement positif, pourraient indifféremment être notés par les deux symboles « $\frac{p}{m}$ » et « $\frac{q}{n}$ ».*

## 3. Nombres fractionnaires strictement positifs et relation d'ordre

Si on en reste à la définition 1.1, il semblerait possible de définir de manière totalement libre une relation d'ordre strict sur les nombres fractionnaires strictement positifs. On pourrait dire par exemple que $\frac{p}{q} < \frac{n}{m}$ si et seulement si $p + q < n + m$. Pourtant, si on veut une relation d'ordre strict sur les nombres fractionnaires positifs qui soit compatible avec la définition 2.2 — c'est-à-dire que les nombres fractionnaires strictement positifs qui correspondent à des nombres entiers strictement positifs (ou, si on veut, les nombres fractionnaires strictement positifs qui sont, ou se réduisent à, des nombres entiers strictement positifs) se comportent, relativement les uns aux autres, par rapport à la relation $<$, comme les nombres entiers strictement positifs qui leur correspondent se comportent, relativement les uns aux autres, par rapport à cette même relation —, alors une seule définition s'impose. Elle est, tout simplement, dictée par le théorème 2.2. La voici :

Définition 3.1. *Si $\frac{p}{q}$ et $\frac{n}{m}$ sont deux nombres fractionnaires strictement positifs, alors on dira que $\frac{p}{q}$ précède (ou est plus petit que) $\frac{n}{m}$, en symboles : $\frac{p}{q} < \frac{n}{m}$, si et seulement si $mp < qn$ (la relation $<$ entre les nombres entiers strictement positifs pm et nq étant celle qui correspond à la définition 2.2).*

On a dit que la relation ainsi définie est une relation d'ordre strict sur l'ensemble des nombres fractionnaires strictement positifs. Pour le montrer, il faut montrer qu'elle est anti-réflexive, anti-symétrique et transitive sur cet ensemble. Or il est facile de montrer que les deux premières conditions se vérifient en n'opérant que sur les nombres entiers strictement positifs, car :

*i*) pour aucun couple de nombres entiers strictement positifs $p$ et $q$ on ne peut avoir $pq < pq$ ; donc il n'y a pas de nombre fractionnaire strictement positif $\frac{p}{q}$ tel que $\frac{p}{q} < \frac{p}{q}$ ; la relation définie ci-dessus est donc anti-réflexive ;

*ii*) pour aucun couple de couples de nombres entiers strictement positifs, $p, q$ et $n, m$ on ne peut avoir en même temps $pm < nq$ et $nq < pm$ ; donc il n'y a pas de nombres fractionnaires strictement positifs $\frac{p}{q}$ et $\frac{n}{m}$ tels que $\frac{p}{q} < \frac{n}{m}$ et $\frac{n}{m} < \frac{p}{q}$ et la relation définie ci-dessus est donc anti-symétrique.

En revanche pour démontrer la troisième condition, il faut recourir aux nombres fractionnaires strictement positifs eux-mêmes. Voici comment :

*iii)* pour tout triplet de couples de nombres entiers strictement positifs $p, q$ ; $n, m$ ; et $h, k$, si $pm < nq$ et $nk < hm$, alors $p < \frac{nq}{m}$ — car $p = \frac{p}{1}$ et $1 \cdot nq = nq$, donc si $pm < nq$, alors $pm < 1 \cdot nq$ — et $k < \frac{hm}{n}$ — par un argument analogue au précédent — et donc : $pk < \frac{nq}{m} \cdot \frac{hm}{n} = qh$ ; il s'ensuit, grâce à la définition précédente, que si $\frac{p}{q} < \frac{n}{m}$ et $\frac{n}{m} < \frac{h}{k}$, alors $\frac{p}{q} < \frac{h}{k}$ et la relation définie ci-dessus est donc transitive.

Dans cette dernière preuve, on a employé une propriété que, à strictement parler, on n'a pas encore démontrée. Du fait que

$$p < \frac{nq}{m} \qquad \text{et} \qquad k < \frac{hm}{n}$$

on a tiré que

$$pk < \frac{nq}{m} \cdot \frac{hm}{n}$$

Comme on a vu que pour tout nombre entier positif $s$, $s = \frac{s}{1}$, cette propriété n'est pourtant qu'un cas particulier d'une propriété des nombres fractionnaires strictement positifs qu'on peut aisément démontrer en général. Cette propriété peut s'énoncer ainsi : la relation $<$ sur les nombres fractionnaires strictement positifs est stable la relation $<$ définie sur les nombres fractionnaires strictement positifs par rapport à la multiplication par un facteur commun. La preuve de ceci est immédiate : si $m, p, q$ et $n$ sont des nombres entiers strictement positifs et $pm < qn$, alors, pour tout couple de nombres entiers strictement positifs $h$ et $k$, $ph \cdot mk < qk \cdot nh$ et donc, si $\frac{p}{q} < \frac{n}{m}$, alors, pour tout nombre fractionnaire strictement positif $\frac{h}{k}$, $\frac{p}{q} \cdot \frac{h}{k} < \frac{n}{m} \cdot \frac{h}{k}$. Il ne sera pas difficile de montrer la même chose (et de la même manière) pour la division et l'addition.

Du fait que la relation $<$ sur les nombres fractionnaires strictement positifs est une relation d'ordre strict, il s'ensuit que la relation $\leq$ ($<$ ou $=$) définie sur les mêmes nombres est une relation d'ordre. Il ne reste alors qu'à énoncer et démontrer le théorème suivant :

THÉORÈME 3.1. *L'ensemble des nombres fractionnaires strictement positifs est totalement ordonné relativement à la relation* $\leq$.

**Preuve** Soient $\frac{p}{q}$ et $\frac{n}{m}$ deux nombres fractionnaires strictement positifs ; imaginons qu'on n'ait pas $\frac{p}{q} \leq \frac{n}{m}$. Cela signifie qu'on n'a pas $pm \leq qn$. Or, comme l'ensemble des nombres entiers positifs est totalement ordonné par rapport à la relation $\leq$ définie sur ces nombres, cela signifie que $qn < pm$, c'est-à-dire $nq < mp$, et donc $\frac{n}{m} < \frac{p}{q}$ et ainsi $\frac{n}{m} \leq \frac{p}{q}$. □

## 4. Nombres rationnels positifs

Les théorèmes qu'on a démontrés dans les paragraphes 2 et 3 énoncent les plus élémentaires propriétés des nombres fractionnaires strictement positifs. Ils ne sont, à strictement parler, que des conséquences des définitions 1.1-1.3, 2.1 et 3.1, des axiomes 1-3 et des propriétés préalablement démontrées des nombres entiers strictement positifs, tirées par l'application des règles de déduction qui ne se réfèrent aucunement, en tant que telles, à la nature particulière des objets que, dans le chapitre 1, on a identifié aux nombres entiers positifs. Si ces prémisses sont accordées, les preuves de ces théorèmes suivent des modalités déductives qui ne diffèrent pas essentiellement de celles que suivent les preuves des théorèmes concernant les nombres naturels démontrés à partir des axiomes de Peano et des définitions 3.2 et 2.7 . À la différence de ces derniers axiomes et de ces définitions, les définitions 1.1-1.3, 2.1 et 3.1 et les axiomes 1-3 ne caractérisent pas, pourtant, une structure ensembliste, prise dans sa totalité, mais ne font qu'établir des règles opérationnelles référées à des couples de nombres entiers strictement positifs, et justifiées par une analyse de l'opération de partage d'une grandeur, en laissant, d'ailleurs, libres de penser et de définir ces derniers nombres comme on le veut. Ce n'est qu'*a posteriori* qu'on pourrait montrer que l'ensemble des nombres fractionnaires strictement positifs, pris avec les opérations d'addition et de multiplication et la relation d'ordre qu'on a définies sur ces nombres, est une structure ensembliste d'un certain type, similaire par certains aspects à l'ensemble totalement ordonné des nombres naturels pris avec les opérations d'addition et de multiplication correspondantes, et différente de celui-ci par d'autres aspects.

On peut pourtant inverser le cheminement : commencer en caractérisant une structure ensembliste particulière et reconnaître ensuite, dans ses éléments, des objets qui se comportent, relativement les uns aux autres, comme les nombres fractionnaires strictement positifs, tels qu'on les a définis ci-dessus, et qui peuvent donc être employés, comme ceux-ci, pour exprimer des propriétés de l'opération de partage d'une grandeur. C'est la deuxième des stratégies dont on a discuté au début du présent chapitre. Formellement, les deux ensembles qu'on construit en suivant ces deux stratégies ne sauraient pas différer l'un de l'autre, de même que l'ensemble des nombres entiers positifs, tels qu'on les a définis dans le chapitre 1, ne diffère pas formellement de l'ensemble des nombres naturels, défini dans le chapitre 2. Pourtant, pour souligner la différence de procédure qui nous conduit finalement au même résultat, on emploiera, également dans ce cas, des noms différents, et on parlera, dans ce deuxième cas, de *nombres rationnels positifs*. En vérité, comme on le verra, l'ensemble des nombres rationnels positifs, qu'on construira par extension de $\mathbb{N}$ et qu'on indiquera par les symbole « $\mathbb{Q}^+$ », diffère de l'ensemble des nombres fractionnaires strictement positifs par le fait de présenter, parmi ses éléments, un élément qu'on pourrait identifier avec le nombre zéro. Rien n'empêche pourtant d'ajouter un tel élément à l'ensemble des nombres fractionnaires strictement positifs. Si on a construit cet ensemble de sorte qu'il résulte privé d'un tel élément, ce n'est que pour éviter des complications inutiles dans l'acte de la définition. Mais, une fois que l'ensemble des nombres fractionnaires strictement positifs a été construit, comme on l'a fait ci-dessus, l'introduction de cet élément ne présente pas de difficultés majeures. L'ensemble qu'on obtient après cette introduction, pourrait être dit « ensemble des nombres fractionnaires positifs » et, pris en tant que tel, c'est-à-dire indépendamment de la manière selon laquelle il a été construit, il ne différerait guère de $\mathbb{Q}^+$. Si on ne se réfère, donc, qu'au résultat final de la construction, les deux termes « nombres fractionnaires positifs » et « nombres rationnels positifs » peuvent être pris comme synonymes, de même qu'on peut prendre comme synonymes les termes « nombres entiers positifs » et « nombres naturels ».

Comme on l'a dit, en suivant la seconde stratégie, on arrive exactement aux mêmes résultats qu'en suivant la première, c'est pourquoi je me limiterai à indiquer comment procéder, sans entrer dans les détails.

Remarque 4.5. Avant de commencer, il convient pourtant de fixer soigneusement notre langage, pour éviter de possibles incompréhensions. À la fin du paragraphe 1, j'ai introduit une distinction entre l'ensemble $\mathbb{N}$ des nombres naturels, ainsi qu'il est caractérisé par les cinq axiomes de Peano, en tant que couple formé par un ensemble proprement dit et une application définie sur cet ensemble, de l'ensemble N des éléments de $\mathbb{N}$ considérés séparément, et donc indépendamment de toute fonction qu'on peut définir sur eux. Même si on n'a pas insisté outre mesure sur cette distinction, la différence entre ces deux objets est essentielle. Or, il est clair que, dans notre construction de $\mathbb{Q}^+$, on partira de la donnée de $\mathbb{N}$, et non pas de celle de N, car on emploiera, au cours de cette construction, des propriétés des nombres naturels qui ne sauraient être pensées ni comme des propriétés de N ni comme des propriétés des éléments de N pris séparément. Bien que le résultat auquel on aboutira sera appelé « ensemble », en accord avec une terminologie universellement acceptée, à proprement parler, il sera, lui aussi, plus qu'un ensemble, car il héritera des propriétés des nombres naturels dont on s'est servi au cours de sa construction.

Toutefois, même si la différence entre un ensemble, au sens propre de ce terme, et la structure donnée par cet ensemble pris avec les fonctions, les relations, ou les opérations qui sont définies sur ses éléments est fondamentale, elle ne concerne pas ce qu'on pourrait qualifier comme la dimension de l'ensemble lui-même. En philosophie du langage, on parle souvent d'extension, pour indiquer la donnée des éléments d'un ensemble. Si on veut employer cette terminologie, on dira alors qu'en passant d'un ensemble, au sens propre de ce terme, à n'importe quelle structure donnée par cet ensemble pris avec les fonctions, les relations, ou les opérations qui sont définies sur ses éléments, on ne modifie pas l'extension de l'ensemble de départ. Or, il y a des propriétés essentielles des structures mathématiques, et en particulier de $\mathbb{Q}^+$, pour ce qui nous intéresse dans la suite, qui ne dépendent que de la « dimension » ou « extension » de l'ensemble qui fournit les éléments de cette structure. On apprendra plus tard que ce que nous appelons ici, de manière encore fort imprécise, « dimension » ou « extension » s'appelle, en mathématiques, « cardinalité ». On peut pourtant, pour l'instant, laisser de côté la caractérisation précise de cette notion de cardinalité et observer tout simplement que pour mettre en évidence ces propriétés, on doit souvent faire abstraction des fonctions, relations ou opérations particulières qu'on a déjà définies sur l'ensemble sur lequel on travaille, et considérer, pour ainsi dire, les éléments de cet ensemble comme le substrat de possibles définitions d'autres fonctions, relations ou opérations. Pour éclairer ainsi la nature des arguments qui sont employés au cours des démonstrations qui visent à exhiber ces propriétés, il convient de distinguer de manière explicite entre la structure $\mathbb{Q}^+$ et le simple ensemble de ses éléments pris séparément, qu'on notera par la suite avec le symbole « $\mathrm{Q}^+$ ». Comme ces éléments seront pourtant identifiés à des couples de nombres naturels, leur simple dénomination entraîne l'instauration de certaines relations entre ces éléments, qui dépendent des relations connues entre les nombres naturels. Ainsi si les éléments de $\mathrm{Q}^+$ sont caractérisés de cette manière, $\mathrm{Q}^+$ est, lui aussi, à strictement parler, plus qu'un ensemble, étant en quelque sorte déjà une structure. C'est justement sur cette structure minimale qu'on travaillera par la suite pour prouver des propriétés de $\mathbb{Q}^+$ relatives à sa dimension ou extension.

L'idée essentielle qu'on va suivre est de construire l'ensemble $\mathbb{Q}^+$ comme la plus petite des extensions de $\mathbb{N}$ qui soit fermée par rapport à l'opération inverse de la multiplication, c'est-à-dire la division, en n'admettant qu'une exception : l'impossibilité de la division par 0.

On essaye d'abord de comprendre ce qui nous pousse à admettre (et même à exiger) cette exception. La réponse à cette question est très simple : on exclut la division par 0 pour sauvegarder l'univocité des opérations sur $\mathbb{Q}^+$. Imaginons en effet qu'on autorise la division d'un

nombre naturel quelconque par 0. Alors on pourrait raisonner comme l'a fait le mathématicien et logicien anglais du XIX$^{e}$ siècle Augustus De Morgan pour trouver le plus élégant des paradoxes (appelé justement depuis « paradoxe de De Morgan » ). On suppose d'abord que $p = 1$. Alors $p^2 = p$ et donc

$$p^2 - 1 = p - 1 \tag{34}$$

Mais, d'autre part, quel que soit le nombre naturel $x$, plus grand ou égal à 1, on aura, en accord avec les propriétés de l'addition, de la soustraction et de la multiplication sur $\mathbb{N}$,

$$x^2 - 1 = (x + 1)(x - 1)$$

donc, de (34), il suit

$$(p + 1)(p - 1) = p - 1$$

Or, comme on avait supposé que $p = 1$, on doit en conclure que $p - 1 = 0$. Si on permettait alors de diviser un nombre naturel par zéro, on pourrait passer de là à l'égalité

$$p + 1 = 1$$

d'où il suit que $p = 0$ et donc finalement que $p$ est en même temps égal à 1 et 0, c'est-à-dire que $0 = 1$. Pour tout nombre naturel $n$, on aurait en même temps

$$n + p = n + 1 = n' \qquad \text{et} \qquad n + p = n + 0 = n$$

et

$$n \cdot p = n \cdot 1 = n \qquad \text{et} \qquad n \cdot p = n \cdot 0 = 0$$

et donc, finalement $n' = n = 0$. Rien n'empêche de construire une algèbre où il en aille ainsi, mais cette algèbre ne pourrait certes pas être celle des nombres auxquels nous nous attendons et que nous prétendons pouvoir utiliser dans notre vie quotidienne et dans la plupart de nos recherches scientifiques.

Note Historique 4.5. Fils d'un colonel de l'*Indian Army*, Augustus De Morgan naquit à Madura en Inde, au le mois de juin 1806 et mourut à Londres le 18 mars 1871. Rentré en Angleterre à l'âge de sept mois, il fit ses études dans différentes écoles privées, où il apprit les langues classiques, l'Hébreu et les mathématiques, puis il entra en 1823 au *Trinity College* de Cambridge, où il étudia le droit et la médecine. En 1828, il fut nommé professeur de mathématiques à l'*University College* de Londres, mais il démissionna trois ans plus tard pour protester contre le licenciement injustifié d'un collégue. La mort accidentelle de son successeur, en 1836, lui permit pourtant de retrouver sa place, de laquelle il démissionnera une deuxième fois en 1866. Il fut l'un des fondateurs de la *London Mathematical Society*, dont il fut même le premier président, dès 1865.

Collaborateur assidu de la *Penny Cyclopaedia* (pour laquelle il écrivit plus de 800 articles), il s'intéressa surtout aux fondements des mathématiques et à leur logique démonstrative, et fut l'auteur de nombreux manuels dans différents domaines des mathématiques, dans lesquels il fut toujours attentif à énoncer de la manière la plus claire les principes fondateurs et à organiser le matériel selon une présentation logiquement irréprochable. Ce fut De Morgan qui, dans un article du 1838, codifia pour la première fois, sous le nom d'« induction mathématique », la forme d'inférence que nous avons appelée ici « induction complète ».

Son intérêt envers la nature de l'inférence mathématique fit de lui un des pionniers de la logique formelle moderne. Il fut l'un des premiers à observer et à dénoncer l'inadéquation de la syllogistique aristotélicienne en tant que *canon* de l'inférence

mathématique. Il observa en particulier qu'aucun syllogisme ne pouvait justifier des inférences, largement employées de manière spontanée en mathématiques, et fondées sur des considérations de nature quantitative. Si la plupart des français aime le vin et que la plupart des français aime le fromage, alors il y des français qui aiment en même temps le vin et le fromage : ceci-ci est une inférence sans doute valable, mais d'après De Morgan, aucun syllogisme ne saura la justifier. Cette conviction poussa De Morgan à construire un calcul logique qui préfigure la logique des classes et la théorie de la quantification.

**Lectures possibles** : D. D. Merrill, *Augustus de Morgan and the Logic of Relations*, Kluwer Acad. Pub., Dordrecht, Boston, London, 1990.

Le problème qu'il faut poser pour arriver à $\mathbb{Q}^+$, en partant de $\mathbb{N}$, est alors le suivant : étant donné l'ensemble $\mathbb{N}$ des nombres naturels, est-il possible de construire un ensemble $\mathbb{Q}^+$, contenant $\mathbb{N}$ comme une partie propre (c'est-à-dire, tel que $\mathbb{N} \subset \mathbb{Q}^*$) et tel que pour tout couple d'éléments $\mathfrak{p}$ et $\mathfrak{q}$ de $\mathbb{Q}^+$, où $\mathfrak{q} \neq 0$, il soit possible de définir une opération $\mathfrak{p} : \mathfrak{q}$, qui soit une extension de l'opération $p : q$ $(p, q \in \mathbb{N})$ définie sur les nombres naturels, et soit telle que le résultat de $\mathfrak{p} : \mathfrak{q}$ appartienne à $\mathbb{Q}^+$.

Pour répondre à cette question, on observe d'abord que si $\mathbb{N} \subset \mathbb{Q}^*$ alors pour que la division définie sur $\mathbb{Q}^+$ soit une extension de la division définie sur $\mathbb{N}$, il faut que la division définie sur $\mathbb{Q}^+$ donne le même résultat que la division définie sur $\mathbb{N}$, toutes les fois qu'elle s'applique à des éléments de $\mathbb{Q}^+$ qui sont aussi des éléments de $\mathbb{N}$, pour lesquels il existe un quotient dans $\mathbb{N}$ lui-même. On sait que si $p$ et $q$ sont des nombres naturels et $q \neq 0$, alors il est possible qu'il n'y ait pas de nombre naturel $n$, tel que $p = nq$, de sorte que l'opération $p : q$ n'ait pas de résultat dans $\mathbb{N}$. On peut donc imaginer de considérer deux éléments $p$ et $q$ de $\mathbb{N}$, avec $q \neq 0$, tels qu'il n'y ait aucun élément $n$ de $\mathbb{N}$, tel que $p = nq$, et d'ajouter à $\mathbb{N}$ un nouvel élément, noté « $\frac{p}{q}$ », en posant la convention que, dans le nouvel ensemble ainsi construit, $p : q = \frac{p}{q}$. On peut imaginer que ceci soit fait pour tout couple d'éléments $x$ et $y$ de $\mathbb{N}$, avec $y \neq 0$, tels qu'il n'y ait aucun élément $n$ de $\mathbb{N}$, tel que $x = ny$, en convenant aussi de garder, dans l'ensemble élargi ainsi construit, $n$ comme le résultat de la division $x : y$ entre les nombres naturels $x$ et $y$ $(y \neq 0)$, lorsque $n$ appartient à $\mathbb{N}$ et $x$ et $y$ sont tels que $x = ny$. Pourtant, pour éviter des spécifications fastidieuses, il convient d'assigner aux éléments du nouvel ensemble des propriétés opérationnelles qui permettent de ne pas faire la différence entre le cas où il existe dans $\mathbb{N}$ un élément $n$, tel que $x = ny$ et le cas contraire. Cela signifie que la condition suivante doit être respectée :

$$\text{si } p, q, n \in \mathbb{N},\ q \neq 0 \text{ et } p = nq, \text{ alors } n = \frac{p}{q} \tag{35}$$

Comme, à cause de la fermeture de $\mathbb{N}$ relativement à la multiplication, pour tout nombre naturel $n$, il est toujours possible, lorsque le nombre naturel $q \neq 0$ est fixé arbitrairement, de trouver un nombre naturel $p$ tel que $p = nq$, cette condition assigne à chaque nombre naturel une infinité de nouveaux noms sous la forme d'un symbole de la forme « $\frac{p}{q}$ », ou $p$ et $q$ sont des nombres naturels et $q \neq 0$.

Imaginons que $p = q$ ; alors il existe un nombre naturel $n$ tel que $p = nq$ et ce nombre est évidemment 1, donc de (35), il suit que, pour tout nombre naturel $p \neq 0$,

$$\frac{p}{p} = 1 \tag{36}$$

ce qui est une partie du contenu de (31). Par contre, si $q = 1$ , alors, quel que soit $p$, on aura $p = pq$ et de (35), il suit que, pour tout nombre naturel $p$ :

$$p = \frac{p}{1} \tag{37}$$

qui est une partie du contenu de (32).

De plus, comme $nq = nq$, de (35) il suit que si $n$ et $q$ sont deux nombres naturels et $q \neq 0$, alors

$$\frac{nq}{q} = n \tag{38}$$

qui correspond à (32).

Il reste naturellement à définir l'addition et la multiplication entre les éléments du nouveau ensemble qui n'étaient pas des éléments de $\mathbb{N}$. Le lecteur pourra s'exercer à montrer que si on veut faire ceci en définissant d'emblée ces opérations sur tous les éléments de ce nouvel ensemble, sans faire de distinction entre ceux qui étaient des éléments de $\mathbb{N}$ et ceux qui ne l'étaient pas, et si l'on ne veut pas contredire les stipulations précédentes, alors ces opérations ne peuvent être définies que comme on l'a fait ci-dessus pour ceux qu'on avait appelés des « nombres fractionnaires strictement positifs », en ajoutant la condition suivante :

$$\text{si } q \text{ est un nombre naturel différent de zéro, alors } \frac{0}{q} = 0$$

Ceci fait, il pourra définir la division sur les éléments de l'extension de $\mathbb{N}$ ainsi obtenue comme l'inverse de la multiplication, et vérifier que cette extension est fermée par rapport à la division ainsi définie (à l'exception de la division par 0). Comme, une fois qu'on aura démontré, à partir de ces définitions, que $\frac{p}{q} = \frac{n}{m}$ si et seulement si $pm = qn$, et qu'on aura accepté d'identifier entre eux les éléments d'une telle extension qui sont égaux entre eux, il sera facile de montrer qu'aucune extension de $\mathbb{N}$ plus petite que celle-ci ne peut satisfaire à la condition de fermeture par rapport à la division sur les nombres naturels, cette vérification conclut le parcours : l'ensemble qu'on a ainsi obtenu — qui pourrait être identifié comme l'ensemble de tous les couples ordonnés $< p, q >$ d'éléments de $\mathbb{N}$ tels que $q \neq 0$, ou, si on préfère, comme l'ensemble des classes d'équivalence de ces couples sous la relation d'égalité définie sur l'ensemble de ces couples — est bien l'ensemble $\mathbb{Q}^+$ cherché. Le lecteur pourra ensuite s'attacher à justifier une définition de la relation d'ordre stricte $<$ parfaitement analogue à la définition 3.1, d'où il suivra évidemment que $\mathbb{Q}^+$ est un ensemble totalement ordonné relativement à la relation $\leq$.

La construction de $\mathbb{Q}^+$ qu'on vient d'esquisser nous suggère une remarque qu'on aurait déjà pu introduire ci-dessus par rapport aux nombres fractionnaires (strictement) positifs, mais qu'il me semble plus naturel d'introduire ici, en exploitant justement la suggestion qui nous est fournie par cette construction. Dans ce qui précède, on s'est réclamé en différentes occasions (explicitement ou implicitement) d'une circonstance qui nous a paru évidente : si on ajoute à un ensemble $E$ donné, un élément $x$ distinct de tous les éléments déjà contenus dans $E$, on obtient un ensemble qui est, en un sens, plus large que $E$ : l'ensemble $E$ est une partie propre de l'ensemble ainsi obtenu ; il est un sous-ensemble de cet ensemble et ne coïncide pas avec lui, car ce dernier ensemble contient tous les éléments que $E$ contient et en contient un que $E$ ne contient pas. Pourtant, comme on l'a déjà vu dans le chapitre 2, si l'ensemble $E$ est infini, cela ne signifie pas que le nouvel ensemble contienne plus d'éléments que $E$. En effet, si $E$ est infini, l'ensemble obtenu en lui ajoutant un nouvel élément est également infini et on a vu qu'une des caractéristiques d'un ensemble infini est qu'on peut le mettre en bijection avec certaines de ses parties propres. Ainsi, si l'ensemble $\mathbb{N}$ est donné et qu'on lui ajoute $\frac{1}{2}$ comme nouvel élément,

on obtient l'ensemble $\mathbb{N} \cup \frac{1}{2}$ qui peut parfaitement être mis en bijection avec sa partie propre $\mathbb{N}$ (par exemple grâce à l'application $F : \mathbb{N} \cup \frac{1}{2} \to \mathbb{N}$, qui associe $\frac{1}{2}$ à 0 et ensuite chaque élément $i$ de $\mathbb{N} \cup \frac{1}{2}$ différent de $\frac{1}{2}$ à l'élément $i + 1$ de $\mathbb{N}$). Ainsi $\mathbb{N} \cup \frac{1}{2}$ est plus large que $\mathbb{N}$, car $\mathbb{N}$ est une partie propre de $\mathbb{N} \cup \frac{1}{2}$, mais ne contient pas plus d'éléments que $\mathbb{N} \cup \frac{1}{2}$.

On peut penser qu'il en sera autrement si on ajoute à $\mathbb{N}$ non pas un seul nouvel élément, ni même un nombre fini de nouveaux éléments, mais un nombre infini de nouveaux éléments, voire les éléments d'un ensemble infini supposé plus large que $\mathbb{N}$. Or, pour passer de $\mathbb{N}$ à $\mathbb{Q}^+$, on a justement ajouté à $\mathbb{N}$ les éléments d'un ensemble à son tour infini et sans doute plus large que $\mathbb{N}$. Pour le voir, il suffit d'éliminer de $\mathbb{Q}^+$ tous les éléments qui sont déjà contenus en $\mathbb{N}$ (ou — si on veut identifier $\mathbb{Q}^+$ avec tous les couples $< p, q >$ d'éléments de $\mathbb{N}$, tels que $q \neq 0$ — tous les éléments égaux à des éléments déjà contenus en $\mathbb{N}$). On aura encore dans $\mathbb{Q}^+$ beaucoup d'éléments. En particulier on aura tous les éléments de la forme « $\frac{1}{i}$ », où $i$ est un nombre naturel différent de 0 ou 1, plus deux autres éléments quelconques qui ne sont pas de cette forme, tels, par exemple, $\frac{2}{3}$ et $\frac{3}{2}$, et ces éléments constituent bien un ensemble $E$ qu'il sera facile de mettre en bijection avec $\mathbb{N}$, grâce par exemple à l'application $E \to \mathbb{N}$ qui associe $\frac{2}{3}$ à 0, $\frac{3}{2}$ à 1, et ensuite chaque élément $\frac{1}{i}$ de $E$ tel que $i \neq 0, 1$ avec l'élément $i$ de $\mathbb{N}$. Or si on enlève de $\mathbb{Q}^+$ aussi tous les éléments de $E$, on obtient un ensemble qui non seulement n'est pas vide, mais est encore infini.

On peut donc penser qu'on ne pourra pas mettre $\mathbb{Q}^+$ en bijection avec $\mathbb{N}$, qu'il est non seulement plus large que $\mathbb{N}$, mais qu'il contient aussi bien plus d'éléments que $\mathbb{N}$. C'est pourtant faux. La démonstration est fort simple et en fut faite par le mathématicien allemand Georg Cantor à la fin du XIX$^{\text{e}}$ siècle. Elle permet de prouver le théorème suivant :

THÉORÈME 4.1. *L'ensemble $\mathbb{Q}^+$ est dénombrable, c'est-à-dire qu'il peut être mis en bijection avec l'ensemble $\mathbb{N}$ des nombres naturels.*

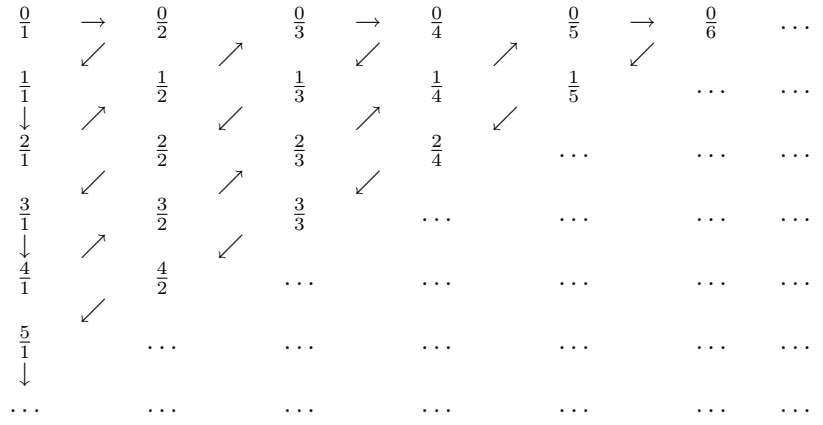
Pour démontrer ce théorème, on va, à proprement parler, travailler sur $\mathrm{Q}^+$, plutôt que sur $\mathbb{Q}^+$. La question à laquelle ce théorème répond concerne en fait une propriété de $\mathbb{Q}^+$ qui ne dépend pas des fonctions, relations ou opérations définies sur ses éléments. Et, pour l'exhiber, on ne fera au fond que définir sur ces éléments un ordre essentiellement différent de l'ordre habituel induit par la relation $\leq$. Il convient donc, pour plus de clarté, de ne considérer d'emblée que l'ensemble $\mathrm{Q}^+$. On considérera en outre $\mathbb{Q}^+$ comme l'ensemble de tous les couples $< p, q >$ d'éléments de $\mathbb{N}$, tels que $q \neq 0$, indépendamment du fait qu'ils soient ou non égaux à d'autres éléments de $\mathbb{Q}^+$. $\mathrm{Q}^+$ sera donc pensé d'emblée comme l'ensemble de tous les couples $< p, q >$ d'éléments de $\mathbb{N}$, tels que $q \neq 0$ (ce qu'on pourra aussi noter par le symbole « $\mathbb{N} \times \mathbb{N}_{\neq 0}$ » ) sans préjuger d'aucun ordre sur ces couples, autre que celui qui est induit par l'ordre propre aux éléments de $\mathbb{N}$ qui constituent les composants de ces couples. Il s'agira alors de définir une application bijective $f : \mathrm{Q}^+ \to \mathbb{N}$, c'est-à-dire une application $f : \mathrm{Q}^+ \to \mathbb{N}$ qui associe tout élément de $\mathrm{Q}^+$ à un et un seul élément de $\mathbb{N}$, de sorte que tout élément de $\mathbb{N}$ resulte associé selon $f$ à un et un seul élément de $\mathrm{Q}^+$. Démontré de cette manière, le théorème vaudra *a fortiori* aussi pour l'ensemble $\mathbb{Q}^+$ conçu comme l'ensemble des classes d'équivalence des couples ordonnés de nombres naturels, sous la relation d'égalité.

**Preuve du théorème 4.1** Il s'agit d'une preuve fort simple. En exploitant l'ordre propre aux éléments de $\mathbb{N}$ qui constituent les composants des couples qui constituent les éléments de

$\mathrm{Q}^+$, on range d'abord ces éléments dans une matrice doublement infinie, comme la suivante :

$$\begin{array}{ccccccc}
\frac{0}{1} & \frac{0}{2} & \frac{0}{3} & \frac{0}{4} & \frac{0}{5} & \frac{0}{6} & \cdots \\
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \frac{2}{6} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \frac{3}{6} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \frac{4}{6} & \cdots \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \frac{5}{6} & \cdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}$$

Ceci fait, il suffit de compter les éléments de cette matrice selon l'ordre indiqué par les flèches dans le schéma suivant



en associant à chaque nombre rationnel positif $\frac{p}{q}$ le nombre naturel $n = f\left(\frac{p}{q}\right)$ qui indique sa position dans l'ordre exhibé pas ce comptage. □

NOTE HISTORIQUE 4.6. Dans la note historique 5.2 on précisera, avec plus de détails, la notion d'équation algébrique, avec coefficients dans un corps **K**, et on dira ce que signifie résoudre une équation algébrique dans **K**. On ne considérera pour l'instant que des équations avec coefficients dans l'ensemble *BbbZ* des nombres entiers, positifs et négatifs, qui, comme on le verra dans le chapitre 5, n'est pas un corps (on définira avec plus de précision cet ensemble dans le paragraphe 5 ; pour le peu qu'on en dira ici, le lecteur pourra se réclamer de ses souvenirs de collégien). On peut définir ces équations comme des égalités de la forme

$$h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0 = 0$$

où les coefficients $h_n, h_{n-1}, \ldots, h_1, h_0$ ($n \in \mathbb{N}$) sont des nombres entiers déterminés, et $x$ est une inconnue qu'il s'agit de déterminer de telle manière que cette égalité soit satisfaite.

Imaginons que $n$ soit égal à 2, et $h_2, h_1$, et $h_0$ soient respectivement égaux à $1, 0$ et $-1$. On aura alors l'égalité :

$$x^2 - 1 = 0$$

Comme $(-1)^2 = (-1) \cdot (-1) = 1 = 1^2$, il est clair que les deux positions $x = 1$ et $x = -1$ satisfont à cette égalité. On dira alors que les nombres entiers 1 et $-1$ sont

racines de l'équation

$$x^2 - 1 = 0$$

Dans ces cas, les racines de l'équation donnée appartiennent à l'ensemble $BbbZ$, auquel sont censés appartenir ses coefficients. Il est pourtant facile de comprendre qu'il n'en est pas toujours ainsi. Si par exemple on pose $h_0 = -2$, tout demeurant, pour le reste, comme ci-dessus, on aura l'équation

$$x^2 - 2 = 0$$

qui n'a évidemment aucune racine ni dans $BbbZ$, ni dans l'ensemble $\mathbb{Q}$ des nombres rationnels, positifs et négatifs. Considérons alors cette équation. Il est clair que, pour satisfaire à l'égalité correspondante, il faut substituer à $x$ un objet (que, pour des raisons que le lecteur comprendra plus tard, on pourra de toute façon appeler « nombre » ) $r$, tel que $r^2 = r \cdot r = 2$. Cet objet est un nombre réel (cf. le chapitre 6), ou, pour être plus précis, il y a deux nombres réels qui, mis à la place de $x$, satisfont à notre égalité. On les note généralement par les symboles « $\sqrt{2}$ » et « $-\sqrt{2}$ », l'un étant l'inverse de l'autre quant à l'addition définie sur les nombres réels (c'est-à-dire que leur somme est 0). Ces deux nombres réels seront alors les racines de l'équation donnée.

Tout demeurant, pour le reste, comme ci-dessus, l'on pose maintenant $h_0 = 1$. On aura alors l'équation

$$x^2 + 1 = 0$$

Les racines de cette équation seront alors des nombres $c$, tels que $c^2 = c \cdot c = -1$. Il est clair qu'aucun nombre réel $r$ ne peut faire l'affaire, car, autant dans le cas où $r$ serait positif que dans les cas où il serait négatif, le carré $r^2$ de $r$ serait positif et, donc différent de $-1$. Les mathématiciens ont pourtant défini des nombres tels que leur carré est négatif. Ces nombres, dits « nombres complexes », se comportent en vérité de manière assez différente des nombres naturels ou des nombres réels, mais, pour des raisons qu'il serait difficile d'expliquer ici, ils méritent d'être justement considérés comme des nombres. Dans le présent volume, on ne traitera pas de nombres complexes. Le lecteur pourra se limiter à noter que les racines d'une équation algébrique à coefficients en $\mathbb{Z}$ peuvent être aussi bien réels que complexes (qu'on note que, comme on le verra dans le chapitre 6, l'ensemble des nombres réels comprend, comme des sous-ensembles propres, les ensembles des nombres naturels, celui des nombres entiers, positifs et négatifs, et celui des nombres rationnels, positifs et négatifs).

Ceci étant dit, revenons à l'équation

$$h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0 = 0$$

(avec $h_n, h_{n-1}, \ldots, h_0 \in \mathbb{Z}$) et supposons que $h_n$ soit différent de 0. On dira alors que cette équation est une équation algébrique de degré $n$. Il sera alors clair qu'une équation algébrique de degré $n$ est déterminée d'une manière univoque par un $(n+1)$-*uple* ordonné de nombres entiers, dont le premier est différent de 0. On appelle « ensemble des nombres algébriques » l'ensemble $\mathbb{A}$ de tous les nombres réels ou complexes $a$, qui sont tels qu'il y a un $(n+1)$-uple, $\{h_n, h_{n-1}, \ldots, h_0\}$, de nombres entiers tel que $a$ est une racine de l'équation :

$$h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0 = 0$$

déterminée par cette $(n + 1)$-uple. Cela revient à dire qu'un nombre algébrique est un nombre réel ou complexe qui satisfait à une équation algébrique avec coefficients dans $\mathbb{Z}$. De ce qu'on a dit ci- dessus, il suit que, parmi les nombres algébriques, il y

en a certains qui ne sont sans doute pas des nombres réels et d'autres qui le sont. Soit alors $\mathbb{A}_{\mathbb{R}}$ le sous-ensemble propre de $\mathbb{A}$ constitué par tous les nombres algébriques réels et seulement par ces nombres.

Le problème que Cantor se posa, dans un très court article de 1874, intitulé « ?ber eine Eigenschaft des Inbegriffes aller reeller algebraischen Zahlen » (« Sur une propriété de l'agrégat de tous les nombres algébriques réels » ), fut de savoir si l'ensemble $\mathbb{A}_{\mathbb{R}}$ des nombres algébriques réels coïncide ou pas avec l'ensemble des nombres réels, c'est-à-dire s'il existe ou pas des nombres réels non algébriques (des nombres réels qui ne sont racine d'aucune équation algébrique avec coefficients dans $\mathbb{Z}$). Une manière de résoudre ce problème aurait pu être de construire un nombre réel particulier et de montrer qu'il ne pouvait être une racine d'aucune équation algébrique avec coefficients dans $\mathbb{Z}$. Cantor jugea pourtant une telle preuve trop longue et difficile et parvint à la solution de son problème par un argument plus simple et génial, qui fut à l'origine de la théorie des cardinaux (on appelle « nombre cardinal » un nombre, d'une nature qu'il serait trop long et difficile de préciser ici, qui exprime la cardinalité d'un ensemble quelconque) : il montra que l'ensemble *BbbA* des nombres algébriques, et donc, *a fortiori*, l'ensemble $\mathbb{A}_{\mathbb{R}}$ des nombres algébriques réels, peut être mis en bijection avec l'ensemble des nombres naturels (c'est-à-dire qu'il est dénombrable), tandis que ceci n'est pas possible pour l'ensemble des nombres réels (qui n'est donc pas dénombrable). Le lecteur comprendra, en lisant le chapitre 6, ce que signifie, au juste, qu'un ensemble (évidemment infini) n'est pas dénombrable. Ici, il lui suffira de comprendre que la non-dénombrabilité de l'ensemble des nombres réels ne peut certes pas dériver de son être en injection sur $\mathbb{N}$, car cet ensemble inclut l'ensemble $\mathbb{N}$. Dire de cet ensemble qu'il n'est pas dénombrable signifie donc dire que l'ensemble des nombres réels contient plus d'éléments que l'ensemble $\mathbb{N}$. En ayant démontré que l'ensemble $\mathbb{A}_{\mathbb{R}}$ contient autant d'éléments que l'ensemble $\mathbb{N}$ (peut être mis en bijection avec cet ensemble), Cantor put conclure qu'il y a des nombres réels qui ne sont pas algébriques.

On s'intéressera ici seulement à la première partie de cette preuve (celle dans laquelle Cantor prouve que l'ensemble $\mathbb{A}_{\mathbb{R}}$ est dénombrable) ; on reviendra en revanche sur la deuxième dans le chapitre 6.

Il est d'abord clair que l'ensemble $\mathbb{Q}^+$ des nombres rationnels positifs est inclus dans *BbbA* comme un sous-ensemble propre. En effet, quels que soient les nombres naturels $p$ et $q$ (avec $q \neq 0$), le nombre rationnel positif $\frac{p}{q}$ sera racine de l'équation algébrique avec coefficients en $\mathbb{Z}$, de premier dégré, $qx - p = 0$. Du fait que l'ensemble *BbbA* est dénombrable, il s'ensuit donc, sur-le-champ, que l'ensemble $\mathbb{Q}^+$ (qui n'est sans doute pas fini) est dénombrable aussi. En démontrant que *BbbA* est dénombrable, Cantor démontra donc, en 1874, que $\mathbb{Q}^+$ l'est aussi. On comprendra pourtant que la démonstration que Cantor donna, pour ce théorème, en 1874, ne fut pas celle qu'on vient de donner pour le théorème 4.4.1. Cette dernière démonstration, qui s'applique directement à l'ensemble $\mathbb{Q}^+$ des nombres rationnels positifs, ne peut en effet s'étendre, tout au plus, qu'à l'ensemble des nombres rationnels positifs ou négatifs (on verra comment dans le paragraphe 5). L'argument de Cantor est néanmoins assez simple. Le voici.

Si une équation algébrique avec coefficients dans $\mathbb{Z}$ est donnée, disons

$$h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0 = 0$$

il ne sera guère difficile de lui associer le nombre naturel $\nu$, défini comme il suit

$$\nu = |h_n| + |h_{n-1}| + \ldots |h_1| + |h_0| + n$$

où quel que soit le nombre entier $k$, le symbole « $|\ k\ |$ » indique le nombre naturel $k$, si $k$ est positif, et le nombre naturel $-k$, si $k$ est négatif. On dira que le nombre naturel $\nu$ associé de cette manière à une équation algébrique à coefficients dans $\mathbb{Z}$ est la *hauteur* de cette équation. Soit maintenant $m$ un nombre naturel quelconque. Il est clair qu'il ne pourra être la hauteur que d'un nombre fini d'équations avec coefficients dans $\mathbb{Z}$. Pour le comprendre fort rapidement, il suffit d'observer qu'aucune équation de la sorte, de degré plus grand ou égal à $m$, ne pourra avoir une hauteur égale à $m$, et que parmi les équations algébriques avec coefficients dans $\mathbb{Z}$, aucune, dont un coefficient $h_i$ est tel que $|h_i| > m$, ne pourra avoir, non plus, une hauteur égale à $m$. Le $(n+1)$-uple de nombres entiers qui détermine une équation de hauteur $m$ ne pourra donc être constitué par plus de $m-1$ termes, et ne pourra être construite qu'en combinant entre eux, avec le signes $+$ et $-$, les nombres naturels plus petits que $m$. Et il est clair que pour tout nombre naturel $m$, il n'y aura qu'un nombre fini de $(n+1)$-uples de cette sorte.

Pour continuer, il faut, à ce stade, se réclamer d'un des théorèmes les plus importants des mathématiques : le théorème fondamental de l'algèbre. Il sera impossible de démontrer ici un tel théorème qui, énoncé, sous forme d'une conjecture, par Descartes en 1637, dans le troisième livre de la *Géométrie*, ne fut démontré, sous une forme qu'aujourd'hui on considère correcte, que par Gauss, en 1816. On pourra pourtant l'énoncer sans difficulté : une équation algébrique quelconque de degré $n$, avec coefficients réels ou complexes, a exactement $n$ racines réelles ou complexes. Ce qui nous intéresse ici n'est en vérité qu'un corollaire de ce théorème vraiment fondamental : une équation algébrique de degré $n$, avec coefficients dans $\mathbb{Z}$, n'a pas plus de $n$ racines réelles ou complexes. Le nombre des racines réelles ou complexes de toutes les équations algébriques avec coefficients dans $\mathbb{Z}$ de hauteur $m$ sera ainsi, pour tout $m$, un nombre fini. On pourra donc compter ces racines et, de cette manière, associer à chacune de ces racines un nombre naturel. Or, il est facile de voir qu'aucune équation algébrique à coefficients dans $\mathbb{Z}$ ne pourra avoir une hauteur plus petite que 2. On commencera alors par prendre $m = 2$ et on comptera toutes les racines des équations algébriques à coefficients dans $\mathbb{Z}$ dont la hauteur est 2 ; lorsqu'on aura fini, on prendra $m = 3$ et on comptera toutes les racines des équations algébriques à coefficients dans $\mathbb{Z}$ dont la hauteur est 3 ; lorsqu'on aura fini, on passera à $m = 4$ ; et ainsi de suite. Il est clair que de cette manière on pourra compter tous les nombres algébriques. Cela démontre le théorème de Cantor.

Il reste seulement à dire, pour conclure, que Cantor présenta la preuve qu'on a donnée ci-dessus pour le théorème 4.4.1, quelques années plus tard, en 1895, dans un mémoire intitulé « Beiträge zur Begrundung der transfiniten Mengenlehre » (« Contribution au fondement de la théorie des ensembles transfinis » ). On observe d'ailleurs que la preuve de 1895 n'est qu'une géniale simplification de la preuve de 1874. En effet, tout nombre rationnel positif $\frac{p}{q}$ est, comme on l'a dit, racine d'une équation algébrique avec coefficient dans $\mathbb{Z}$, $qx - p = 0$, de premier degré et de hauteur $p+q+1$. Compter les nombres rationnels positifs équivaut ainsi à compter les racines des équations de la forme $qx - p = 0$, où $p$ et $q$ sont des nombres naturels et $q \neq 0$. La preuve de 1895 ne fait qu'exposer une procédure fort simple pour réaliser ce comptage.

**Lectures possibles** : F. Klein, « Existence des nombres transcendants. Démonstration de Cantor », *in* F. Klein, *Leçons sur certaines questions de Géométrie élémentaire*, Diderot éditeur, Paris, 1997, pp. 61-66.

REMARQUE 4.6. Comme l'application $f : \mathrm{Q}^+ \to \mathbb{N}$ qu'on a ainsi définie est bijective, on pourra l'inverser, c'est-à-dire qu'on pourra considérer l'application qui associe à chaque élément $n$ de $\mathbb{N}$, l'élément $\mathfrak{q}$ de $\mathrm{Q}^+$ tel que $n = f(\mathfrak{q})$. Si, en suivant une convention habituelle on note l'application inverse d'une application $\varphi$ donnée par le symbole « $\varphi^{-1}$ », on aura alors une application, évidemment bijective, $f^{-1} : \mathbb{N} \to \mathrm{Q}^+$ telle que $\mathfrak{q} = f^{-1}(n)$ si et seulement si $n = f(\mathfrak{q})$. L'application $f^{-1} : \mathbb{N} \to \mathrm{Q}^+$ ainsi définie par inversion exhibera alors un nouvel ordre sur $\mathrm{Q}^+$, qu'on pourra représenter ainsi :

$$\mathfrak{q}_0 = \frac{0}{1} \to \mathfrak{q}_1 = \frac{0}{2} \to \mathfrak{q}_2 = \frac{1}{1} \to \mathfrak{q}_3 = \frac{2}{1} \to \mathfrak{q}_4 = \frac{1}{2} \to \dots$$

où on aura écrit, par simplicité, « $\mathfrak{q}_i$ » en lieu de « $f^{-1}(i)$ » $(i = 0, 1, 2, ...)$. Bien que cet ordre ait été construit en s'appuyant sur l'ordre défini sur $\mathbb{N}$, il n'est, en tant que tel, qu'un ordre sur les éléments de $\mathrm{Q}^+$. On pourra donc l'associer à une relation d'ordre stricte sur $\mathrm{Q}^+$, qu'on notera « $\prec$ », et qu'on définira ainsi : si $\mathfrak{p}$ et $\mathfrak{q}$ appartiennent à $\mathrm{Q}^+$, alors $\mathfrak{p} \prec \mathfrak{q}$ si et seulement si $f(\mathfrak{p}) < f(\mathfrak{q})$, la relation $<$ étant l'habituelle relation d'ordre définie sur $\mathbb{N}$. De cette manière, on aura ainsi construit implicitement une structure $< \mathbb{Q}^+, \prec >$ essentiellement différente de $\mathbb{Q}^+$.

Or, au lieu de raisonner comme on vient de le faire sur l'ensemble $\mathrm{Q}^+$, on peut raisonner de la même manière sur une structure un peu plus élaborée. On peut imaginer de considérer $\mathbb{Q}^+$ comme l'ensemble des classes d'équivalence des couples $< p, q >$ des éléments de $\mathbb{N}$, tels que $q \neq 0$, sous la relation d'égalité définie sur ces couples. Comme la définition de cette relation fait intervenir la multiplication définie sur les éléments de $\mathbb{N}$, il faudra, pour parvenir à la détermination des éléments de cet ensemble, se référer à quelque chose de plus qu'à la relation $<$ définie sur $\mathbb{N}$, qui nous avait permis de construire la matrice sur laquelle porte la preuve du théorème 4.1. La manière la plus simple pour parvenir à travailler sur l'ensemble des éléments de $\mathbb{Q}^+$ conçu de cette manière, indépendamment de toute fonction, relation ou opération définie sur ces éléments, pris justement en tant qu'éléments de $\mathbb{Q}^+$, est la suivante. On part de $\mathrm{Q}^+$, défini comme ci-dessus comme l'ensemble, aussi noté « $\mathbb{N} \times \mathbb{N}_{\neq 0}$ », de tous les couples $< p, q >$ d'éléments de $\mathbb{N}$, tels que $q \neq 0$ et on définit sur $\mathrm{Q}^+$ la relation $=$ comme il suit : si $< n, m >$ et $< s, t >$ appartiennent à $\mathrm{Q}^+$, $< n, m >=< s, t >$ si et seulement si $nt = ms$. On obtient ainsi une nouvelle structure $< \mathbb{Q}^+, = >$, qu'on pourra noter « $\mathrm{Q}^+_=$ » sur laquelle on va justement travailler. Les éléments de cette structure seront évidemment les éléments de $\mathrm{Q}^+$, et on pourra donc les ranger comme on l'a fait dans la preuve du théorème 4.1. Mais, comme on dispose maintenant de la relation $=$ définie sur ces éléments, on pourra maintenant ne pas considérer, dans notre comptage, les éléments de $\mathrm{Q}^+_=$ égaux à des éléments de $\mathrm{Q}^+_=$ qu'on a déjà comptés. On aura ainsi directement une preuve de la dénombrabilité de $\mathbb{Q}^+$ pensé comme classe d'équivalence des couples $< p, q >$ des éléments de $\mathbb{N}$, tels que $q \neq 0$, sous la relation d'égalité. Cette procédure nous fournira, comme tout à l'heure, deux bijections mutuellement inverses $f : \mathrm{Q}^+_= \to \mathbb{N}$ et $f^{-1} : \mathbb{N} \to \mathrm{Q}^+_=$, qui induiront un ordre strict sur $\mathrm{Q}^+_=$ représenté comme il suit :

$$\mathfrak{q}_0 = \tfrac{0}{1} \to \mathfrak{q}_1 = \tfrac{1}{1} \to \mathfrak{q}_2 = \tfrac{2}{1} \to \mathfrak{q}_3 = \tfrac{1}{2} \to$$
$$\to \mathfrak{q}_4 = \tfrac{1}{3} \to \mathfrak{q}_5 = \tfrac{3}{1} \to \mathfrak{q}_6 = \tfrac{4}{1} \to \dots$$

(où on aura naturellement encore écrit, par simplicité, « $\mathfrak{q}_i$ » en lieu de « $f^{-1}(n)$ » ($i = 0, 1, 2, ...$) ), ou bien

$$0 \to 1 \to 2 \to \frac{1}{2} \to \frac{1}{3} \to 3 \to 4 \to \frac{3}{2} \to \frac{2}{3} \to \frac{1}{4} \to \frac{1}{5} \to \dots$$

Encore une fois, bien que cet ordre ait été construit en s'appuyant sur les relations $=$ et $<$ et sur la multiplication définies sur $\mathbb{N}$, il n'est, en tant que tel, qu'un ordre sur les éléments de $\mathrm{Q}^{+}_{=}$. On pourra donc, à nouveau, l'associer à une relation d'ordre strict sur $\mathrm{Q}^{+}_{=}$, qu'on pourra encore noter « $\prec$ » et qu'on définira ainsi : si $\mathfrak{p}$ et $\mathfrak{q}$ appartiennent à $\mathrm{Q}^{+}_{=}$, alors $\mathfrak{p} \prec \mathfrak{q}$ si et seulement si $f(\mathfrak{p}) < f(\mathfrak{q})$. On aura alors construit une nouvelle structure $< \mathbb{Q}^{*}_{=}, \prec >$ qui est aussi essentiellement différente de $\mathbb{Q}^{+}$, où on aura :

$$0 \prec 1 \prec 2 \prec \frac{1}{2} \prec \frac{1}{3} \prec 3 \prec 4 \prec \frac{3}{2} \prec \frac{2}{3} \prec \frac{1}{4} \prec \frac{1}{5} \prec \dots$$

Tout cela peut être résumé ainsi : pour montrer que $\mathbb{Q}^{+}$ est dénombrable, on a ordonné ses éléments selon une relation d'ordre strict différente de $<$, en construisant soit la structure $< \mathbb{Q}^{+}, \prec >$, soit la structure $< \mathbb{Q}^{+}_{=}, \prec >$, selon la conception de $\mathbb{Q}^{+}$ de laquelle on est parti. Or, si on réfléchit à cette démonstration, on se rend aisément compte qu'elle ne revient, en dernière instance, qu'à montrer que l'ordre de $\mathbb{Q}^{+}$ ou $\mathbb{Q}^{+}_{=}$, induit par les relations d'ordre strict $\prec$ définies sur ces structures est tel que chaque élément de $\mathbb{Q}^{+}$ ou $\mathrm{Q}^{+}_{=}$ possède, relativement à ces relations, un et un seul successeur, c'est-à-dire que pour tout élément $x$ de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$, il y a un et un seul autre élément $y$ respectivement de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$, tel que $x \prec y$ et que, quel que soit $z$, différent de $x$ et $y$ et appartenant respectivement à $\mathrm{Q}^{+}$ ou à $\mathrm{Q}^{+}_{=}$, soit $z \prec x \prec y$, soit $x \prec y \prec z$, mais non $x \prec z \prec y$. On pourra dire alors que l'élément $y$ de $\mathrm{Q}^{+}$ ou de $\mathbb{Q}^{+}_{=}$ qui satisfait à cette condition relativement à un élément $x$ donné de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$ est le $\prec$-*successeur* de $x$ en $\mathrm{Q}^{+}$ ou en $\mathrm{Q}^{+}_{=}$. Il est de surcroît clair que l'élément 0 autant de $\mathrm{Q}^{+}$ que de $\mathrm{Q}^{+}_{=}$ est tel qu'il n'y a aucun autre élément $x$ respectivement de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$, tel que $x \prec 0$, c'est-à-dire que 0 n'est le $\prec$ -successeur d'aucun élément de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$. Il est donc facile de montrer que si on définit sur $\mathrm{Q}^{+}$ ou sur $\mathrm{Q}^{+}_{=}$ une application $\Phi : \mathrm{Q}^{+} \to \mathrm{Q}^{+}$ ou $\Phi : \mathrm{Q}^{+}_{=} \to \mathrm{Q}^{+}_{=}$, telle que si $x$ et $y$ sont des éléments de $\mathrm{Q}^{+}$ ou de $\mathrm{Q}^{+}_{=}$, alors $y = \Phi(x)$ si et seulement si $y$ est le $\prec$-successeur de $x$ respectivement en $\mathrm{Q}^{+}$ ou en $\mathrm{Q}^{+}_{=}$, alors les couples $< \mathrm{Q}^{+}, \Phi >$ et $< \mathrm{Q}^{+}_{=}, \Phi >$ sont des progressions et ne diffèrent donc pas, quant à leur forme logique, de $\mathbb{N}$, ainsi qu'il est caractérisé par les axiomes de Peano.

Il est clair que cela n'est guère la même chose que de dire que $\mathbb{Q}^{+}$ est une progression. La propriété d'être une progression s'assigne en fait à un ensemble relativement à une application définie sur les éléments de cet ensemble, c'est-à-dire, comme on vient de le dire implicitement, qu'elle est une propriété propre à une structure formée par un ensemble et une application définie sur cet ensemble. Si ci-dessus on a souvent dit que $\mathbb{N}$ est une progression, c'est parce que la définition de $\mathbb{N}$ due aux axiomes de Peano caractérise directement cet ensemble comme une structure de cette sorte, en faisant intervenir d'emblée la relation $(-)'$ qui induit une application sur cet ensemble.

Le fait que $\mathbb{Q}^{+}$ soit dénombrable montre que, quant à la dimension, la nature de cet ensemble est similaire à celle de l'ensemble $\mathbb{N}$. La remarque précédente devrait avoir montré en quoi consiste précisément cette similarité. Mais qu'il y ait similarité ne doit cependant pas cacher qu'il y a aussi différence. Cette différence apparaît dès qu'on remarque, tout simplement, que l'ordre strict sur $\mathrm{Q}^{+}$ ou sur $\mathrm{Q}^{+}_{=}$, exhibé lors de la preuve du théorème 4.1, n'est pas celui établi par la relation $<$ définie sur $\mathbb{Q}^{+}$comme extension de la relation $<$ définie sur $\mathbb{N}$, et on se demande quelle est la structure logique de $\mathbb{Q}^{+}$ conçu comme une extension de $\mathbb{N}$, et donc

pris sans faire abstraction de la relation $<$ définie sur lui, en tant qu'extension de la relation $<$ définie sur les nombres naturels.

Pour parvenir à répondre de manière précise à cette question, on commence par introduire la définition suivante :

DÉFINITION 4.1. *On dit qu'un ensemble $E$, totalement ordonné relativement à une relation d'ordre strict $\mathbf{R}$, est dense par rapport à cette relation ou qu'un ensemble totalement ordonné $< E, \mathbf{R} >$, $\mathbf{R}$ étant une relation d'ordre strict, est dense, si et seulement si, pour tout couple d'éléments distincts de $E$, $x$ et $y$, tels que $x\mathbf{R}y$, il existe un élément $z$ de $E$ tel que :*

$$z \neq x,\ z \neq y,\ x\mathbf{R}z \text{ et } z\mathbf{R}y$$

REMARQUE 4.7. Dans le chapitre 2, on n'a parlé que d'ensembles (partiellement ou totalement) ordonnés relativement à une relation d'ordre et non pas relativement à une relation d'ordre strict. Il est pourtant clair que les définitions données à cette occasion peuvent être modifiées si on veut se référer à une relation d'ordre strict. On dira par exemple qu'un ensemble $E$ est totalement ordonné relativement à la relation d'ordre strict $\mathbf{R}$ (ou que $< E, \mathbf{R} >$ est un ensemble totalement ordonné) si et seulement si $\mathbf{R}$ est une relation d'ordre strict sur $E$ et pour tout couple d'éléments $x$ et $y$ de $E$, soit $x = y$, soit $x\mathbf{R}y$, soit $y\mathbf{R}x$.

La définition 4.1 étant donnée, il est facile de voir que $\mathbb{N}$ n'est pas dense (par rapport à $<$), car quel que soit le nombre naturel $n$, il n'y a aucun intermédiaire selon $<$ entre $n$ et $n' = n+1$. Mais, il est également facile de démontrer que $\mathbb{Q}^+$ est en revanche dense (par rapport à $<$). C'est l'objet du théorème suivant :

THÉORÈME 4.2. *L'ensemble (totalement ordonné) $\mathbb{Q}^+$ est dense (par rapport à la relation $<$).*

**Preuve** Considérons deux nombres rationnels positifs quelconques $\frac{p}{q}$ et $\frac{n}{m}$, tels que $\frac{p}{q} < \frac{n}{m}$. Selon la définition 3.1, on aura aussi : $pm < qn$. Il suffira alors de poser $h = n + p$ et $k = m + q$ pour avoir : $\frac{p}{q} < \frac{h}{k} < \frac{n}{m}$. En effet de $pm < qn$ et du théorème 3.4$(i)$, il s'ensuit que $pm + qp < qn + qp$ et $pm + nm < qn + nm$ et donc, en accord au théorème 3.2$(i)$, $p\,(m + q) < q\,(n + p)$ et $m\,(p + n) < n\,(q + m)$. De la définition 3.1 il suivra alors $\frac{p}{q} < \frac{n+p}{m+q}$ et $\frac{p+n}{q+m} < \frac{n}{m}$, c'est-à-dire : $\frac{p}{q} < \frac{h}{k} < \frac{n}{m}$. □

REMARQUE 4.8. Ce théorème ayant été démontré, on pourrait se demander s'il est possible de définir sur l'ensemble N des éléments de $\mathbb{N}$, une relation d'ordre strict $\prec$, différente de $<$, telle que $< \mathrm{N}, \prec >$ soit dense. Comme on peut s'y attendre, la réponse est positive et il est même assez facile de définir une relation de la sorte. Il suffit de considérer l'application bijective $f^{-1} : \mathbb{N} \to \mathrm{Q}^+_=$ , en observant que les éléments de N sont exactement les éléments de N, de sorte que rien n'empêche, une fois que cette application a été construite, de la penser comme une application bijective $f^{-1} : \mathrm{N} \to \mathrm{Q}^+_=$, et de définir la relation $\prec$ ainsi : si $n$ et $m$ appartiennent à N, alors $n \prec m$, si et seulement si $f^{-1}(n) < f^{-1}(m)$. Que $< \mathrm{N}, \prec >$ soit dense, lorsque $\prec$ est définie ainsi, c'est un simple corollaire du théorème 4.2. La preuve de ce corollaire est tout à fait banale et peut être laissée au lecteur comme exercice.

La morale qu'on peut tirer après cette dernière démonstration est la suivante : d'un point de vue formel, $\mathbb{N}$ et $\mathbb{Q}^+$ ne diffèrent que par l'ordre qui est assigné à leurs éléments. Qui pense ainsi que les nombres naturels sont des objets essentiellement distincts des nombres rationnels positifs, ou bien se trompe, ou bien se réfère non pas aux éléments de $\mathbb{N}$ et $\mathbb{Q}^+$, mais à des éléments d'autres ensembles définis différemment et de manière non formelle, dont les ensembles $\mathbb{N}$ et $\mathbb{Q}^+$ expriment les propriétés relationnelles essentielles. Certains nient que

des ensembles de ce type soient définissables, d'autres pensent que, s'ils le sont, ce ne sont pas des objets mathématiques. Personnellement je ne pense pas ainsi. Il me semble que le chapitre 1 et la première partie du présent chapitre fournissent des soutiens à mon point de vue. Cependant, on ne comprendra pas les mathématiques modernes si on ne comprend pas qu'une manière fort élégante, compacte et logiquement satisfaisante de définir les nombres rationnels — la manière qui est implicitement acceptée par la plupart des mathématiciens — conduit inévitablement à cette conclusion.

Arrivé à ce point, on peut ensuite se demander si, en dépit de ce qu'on a dit ci-dessus, la propriété de dénombrabilité de $\mathbb{Q}^+$ ne dépend pas, elle-aussi, de l'ordre qu'on assigne aux éléments de cet ensemble. En effet, peut-on argumenter, si on compare le théorème 4.1 avec sa preuve, ce théorème nous dit que $\mathbb{Q}^+$ est dénombrable lorsque ses éléments sont ordonnés selon la relation $\prec$. Et il est aussi clair que si on essaye de compter les éléments de $\mathbb{Q}^+$ en suivant l'ordre induit par la relation $<$, on va à coup sûr échouer. Même si, à première vue, ce raisonnement semble plausible, il dépend d'une incompréhension profonde qu'il faut dénoncer. La notion de dénombrabilité d'un ensemble se réfère non pas à la définition actuelle d'un ordre sur cet ensemble qui permet le comptage, mais à la possibilité de définir un tel ordre. Cela est tout à fait raisonnable. Pour le comprendre, on observe d'abord que bien que le fait qu'un ensemble soit fini soit connecté avec la possibilité d'en compter les éléments en les épuisant après un certain temps, et que ce comptage est seulement possible si l'on définit, d'une manière ou d'une autre, un ordre sur ces éléments, le fait qu'un ensemble est fini ne dépend pas de l'ordre choisi : si un ensemble est fini, on peut certainement définir un ordre, quel qu'il soit, qui permet d'en compter les éléments, en les épuisant après un certain temps. Or, quand on dit d'un ensemble qu'il est dénombrable on veut dire de cet ensemble quelque chose de même nature que ce que on dit quand l'on dit qu'il est fini : on veut se référer à une propriété de cet ensemble qui fait qu'il est possible de définir un ordre d'un certain type sur ses éléments. Cela ne signifie pas pourtant que tous les ordres qu'on peut définir sur ses éléments sont nécessairement de ce type.

On a donc au moins trois types d'ensembles : les ensembles finis, les ensembles dénombrables et les ensembles non dénombrables. Les ensembles des deux derniers types sont évidemment infinis, ceux des deux premiers types sont dits par contre « comptables ». Ici, on n'a pas encore exhibé des ensembles infinis non dénombrables. On en exhibera un dans le prochain chapitre 6 . Il faut aussi ajouter que si tous les ensembles dénombrables peuvent être mis en bijection les uns avec les autres, car ils peuvent tous être mis en bijection avec l'ensemble $\mathbb{N}$, cela n'est pas le cas de tous les ensembles infinis non dénombrables. Ceci détermine une hiérarchie d'ensembles infinis qu'on peut caractériser ainsi : d'abord les ensembles dénombrables, puis les ensembles infinis non dénombrables qui peuvent être mis en bijection avec l'ensemble de tous les sous-ensembles de $\mathbb{N}$ (ou d'un ensemble dénombrable quelconque), puis encore les ensembles qui peuvent être mis en bijection avec l'ensemble de tous les sous-ensembles d'un ensemble infini dénombrable du premier type, ensuite les ensembles qui peuvent être mis en bijection avec l'ensemble de tous les sous-ensembles d'un ensemble infini dénombrable du deuxième type, et ainsi de suite. Si on ne se réclame que des axiomes habituels de la théorie des ensembles (les axiomes dits habituellement « de Zermelo-Fraenkel », [cf. la note historique 1.6]), on n'a pas moyen de s'assurer qu'il n'y a pas d'ensembles infinis, autres que ceux-ci. L'hypothèse qui nie cette possibilité est dite « hypothèse généralisée du continu » : on sait aujourd'hui (et ce résultat a été le fruit de beaucoup d'efforts) que cette hypothèse est indépendante des axiomes de Zermelo-Fraenkel, c'est-à-dire que, à partir de ces axiomes, on ne peut démontrer ni cette hypothèse, ni sa négation. Si on suppose l'hypothèse généralisée du continu (c'est-à-dire qu'on ajoute cette

hypothèse aux axiomes de Zermelo-Fraenkel), alors on peut dire que la propriété d'un ensemble infini qui consiste dans le fait qu'il appartient à l'une ou à l'autre de ces catégories est la cardinalité de cet ensemble (si on ne suppose pas l'hypothèse généralisée du continu, alors on ne peut pas caractériser ainsi la cardinalité d'un ensemble ; comme mon but n'est ici que de donner une idée informelle de la notion de cardinalité, je me limiterai pourtant à cette caractérisation). En employant cette terminologie, on dira alors que l'ensemble $\mathbb{Q}^+$ des nombres rationnels positifs a la cardinalité du dénombrable, c'est-à-dire la cardinalité de $\mathbb{N}$.

## 5. Nombres rationnels

Il s'agit maintenant de parcourir la dernière étape : le passage de l'ensemble $\mathbb{Q}^+$ des nombres rationnels positifs à l'ensemble, noté « $\mathbb{Q}$ », des nombres rationnels tout court. Pour ce faire, il suffit de reprendre la méthode qui nous a amenés de $\mathbb{N}$ à $\mathbb{Q}^+$, par rapport à l'opération de soustraction, plutôt qu'à celle de division. Pour simplifier, on montrera d'abord comment, en employant cette méthode, on peut construire l'ensemble, noté « $\mathbb{Z}$ » des nombres relatifs (ou entiers, autant positifs que négatifs) à partir de $\mathbb{N}$.

Comme le problème est celui de construire une extension de $\mathbb{N}$ qui soit fermée par rapport à la soustraction, l'opération inverse de l'addition, et que l'on sait que si $p$ et $q$ sont deux nombres naturels, alors il y a un élément $x$ de $\mathbb{N}$, tel que $p + x = q$ si et seulement si $p \leq q$, on pourrait penser d'abord à ajouter à $\mathbb{N}$ un nouvel élément pour tout couple ordonné de nombres naturels $p$ et $q$ tels que $p \leq q$ (et ensuite prendre l'ensemble des classes d'équivalence des éléments de l'ensemble ainsi construit sous une relation d'égalité qu'il sera facile de définir). Il est pourtant facile de comprendre qu'on peut arriver au résultat voulu de manière bien plus rapide. Il suffit d'ajouter à $\mathbb{N}$ un nouvel élément pour tout élément $p$ de $\mathbb{N}$ différent de 0. À chaque élément $p$ de $\mathbb{N}$, différent de 0, on associe un nouvel élément qu'on notera « $[-p]$ ». On pourra alors stipuler que

$$p + [-p] = 0 \tag{39}$$

et définir ensuite la soustraction sur l'ensemble ainsi obtenu comme l'inverse de l'addition, ce qui donne, $x$, $y$ et $z$ étant trois éléments quelconques de l'ensemble ainsi obtenu :

$$x - y = z \text{ si et seulement si } z + y = x \tag{40}$$

Si $p$ et $q$ sont deux nombres naturels quelconques tels que $p < q$, il suffira alors de stipuler que

$$[-(q - p)] + q = p \tag{41}$$

pour obtenir

$$p - q = -(q - p) \tag{42}$$

où $q - p$ est évidemment un nombre naturel, et donc $[-(q - p)]$ est un des éléments nouveaux qu'on a ajouté à $\mathbb{N}$. Cet ensemble, qu'on appellera justement « $\mathbb{Z}$ » sera alors fermé par rapport à la soustraction définie sur les nombres naturels. Il s'agira alors de montrer qu'il est aussi fermé par rapport à la soustraction définie, conformément à (40 ), sur tous les éléments de lui-même. Pour ceci il faudra définir préalablement l'addition sur $\mathbb{Z}$, de manière qu'elle soit compatible avec l'addition définie sur $\mathbb{N}$.

On observe d'abord que, d'après (41), on aura, pour tout nombre naturel $n$ (différent de 0),

$$[-n] + q = p \text{ si et seulement si } n = q - p \tag{43}$$

c'est-à-dire, selon (40),

$$[-n] + q = p \text{ si et seulement si } n + p = q \tag{44}$$

Il suffira alors de poser, pour tout couple de nombres naturels $p$ et $q$ (différents de 0)

$$[-n] + q = q + [-n]$$

et

$$[-p] + [-q] = [-(p + q)] \tag{45}$$

(ce qui entraîne la commutativité de l'addition entre tous les éléments de $\mathbb{Z}$), pour disposer d'une addition sur $\mathbb{Z}$ et vérifier donc que $\mathbb{Z}$ est bien fermé par rapport à la soustraction définie par la (40).

Une fois que l'ensemble $\mathbb{Z}$ a été ainsi construit, on peut étendre à cet ensemble la multiplication sur les naturels. Pour ce faire, il suffit de poser, pour tout nombre naturel $p$ (différent de 0) :

$$[-p] = [-1] \cdot p = p \cdot [-1] \tag{46}$$

et

$$[-1] \cdot [-1] = 1 \tag{47}$$

et de présupposer l'associativité de la multiplication. En fait, de (46) et de l'associativité supposée de la multiplication sur les nombres relatifs, il suit

$$[-p] \cdot q = ([-1] \cdot p) \cdot q = [-1] \cdot (pq) = [-pq] \tag{48}$$

et

$$q \cdot [-p] = q \cdot ([-1] \cdot p) = (q \cdot [-1]) \cdot p = [-q] \cdot p = [-qp]$$

et donc, comme $pq = qp$,

$$[-p] \cdot q = q \cdot [-p]$$

Et, de même :

$$\begin{array}{rcl} [-p] \cdot [-q] & = & ([-1] \cdot p) \cdot ([-1] \cdot q) = [-1] \cdot [-1] \cdot pq \\ & = & 1 \cdot pq = pq = qp \\ & = & 1 \cdot qp = [-1] \cdot [-1] \cdot qp = \\ & = & ([-1] \cdot q) \cdot ([-1] \cdot p) = [-q] \cdot [-p] \end{array} \tag{49}$$

De là il sera ensuite facile de vérifier que $\mathbb{Z}$ est fermé par rapport à la multiplication ainsi définie.

Quant à la relation d'ordre, il suffira de poser, pour tout couple de nombres naturels $p$ et $q$, différents de 0 :

$$[-p] < 0 \tag{50}$$

(ce qui donne, pour tout couple de nombres naturels $p$ et $m$, $[-p] < m$) et

$$[-p] < [-q] \text{ si et seulement si } q < p$$

d'où il ne sera guère difficile de prouver que $\mathbb{Z}$ est totalement ordonné par rapport à la relation $\leq$, définie à partir de la relation $<$ ainsi définie.

Enfin, on n'aura pas de difficulté à simplifier la notation en éliminant les crochets, ce qui permettra de comprendre sur le champ que, sur $\mathbb{Z}$, l'addition et la soustraction peuvent être prises comme la même opération, dite généralement « addition algébrique ».

Bien que $\mathbb{Z}$ soit fermé par rapport à l'addition algébrique (ou si on veut par rapport à l'addition et à la soustraction, définie comme l'opération inverse de l'addition), il est facile

de vérifier qu'il est ouvert par rapport à la division, définie comme l'opération inverse de la multiplication. Pourtant, le lecteur aura désormais compris comment construire une extension minimale de $\mathbb{Z}$ qui soit fermée par rapport à la division. Il n'aura pas plus de peine à imaginer que cette extension correspond (à des équivalences près, qu'il sera facile de déterminer) à la plus petite extension de $\mathbb{Q}^+$ qui soit fermée par rapport à la soustraction. On notera cet ensemble par « $\mathbb{Q}$ » et on l'appellera « ensemble des nombres rationnels ». Le lecteur pourra s'exercer en le construisant, soit comme extension de $\mathbb{Z}$, soit comme extension de $\mathbb{Q}^+$. Ici on notera simplement que la stipulation (46 ), qu'on pourra écrire en faisant abstraction des crochets, ce qui donne $-p = -1 \cdot p$, rend manifeste la possibilité d'étendre les règles opérationnelles établies sur $\mathbb{Q}^+$ à l'ensemble $\mathbb{Q}$, et indique comment construire une relation d'ordre strict telle que $\mathbb{Q}$ soit totalement ordonné relativement à la relation d'ordre associée.

Quant à la dénombrabilité de $\mathbb{Q}$, la question se résout de façon banale. En fait, le lecteur aura compris que $\mathbb{Q}$ est issu de $\mathbb{Q}^+$ par l'ajout à ce dernier d'un élément nouveau pour tout élément de $\mathbb{Q}^+$ différent de 0. Ainsi tout élément $\frac{p}{q}$ de $\mathbb{Q}^+$, différent de 0 sera associé à un et un seul élément de $\mathbb{Q}- \mathbb{Q}^+$ (c'est-à-dire de l'ensemble obtenu en soustrayant de $\mathbb{Q}$ tous les éléments de $\mathbb{Q}^+$) par la bijection $\frac{p}{q} \to -\frac{p}{q} = \frac{-p}{q} = -1 \cdot \frac{p}{q}$. Il suffira alors de compter les éléments de $\mathbb{Q}$, en suivant l'ordre adopté dans la preuve du théorème (4.1) pour les éléments de $\mathbb{Q}^+$, en passant à $-\frac{p}{q}$ toutes les fois qu'on rencontre un élément $\frac{p}{q}$ de $\mathbb{Q}^+$ différent de 0, avant de passer au successeur de $\frac{p}{q}$ selon cet ordre.

REMARQUE 4.9. On aura alors prouvé que $\mathbb{Q}$ est également dénombrable, et qu'on peut définir sur l'ensemble $\mathbb{Q}$ de ces éléments, pris séparément, une application bijective $\Phi$, telle que $< \mathbb{Q}, \Phi >$ est une progression. Tout ce qu'on a dit pour $\mathbb{Q}^+$ peut donc être répété pour $\mathbb{Q}$.

CHAPITRE 5

# Quelques structures algébriques élémentaires : groupes, anneaux et corps

Dans le chapitre 4, on a montré comment passer de $\mathbb{N}$ à $\mathbb{Q}^+$ et à $\mathbb{Z}$, en cherchant une extension de l'ensemble donné, fermée par rapport aux opérations respectivement inverses de la multiplication et de l'addition. De cette manière, on a construit des structures, c'est-à-dire des ensembles sur lesquels sont définies certaines opérations, fonctions et/ou relations, qui satisfont à certaines conditions. L'étude de quelques structures, indépendamment de la nature spécifique des éléments des ensembles concernés et des opérations, fonctions et/ou relations définies sur eux, est une des tâches majeures de l'algèbre moderne. Dans le présent chapitre, on définira quelques-unes de ces structures (dites justement et en général « algébriques » ) et on montrera comment les ensembles $\mathbb{Z}$, $\mathbb{Q}^+$ et $\mathbb{Q}$ satisfont, lorsqu'ils sont considérés relativement au comportement de leurs éléments vis-à-vis de certaines des opérations ou relations définies sur eux, aux conditions qui interviennent dans les définitions de ces structures. On essaiera de comprendre ainsi, plus généralement, la nature logique autant des procédures par lesquelles on a construit les ensembles des nombres relatifs et des nombres rationnels, que de ces ensembles mêmes.

REMARQUE 5.1. Bien qu'on considèrera par la suite les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}^+$ et $\mathbb{Q}$ relativement au comportement de leurs éléments vis-à-vis de certaines des opérations ou relations définies sur eux, ces ensembles participeront des structures considérées, pour ainsi dire, dans toute leur intégrité définitionnelle, avec la totalité des opérations, relations et/ou fonctions définies sur eux. C'est donc bien de ces ensembles, et non des ensembles N, Z, $\mathrm{Q}^*$ et Q de leurs éléments, qu'il s'agira dans la suite.

## 1. Groupes

La plus simple des structures algébriques qu'on définira ici est généralement dite « magma » :

DÉFINITION 1.1. *On appelle « magma » un couple $< E, * >$ composé par un ensemble $E$ quelconque et une opération $*$ définie sur les éléments de $E$, telle que $E$ est fermé par rapport à $*$ ; une opération de ce type est alors généralement dite « loi de composition interne sur $E$ » (car elle associe à chaque couple d'éléments de $E$ un et un seul élément de $E$ lui-même, ou, dit d'une autre manière, elle correspond à une application de $E^2$ vers $E$, qu'on pourrait noter « $* : E^2 \to E$ » ) ; un magma est donc un couple $< E, * >$ formé d'un ensemble quelconque $E$ et d'une loi de composition interne $*$ sur cet ensemble. Si l'opération $*$ est associative — c'est-à-dire que $x, y, z \in E \Rightarrow [(x * y) * z = x * (y * z)]$ —, alors le magma est dit lui-même « associatif », tandis que si l'opération $*$ est commutative — c'est-à-dire que $x, y \in E \Rightarrow [x * y = y * x]$ —, alors le magma lui-même est dit « commutatif ».*

Il est facile de vérifier que $< \mathbb{N}, + >$, $< \mathbb{N}, \cdot >$, $< \mathbb{Z}, + >$, $< \mathbb{Z}, \cdot >$, $< \mathbb{Q}, + >$ et $< \mathbb{Q}, \cdot >$ sont tous des magmas associatifs et commutatifs, tandis que ni $< \mathbb{N}, - >$, ni $< \mathbb{N}, : >$ ne sont

des magmas, et $< \mathbb{Q}, : >$ est un magma ni associatif, ni commutatif. Le lecteur pourra s'exercer à conduire ces vérifications.

La condition qui définit un magma est apparemment très faible : elle se résume à demander la fermeture de l'ensemble considéré par rapport à l'opération choisie. Pourtant, il est facile de trouver, dans la réalité et dans les mathématiques, des structures qui ne satisfont pas à cette condition, qui relève déjà d'une exigence profonde : les communautés religieuses et/ou politiques, ne sont pas fermé par rapport à l'opération de procréation ; prétendre qu'ils le sont est une option politique très forte (et même, à mon sens, très dommageable). En mathématiques, la fermeture est une condition essentielle qui est souvent utilisée pour construire des extensions d'ensembles donnés. Les exemples avancés au cours du chapitre précédent le montrent bien.

Pourtant dans ces exemples on a considéré des opérations qui ont aussi une autre caractéristique saillante ; comme on le dit généralement, elles sont « unitaires », c'est-à-dire qu'on peut trouver, dans l'ensemble sur lequel elles sont définies, un élément $e$, dit « élément neutre de ces opérations », tel que si $x$ est un élément quelconque de cet ensemble et $*$ est l'opération en question, alors $x * e = e * x = x$. Le lecteur attentif aura de plus remarqué que, parmi les propriétés des opérations qu'on a considérées, l'une a joué un rôle particulièrement important ; il s'agit évidemment de l'associativité, qui permet de réitérer l'opération en question selon des modalités très simples. Si on ajoute à la condition de fermeture, ces deux conditions, on passe de la structure de magma à la structure dite de « monoïde ». En voici la définition précise :

DÉFINITION 1.2. *On appelle « monoïde » un magma associatif et unitaire, c'est-à-dire un couple $< E, * >$ composé d'un ensemble $E$ quelconque et une loi de composition interne associative et unitaire $*$ définie sur les éléments de $E$. En d'autres termes, un couple $< E, * >$ est un monoïde si et seulement si :*

**(*i*)**: *pour tout $x$ et $y$ appartenant à $E$, $x * y$ appartient à $E$ ; en symboles :*

$$x, y \in E \Rightarrow x * y \in E$$

**(*ii*)**: *pour tout $x$, $y$ et $z$ appartenant à $E$, $(x * y) * z = x * (y * z)$ ; en symboles :*

$$x, y, z \in E \Rightarrow (x * y) * z = x * (y * z)$$

**(*iii*)**: *il y a dans $E$ un élément $e$ (dit « élément neutre de $*$ » ), tel que pour tout $x$ appartenant à $E$, $x * e = e * x = x$ ; en symboles :*

$$\exists y \in E \, [x \in E \Rightarrow (x * y = y * x = x)] \wedge y = e$$

*ou*

$$e \in E \wedge (x \in E \Rightarrow x * e = e * x = x)$$

REMARQUE 5.2. Qu'on remarque que, d'après la définition de l'élément neutre, si $e$ et $\tilde{e}$ étaient deux éléments neutres de $*$ dans $E$, on aurait : autant $e * \tilde{e} = e$, car $e$ est un élément de $E$, que $e * \tilde{e} = \tilde{e}$, car $\tilde{e}$ est ausi un élément neutre de $E$, donc $e = \tilde{e}$ ; quelle que soit l'opération $*$, tous les éléments neutres de $*$ dans $E$ sont donc égaux, c'est-à-dire qu'ils appartiennent tous à la même classe d'équivalence sous la relation $=$. En général, on exprime cette conséquence de la définition donnée, en disant que, quelle que soit l'opération $*$, il ne peut y avoir dans $E$ qu'un seul élément neutre de $*$.

Le lecteur sera à même de vérifier, sans aucune difficulté, que $< \mathbb{N}, + >$, $< \mathbb{N}, \cdot >$, $< \mathbb{Z}, + >$, $< \mathbb{Z}, \cdot >$, $< \mathbb{Q}, + >$ et $< \mathbb{Q}, \cdot >$ sont tous des monoïdes.

On aura remarqué que parmi les conditions qui définissent un monoïde, on ne fait pas mention de la commutativité de l'opération $*$. En effet celle-ci n'est pas une condition nécessaire.

Si dans un monoïde $< E, * >$, l'opération $*$ est aussi commutative, alors on dit que le monoïde est lui-même *commutatif*.

À ce stade, on peut comprendre, dans les termes généraux de l'algèbre, la nature de la procédure qui nous a conduits, dans les chapitres précédents, de $\mathbb{N}$ à $\mathbb{Z}$ : on disposait d'un monoïde $< E, * >$ qui n'était pas fermé par rapport à l'opération inverse de $*$ — que, généralementisant la notation dite « multiplicative », on note souvent « $*^{-1}$ » — et on a cherché une extension de l'ensemble $E$, apte à produire le plus petit des ensembles contenant $E$ et fermés par rapport à $*^{-1}$ (cette opération étant définie sur le nouvel ensemble de manière compatible avec sa définition sur $E$). Pour ce faire, on est parti de $E$ et, pour tout élément $x$ de $E$, on a ajouté à $E$ un nouvel élément $y$, de manière que $x * y = y * x = e$ ($e$ étant l'élément neutre de $*$ dans $E$). Cela signifie qu'on a ajouté à $E$ un inverse relativement à $*$ de chaque élément du même $E$, et on l'a fait en sorte que ce dernier élément de $E$ puisse être traité à son tour comme l'inverse de son inverse. De cette manière, on a obtenu un ensemble où tout élément (ancien et nouveau) possède un inverse relativement à $*$ — ou, comme on le dit généralement, est inversible relativement à $*$. En procédant ainsi, on est passé d'un monoïde à une nouvelle structure algébrique qu'on appelle « groupe » : un monoïde $< E, * >$ dans lequel tout élément de $E$ possède un inverse (relativement à $*$). Voici alors la définition d'un groupe, que le lecteur n'aura aucune difficulté à imaginer :

Définition 1.3. *On appelle « groupe » un monoïde $< E, * >$ où tout élément de $E$ est inversible relativement à l'opération $*$ , c'est-à-dire un couple $< E, * >$ composé par un ensemble $E$ quelconque et une loi de composition interne associative et unitaire $*$, définie sur les éléments de $E$, par rapport à laquelle tout élément de $E$ est inversible. En d'autres termes, un couple $< E, * >$ est un groupe si et seulement si :*

- **(*i*):** *pour tout $x$ et $y$ appartenant à $E$, $x * y$ appartient à $E$ ;*
- **(*ii*):** *pour tout $x$, $y$ et $z$ appartenant à $E$, $(x * y) * z = x * (y * z)$ ;*
- **(*iii*):** *il y a dans $E$ un et un seul élément $e$ (dit « élément neutre de $*$ » ), tel que pour tout $x$ appartenant à $E$, $x * e = e * x = x$ ;*
- **(*iv*):** *pour tout $x$ appartenant à $E$, il y a dans $E$ un (et un seul) élément $y_{x,*}$ (dit « élément inverse de $x$ relativement à $*$ » ), tel que $x * y_{x,*} = y_{x,*} * x = e$ ; en symboles :*

$$x \in E \Rightarrow (\exists! y \in E, [x * y = y * x = e] \wedge y = y_{x,*})$$

Remarque 5.3. Le lecteur est invité à observer la différence entre la nature logique de la clause (*iii*) et la nature logique de la clause (*iv*) dans la définition 1.3. La première de ces clauses stipule l'existence d'un objet $x$ qui se comporte d'une certaine manière vis-à-vis de tous les objets $y$ d'un ensemble donné. Cet objet est donc fixé indépendamment de la considération de l'élément $y$ avec lequel il opère à chaque fois, c'est-à-dire qu'il est indépendant de lui et il est donc le même, quel que soit $y$. Cela serait le cas même si la clause (*iii*) ne stipulait pas l'unicité de $x$. On peut en fait avoir plusieurs objets $x$ qui se comportent tous de la même manière vis-à-vis de chaque élément $y$ de l'ensemble considéré. La clause (*iv*) stipule par contre l'existence, pour chacun des objets $x$ de l'ensemble considéré, d'un objet $y$ qui se comporte d'une certaine manière vis-à-vis de cet objet. L'objet $y$ qui satisfait à cette condition dépend donc du choix de $x$ et il n'est pas nécessairement le même quel que soit $x$. Dans le langage habituelle de la logique moderne, cette différence est exprimée en écrivant respectivement

$$\exists y \, [\mathcal{A}(x) \Rightarrow \mathcal{B}(x, y)]$$

ou, en utilisant le quantificateur « $\forall$ » qu'on a évité jusqu'ici,

$$\exists y \forall x \left[\mathcal{B}(x, y)\right]$$

pour la première condition, et

$$\mathcal{A}(x) \Rightarrow \exists y \left[\mathcal{B}(x, y)\right]$$

ou

$$\forall x \exists y \left[\mathcal{B}(x, y)\right]$$

pour la seconde. La différence entre ces deux sortes de conditions est essentielle et, si on ne la remarque pas, on n'arrive pas à faire de distinction entre de nombreuses situations mathématiques, et pas exclusivement mathématiques, fort différentes. Après tout, il y a une grande différence entre une communauté d'individus, où il y a un individu qui peut juger tous les autres, et une autre communauté d'individus où chaque individu peut-être jugé par un autre individu de la communauté. Dans un sens, c'est la différence entre une dictature et une démocratie. Ne pas voir cette différence, ou ne pas être en condition de l'exprimer, signifie s'empêcher à jamais de tenir un discours politique doué de sens.

NOTE HISTORIQUE 5.1. Lorsqu'on analyse un cas concret, et qu'on s'interroge sur l'existence, parmi les objets d'un certain domaine, d'un objet qui satisfait à une certaine condition relationnelle, il est généralement facile de distinguer entre l'existence d'un objet satisfaisant à cette condition vis-à-vis de tous les objets du domaine — ce qu'on pourra appeler « existence inconditionnée » —, et l'existence, pour tout objet du domaine, d'un objet satisfaisant à cette condition vis-à-vis de cet objet — ce qu'on pourra dire, en revanche, « existence conditionnée ». Dans l'histoire de la pensée, on n'a aucune mémoire, à ce que je sache, d'une confusion entre ces deux circonstances fort différentes : dans la logique d'Aristote, pour tout énoncé il y a un énoncé contradictoire, mais Aristote ne pensa jamais qu'il y a un énoncé qui est le contradictoire de tout énoncé ; Descartes savait bien, pour ne prendre qu'un autre exemple, que toute équation de premier degré à coefficients réels a une racine réelle, mais il ne fut jamais sur le point d'affirmer l'existence d'un nombre réel qui soit racine de toute équation de premier degré à coefficients réels. La capacité de distinguer entre ces circonstances est une condition préalable à tout exercice de la rationalité.

Cette capacité de distinction, pour ainsi dire *in concreto*, ne s'accompagna pas, pourtant, pendant très longtemps, de la capacité de distinguer, généralement, entre deux formes logiques distinctes, correspondant respectivement à une existence inconditionnée et à une existence conditionnée. L'acquisition d'un langage et d'un outillage logique qui permet d'exprimer généralement cette différence et de la reconnaître à coup sûr, en ne se réclamant que de la forme logique de l'énoncé qui exprime une condition d'existence, fut une acquisition assez tardive, qui ne date que de la deuxième moitié du XIX$^{\text{ème}}$ siècle. Cette acquisition correspond, pour l'essentiel, à la naissance de la théorie de la quantification et à la codification de ce que nous reconnaissons aujourd'hui comme une quantification enchaînée, ce qui n'est rien d'autre que l'introduction d'un quantificateur, universel ou existentiel, dans le domaine d'action d'un autre quantificateur. Dans le langage de la théorie de la quantification, la différence entre existence inconditionnée et existence conditionnée se réduit, ainsi à une différence dans l'ordre d'enchaînement de deux quantificateurs, respectivement universel et existentiel. En posant d'abord le quantificateur existentiel et après le quantificateur universel, comme dans un énoncé de la forme « $\exists x \forall y \ldots$ » (de sorte

que le quantificateur existentiel agit sur l'universel), on exprime une existence inconditionnée ; en posant, en revanche, d'abord le quantificateur universel et après le quantificateur existentiel, comme dans un énoncé de la forme « $\forall x \exists y \ldots$ » (de sorte que le quantificateur universel agit sur l'existentiel), on exprime une existence conditionnée.

Les traités mathématiques du XVIII$^{\text{ème}}$ siècle contiennent, par exemple, beaucoup de formulations ambiguës de conditions d'existence, et aussi de descriptions de certaines circonstances mathématiques utilisant des formulations qui, selon les normes logico-linguistiques modernes, renvoient à une forme d'existence distincte de celle qui *de facto* est en revanche propre à la circonstance considérée. On n'a pourtant pas de souvenirs de cas particuliers dans lesquels cette ambiguïté dans l'exposition conduisit à des erreurs mathématiques majeures. Souvent, on cite comme une erreur induite par une confusion de cette nature, une célèbre démonstration, évidemment erronée, d'une proposition fausse que Cauchy énonça comme un théorème dans son *Cours d'Analyse*, en 1821 (sur Cauchy et le *Cours d'Analyse*, cf. la note historique 6.7). L'explication de la nature mathématique de l'erreur de Cauchy — qui assigna à toute série convergente de fonctions continues une propriété (la convergence à une fonction, à son tour, continue) qui n'est en revanche propre qu'à une classe particulière de séries convergentes de fonctions continues, dites « uniformément convergentes » — demanderait l'introduction de notions mathématiques qui, sans être d'une difficulté particulière, n'entrent pas dans le programme de mon exposé. Il suffira d'observer que, s'il est certainement vrai que, en bonne logique moderne, la différence entre une série convergente et une série uniformément convergente correspond à la différence entre l'ordre d'enchaînement de deux quantificateurs dans les énoncés exprimant respectivement ces deux conditions, il est vrai aussi que l'erreur de Cauchy tient, plus qu'à une inversion de la quantification, à la non disponibilité d'un langage et d'une conceptualisation mathématiques aptes à réduire la notion de convergence à une condition d'existence ; lorsque Seidel entrevit, le premier, cette possibilité, en 1849, la distinction entre convergence et convergence uniforme, et l'erreur dans la preuve de Cauchy, apparurent immédiatement. Le lecteur comprendra mieux cette observation en comparant, lors de la lecture du paragraphe 2, l'énonciation informelle de la propriété de convergence d'une suite ou d'une série (où il ne sera question que de l'approche indéfinie d'une suite de nombres vers un nombre donné) à l'énonciation formelle de cette propriété (qui fera justement intervenir une quantification enchaînée). Il devra pourtant observer que, dans le paragraphe en question, et partout ailleurs dans le présent livre, il ne sera question que de suites et de séries de constates et non pas de fonctions. La différence qui est responsable de la distinction entre convergence et convergence uniforme (qui ne concerne que suites et séries de fonctions) ne peut donc pas être observée à partir des définitions énoncées dans un tel paragraphe.

**Lectures possibles** : W. and M. Kneale *The Development of Logic*, Clarendon Press, Oxford, 1962 ; E. Giusti, « Gli errori di Cauchy e i fondamenti dell'analisi », *Bollettino di storia delle scienze matematiche*, 4, 1984, pp. 24-54.

Encore une fois, la condition de commutativité n'est pas demandée. Si $< E, * >$ est un groupe et $*$ une opération commutative sur $E$, alors on dit que le groupe est lui-même *commutatif*, ou *abélien*, en l'honneur du mathématicien suédois Niels H. Abel qui étudia, le premier, des sortes de groupes commutatifs, dans la première moitié du XIX$^{\text{e}}$ siècle.

NOTE HISTORIQUE 5.2. Imaginons que les symboles « $A_i$ » ($i = 0, 1, 2, \ldots, n-1$) désignent les éléments d'un ensemble **K** fermé par rapport à l'addition, la multiplication, la soustraction et la division définies sur cet ensemble, exception faite pour la division par l'élément neutre de l'addition. Dans le paragraphe 3 on verra que ceci est toujours le cas si **K** est un corps. Sans entrer dans d'autres détails, on supposera ici que **K** est un corps, en observant que, pour le fait d'être un corps, **K** est un ensemble qui a la propriété de quadruple fermeture qu'on vient d'indiquer. Imaginons encore qu'on pose la condition

$$x^n + A_{n-1}x^{n-1} + \ldots + A_1 x + A_0 = 0$$

où $n$ est un nombre naturel différent de zéro, et qu'on demande s'il y a un élément $x$ de **K** qui satisfait à cette condition, et, si la réponse est positive, qu'on demande de déterminer cet élément, ou, s'il y en a plusieurs, ces éléments, et, si elle est négative, qu'on demande comment on doit étendre **K** pour obtenir un ensemble qui contient un ou plusieurs éléments qui satisfont à cette condition. On dira qu'il s'agit de résoudre une équation algébrique dans **K**. La réponse qu'aujourd'hui nous donnons à ces questions, lorsque $n$ n'est pas plus grand que 2 et **K** est soit l'ensemble des nombres rationnels, soit l'ensemble des nombres réels (cf. le chapitre 6), se réclame de connaissances qui, pour l'essentiel, étaient déjà en possession des mathématiciens grecs. Au XVI$^{\text{ème}}$ siècle différents mathématiciens italiens (Scipione del Ferro, puis Tartaglia, Cardano et Ferrari) firent des découvertes qu'aujourd'hui nous utilisons pour répondre à ces questions lorsque $n$ n'est pas plus grand que 4 et que **K** est soit l'ensemble des nombres rationnels, soit l'ensemble des nombres réels.

En 1637, dans le troisième livre de la *Géométrie*, Descartes fit une affirmation, en soi-même assez obscure, mais qu'on pourrait interpréter ainsi (la même interprétation, *mutatis mutandis*, fut donnée par les mathématiciens postérieurs à Descartes) : si **K** est l'ensemble des nombres réels, alors, quel que soit le nombre naturel strictement positif $n$, il y a une extension de **K**, dite « ensemble des nombres imaginaire » qui contient $n$ éléments (non nécessairement distincts) qui satisfont à la condition précédente, dits « racines » de l'équation donnée. C'est la première formulation d'un théorème qui deviendra ensuite connu sous le nom de « théorème fondamental de l'algèbre » (cf. la note 4.6).

On savait que si $n$ n'est pas plus grand que 4 et **K** est l'ensemble des nombres réels (cf. le chapitre 6), alors l'extension de **K** qui contient les $n$ racines de l'équation donnée est constituée par l'ensemble de toutes les additions de la forme $a + b\sqrt{-1}$, où $a$ et $b$ sont des nombres réels et $\sqrt{-1}$ est tel (comme on l'a vu dans la note historique 4.6) que $(\sqrt{-1})^2 = -1$. Entre 1637 et le début du XIX$^{\text{ème}}$ siècle beaucoup de mathématiciens essayèrent de montrer que ceci est le cas, quelle que soit la valeur de $n$. Comme une addition de la forme « $a + b\sqrt{-1}$ » est dite « nombre complexe », cela revient à montrer que l'affirmation de Descartes est correcte et que l'ensemble des nombres imaginaires coïncide avec l'ensemble des nombres complexes : c'est, en simplifiant, la version moderne du théorème fondamental de l'algèbre qui fut enfin démontré de manière satisfaisante par Gauss et Cauchy.

En 1799, le mathématicien italien P. Ruffini avait entre-temps crut pouvoir démontrer que si $n$ est plus grand que 4, les racines complexes de l'équation donnée n'étaient pas, généralement, sauf cas particuliers dûs à des choix heureux des coefficients $A_i$, des fonctions algébriques de ces coefficients, c'est-à-dire qu'elles ne pouvaient pas être

obtenues en combinant ces coefficients entre eux par addition, multiplication, soustraction, division et extraction de racine. Dans deux mémoires de 1824 et 1826, un jeune mathématicien norvégien, qui n'avait alors qu'un peu plus de vingt ans, Niels-Henrik Abel, parvint à démontrer la conjecture de Ruffini pour $n$ égal à 5. Pour $n$ plus grand que 5 , la conjecture de Ruffini ne fut démontrée que plus tard, par E. Galois ; on y reviendra dans la note historique 5.5.

En revanche, dans un nouveau mémoire de 1829, le même Abel démontra un théorème positif, caractérisant une classe d'équations dont les racines peuvent être exprimées par des fonctions algébriques des coefficients de ces mêmes équations. D'après le théorème démontré par Abel, pour que ceci soit le cas, il suffit que toutes les racines de l'équation donnée puissent être exprimées par des fonctions rationnelles d'une de ces racines (c'est-à-dire qu'elles puissent être obtenues en opérant par addition, multiplication, soustraction et division à partir de cette racine), et que si $x$ est cette dernière racine et $y = \phi(x)$ et $z = \psi(x)$ sont deux autres racines quelconques de cette équation ($\phi(x)$ et $\psi(x)$ étant justement des fonctions rationnelles de $x$), alors

$$\phi(z) = \psi(y)$$

c'est-à-dire :

$$\phi(\psi(x)) = \psi(\phi(x))$$

Comme on le verra plus tard, si $t = f(v)$ est une fonction de $v$ et que $v$ est à son tour une fonction de $w$, c'est-à-dire qu'on a $v = g(w)$, alors on peut parvenir à $t$ en partant de $w$, d'abord en passant de $w$ à $v$ par le biais de l'association indiquée par la fonction $g$ et ensuite en passant de $v$ à $t$ par le biais de l'association indiquée par la fonction $f$. On dira alors que $t$ est une fonction de $w$ et que la fonction qui lie $t$ à $w$ résulte des fonctions $f$ et $g$ par composition. La composition ainsi définie est donc une opération sur les fonctions, et, si on choisit convenablement un ensemble de fonctions, cette opération peut être une loi de composition interne. La deuxième des conditions sur lesquelles porte le théorème d'Abel nous dit alors que la composition définie sur les fonctions rationnelles, qui lient toutes les racines de l'équation donnée à une de ces mêmes racines, doit être commutative. C'est pour honorer la mémoire de ce théorème et du mathématicien qui le démontra le premier qu'on appelle aujourd'hui « abélien » un groupe dont la loi de composition interne est justement commutative.

**Lectures possibles** : B. L. van der Warden, *A History of Algebre*, Springer, Berlin, Heidelberg, New York, Tokyo, 1985.

* * *

Le mémoire d'Abel de 1829 fut expédié à Berlin, à A. L. Crelle — le directeur de la revue dans laquelle il parut plus tard — le 6 janvier 1829, de Fröland en Norvège, où Abel s'était rendu, après un long voyage dans le froid, pour passer Noël avec sa fiancée Crelly. À Fr ?land, Abel savait pouvoir trouver une maison confortable et jouir de la compagnie de Crelly et de sa famille. Sa situation à Oslo était bien différente.

Il était rentré en Norvège au mois de mai 1827, après un long voyage en Europe, où, grâce à une bourse que le gouvernement norvégien lui avait octroyé pour l'extraordinaire propension qu'il avait montrée pour les études mathématiques, il avait rencontré les plus importants mathématiciens du continent. Durant ce voyage, il avait séjourné surtout à Paris et à Berlin. Assez déçu par le milieu parisien, dominé à l'époque par le génie, mais aussi par l'arrogance et la malhonnêteté de Cauchy (cf.

la note historique 6.5), Abel avait en revanche trouvé son bonheur à Berlin, où il s'était lié en particulier d'une amitié très profonde avec Crelle. Dans le journal que ce dernier venait de fonder et qui, en partie grâce aux contributions d'Abel, fut pendant quelques années un des grands lieux de la recherche mathématique, Abel avait commencé à publier des mémoires qui lui valurent l'admiration inconditionnée des plus grands mathématiciens de l'époque. Quand, sa bourse arrivée à son terme, il rentra à Oslo, la réputation qu'il avait acquise dans le continent, ne fut guère suffisante pour convaincre les autorités locales de lui octroyer une position académique ou un salaire avec lequel il aurait pu vivre. Une autre bourse lui fut refusée pour des raisons administratives (les mêmes auxquelles se heurtent souvent les étudiants de nos universités). Issu d'une famille très pauvre, il ne pouvait pas se permettre de ne pas gagner sa vie. Il commença une vie très sobre et solitaire, vivant de travaux temporaires, soulagée seulement par les voyages à Fröland. Sa santé en fut bientôt atteinte. Crelle, entre-temps, était en train de travailler pour lui trouver une position académique à Berlin et, le cas échéant, pour convaincre le gouvernement norvégien qu'il fallait reconnaître le génie de Abel et lui donner un salaire.

Le 9 janvier 1829 Abel devait quitter Fröland, pour retourner à Oslo. Mais il fut victime d'une forte hémorragie qui se révéla bientôt être le symptôme d'une tuberculose. Il ne repartit jamais pour Oslo, car le 6 avril 1829, il mourut à Fröland. Il était né sur l'île de Finnöy dans la famille d'un pasteur luthérien, le 5 août 1802 ; il n'avait donc pas encore vingt-sept ans. Le 8 avril, Crelle, qui ne savait pas encore la mort de son protégé, lui écrivit une lettre enthousiaste, où il lui annonçait que le ministère allemand de l'instruction publique avait finalement accepté de lui payer un salaire et de l'accueillir à Berlin. Les efforts de Crelle pour sauver la vie d'un mathématicien extraordinaire avaient atteint leur but ; mais, ils l'avaient atteint deux jours trop tard.

**Lectures Possible** : O. Ore, *Abel, un mathématicien romantique*, Belin, Paris, 1989.

Le lecteur ne sera pas surpris de vérifier que $< \mathbb{N}, + >$ n'est pas un groupe, tandis que $< \mathbb{Z}, + >$ est un groupe et qu'il est même abélien.

Remarque 5.4. La définition du groupe étant posée, raisonnons un instant sur les relations entre la condition de fermeture et celle d'inversibilité. On vient de dire que pour passer de $\mathbb{N}$ à $\mathbb{Z}$, on a ajouté à l'ensemble donné autant d'éléments qu'il était nécessaire pour que chaque élément de $\mathbb{N}$ possédât dans le nouvel ensemble ainsi construit, un inverse par rapport à $+$, et qu'on l'a fait de manière à garantir le caractère symétrique de la relation 'être un inverse de'. Or, en procédant de cette manière, on a obtenu un ensemble fermé par rapport à l'opération inverse de l'addition. La question est alors la suivante : serait-il possible que les choses n'en aillent pas ainsi ? pour être plus précis : peut-on imaginer un ensemble $E$, dont tous les éléments soient inversibles relativement à l'opération $*$, qui soit ouvert par rapport à cette opération ? La réponse est clairement positive. L'ensemble $\left\{1, 2, \frac{1}{2}, 3, \frac{1}{3}, 4, \frac{1}{4}, ...\right\}$ est par exemple un ensemble dont tous les éléments ont un inverse relativement à la multiplication, mais qui n'est guère fermé relativement à la division. Pourtant, il est clair que cet ensemble n'est pas fermé non plus par rapport à la multiplication, car si $p$ et $q$ sont deux nombres naturels, tels qu'il n'y a pas de nombre naturel $n$, tel que $p = nq$, alors cet ensemble ne contient ni le produit $\frac{1}{p} \cdot q = \frac{q}{p}$, ni le quotient $\frac{1}{p} : \frac{1}{q} = \frac{q}{p}$, bien que $q$, $\frac{1}{p}$ et $\frac{1}{q}$ appartiennent à cet ensemble. Il suffit d'observer que dans l'ensemble $\mathbb{Q}_+^* = \mathbb{Q}^+ - \{0\}$, qu'on obtient en éliminant de $\mathbb{Q}^+$ l'élément 0, le produit $\frac{1}{p} \cdot q$ et le quotient $\frac{1}{p} : \frac{1}{q}$ coïncident pour supposer que c'est le cas général : un ensemble $E$, qui admet un (et un seul) élément neutre pour une

opération associative $*$, dont tous les éléments possèdent un et un seul inverse relativement à $*$, est fermé par rapport à l'opération inverse $*^{-1}$ si et seulement s'il est fermé relativement à $*$. Il n'est pas difficile de démontrer ceci en général.

Imaginons que $x, y \in E$, qu'on ait défini sur $E$ une opération associative $*$ par rapport à laquelle $E$ est fermé (c'est-à-dire que $*$ est une loi de composition interne associative sur $E$), que $E$ admette un (et un seul) élément neutre de $*$, disons $e$, et que pour chaque élément $x$ de $E$, il y ait en $E$ un et un seul inverse de $x$ par rapport à $*$. Alors, si on note par « $x^{-1}$ » l'inverse de $x$ et par « $y^{-1}$ » l'inverse de $y$ relativement à $*$, on en conclura que $x^{-1}$, $y^{-1}$ et $x^{-1} * y^{-1}$ sont des éléments de $E$, de même que $y * x$ et $(x^{-1} * y^{-1}) * (y * x)$. Mais $*$ étant associative en $E$, on aura

$$\begin{aligned}(x^{-1} * y^{-1}) * (y * x) &= \big[(x^{-1} * y^{-1}) * y\big] * x \\ &= \big[x^{-1} * (y^{-1} * y)\big] * x \\ &= \big(x^{-1} * e\big) * x = x^{-1} * x = e\end{aligned}$$

donc $x^{-1} * y^{-1}$ est l'inverse de $y * x$, de sorte que

$$(y * x)^{-1} = x^{-1} * y^{-1}$$

ou bien

$$(y * x)^{-1} *^{-1} x^{-1} = y^{-1} \tag{51}$$

Mais, quel que soit $x \in E$, tout élément $z$ de $E$ peut s'écrire sous la forme $(y * x)^{-1}$. Il suffit pour cela de poser $y = z^{-1} * x^{-1}$, ce qui, grâce à l'associativité de $*$, donne justement

$$\begin{aligned}(y * x)^{-1} &= \big[\big(z^{-1} * x^{-1}\big) * x\big]^{-1} \\ &= \big[z^{-1} * \big(x^{-1} * x\big)\big]^{-1} \\ &= \big[z^{-1} * e\big]^{-1} = \big(z^{-1}\big)^{-1} = z\end{aligned}$$

Ainsi l'égalité (51) nous dit que le résultat de l'application de $*^{-1}$ à deux éléments quelconques de $E$ est encore un élément de $E$. Si donc l'ensemble $E$ est fermé relativement à l'opération associative $*$, il est aussi fermé relativement à l'opération inverse $*^{-1}$, et comme $*$ est l'opération inverse de $*^{-1}$, cela entraîne la réciproque. La conclusion est donc simple : parmi les conditions qu'un couple $< E, * >$ doit respecter pour être un groupe, il y a aussi, implicitement, celle que l'ensemble $E$ soit fermé relativement à $*^{-1}$, c'est-à-dire que autant $*$ que $*^{-1}$ soient des lois de composition internes sur $E$.

La notion de groupe recouvre donc parfaitement le caractère de l'ensemble $\mathbb{Z}$, qu'on a construit en partant de $\mathbb{N}$, en tant qu'extension minimale de cet ensemble fermée relativement à la soustraction. Et le résultat précédent nous permet de surcroît de comprendre la raison générale pour laquelle la différence entre addition et soustraction semble disparaître dans $\mathbb{Z}$. En fait si $< E, * >$ est un groupe, $x, y \in E$, et $y^{-1}$ est l'inverse de $y$ relativement à $*$, alors $x *^{-1} y = x * y^{-1}$. Ainsi dans un groupe, il revient au même, pour ainsi dire, de faire opérer $y$ avec $x$ par $*^{-1}$, ou de faire opérer $y^{-1}$ avec $x$ par $*$.

Avant de conclure la présente remarque, il me semble utile d'ajouter deux observations ultérieures, D'abord, il faut observer que, bien qu'on ait utilisé ici la notation multiplicative, en notant par « $*^{-1}$ » l'opération inverse de $*$ et par « $x^{-1}$ » l'élément inverse de $x$ par rapport à $*$, l'opération $*$ doit être conçue comme parfaitement quelconque, et rien ne nous oblige à l'assimiler à une multiplication sur $E$, de sorte que si $E = \mathbb{Z}$, rien nous dit, par exemple, que $x^{-1} = \frac{1}{x}$. On voit d'ailleurs que si ceci était le cas, $\mathbb{Z}$ ne serait pas fermé par rapport à $*$.

Je voudrais ensuite attirer l'attention du lecteur sur le rôle essentiel que la condition d'associativité de $*$ joue dans l'argument précédent. Cet argument montre de ce fait une des raisons qui font que dans la définition d'un groupe on demande d'emblée l'associativité de $*$ : il s'agit justement de garantir que la fermeture de $E$ par rapport a $*$ implique la fermeture de $E$ par rapport à l'opération inverse de $*$.

Revenons à présent à la procédure qui nous a conduits de $\mathbb{N}$ à $\mathbb{Q}^+$. Elle diffère de celle qui nous a conduits de $\mathbb{N}$ à $\mathbb{Z}$ sur un aspect essentiel. Pour passer de $\mathbb{N}$ à $\mathbb{Q}^+$, on n'a pas ajouté un nouvel élément pour chaque élément de $\mathbb{N}$ ; on a plutôt ajouté un nouvel élément à $\mathbb{N}$ pour chaque couple ordonné $(x, y)$ d'éléments de $\mathbb{N}$ tel que $y \neq 0$. Donc on n'a pas cherché d'emblée un inverse relativement à $\cdot$ pour chaque élément de $\mathbb{N}$, différent de 0, ce qui ne nous aurait conduit qu'à l'ensemble $\left\{0, 1, \frac{1}{1}, 2, \frac{1}{2}, 3, \frac{1}{3}, 4, \frac{1}{4}, ...\right\}$ qui, comme on vient de le voir, n'est fermé ni par rapport à la multiplication, ni par rapport à la division. Ainsi, on a été forcé d'agir différemment : d'abord, en acceptant d'emblée l'idée que 0 ne serait le diviseur d'aucun élément du nouvel ensemble ; ensuite, en ajoutant directement à $\mathbb{N}$ un élément pour chaque division qui restait ainsi possible entre les éléments de $\mathbb{N}$. De cette manière, on n'a pas seulement construit un ensemble dont chaque élément différent de 0 admet un inverse par rapport à la multiplication, mais on a plutôt construit un ensemble, tel que, si l'élément 0 est éliminé, l'ensemble qui en résulte est fermé par rapport à la division et donc aussi à la multiplication. On pourra observer, en effet, que le couple $< \mathbb{Q}_+^*, \cdot >$ est encore un groupe, de même que les couples $< \mathbb{Q}, + >$ et $< \mathbb{Q} - \{0\}, \cdot >$, tandis que les couples $< \mathbb{Q}^+, \cdot >$ et $< \mathbb{Q}, \cdot >$ ne sont pas des groupes, car l'élément 0 de $\mathbb{Q}^+$ et $\mathbb{Q}$ n'admet pas d'inverse par rapport à $*$ et ces structures ne satisfont donc pas à la clause $(iv)$ de la définition 1.3.

La signification profonde de cette situation sera claire plus tard, quand on introduira les notions d'anneau et de corps. Pour l'instant, cherchons à comprendre plus en général la notion de groupe.

Remarque 5.5. Avant d'introduire quelques définitions ultérieures et quelques exemples qui devraient servir au lecteur pour commencer à se familiariser avec la notion de groupe, il est nécessaire d'observer que l'intérêt mathématique de cette notion, ainsi que de celles d'anneaux et de corps qu'on étudiera plus loin, ou de n'importe quel autre notion identifiant une structure algébrique, réside essentiellement dans sa généralité. Ce n'est pas simplement parce qu'elle rend compte de la nature logique de $\mathbb{Z}$ ou de $\mathbb{Q}$, ou parce qu'elle permet de caractériser plus précisément la procédure constructive qui conduit de $\mathbb{N}$ à $\mathbb{Z}$ ou à $\mathbb{Q}$ que la notion de groupe s'est imposée aux mathématiciens. Ce qui fait tout son intérêt mathématique est le fait qu'elle exprime la forme commune d'une grande variété de structures relationnelles qu'on rencontre en mathématiques.

Note Historique 5.3. Si vous allez un jour à Nancy, ou, encore mieux, si vous y êtes, vous pouvez chercher la statue d'un général, Charles-Denis Sauter Bourbaki, qui prit part à la guerre franco-prussienne, dont une grande partie se déroula en Lorraine. Nancy est la ville où naquit Poincaré et certes, tout jeune mathématicien français des années trente se rendit un jour ou l'autre à Nancy. Le général Bourbaki ne s'appelait pas « Nicolas ». Pour une raison qui ne fut jamais éclaircie tout à fait, le nom « Nicolas Bourbaki » fut en revanche choisi comme pseudonyme par un groupe de mathématiciens français qui, à partir de 1939, commencèrent à publier des fascicules, dans la série *Actualités scientifiques et industrielles*, qui paraissait à l'époque aux éditions Hermann, dont la collection devait former plus tard un immense ouvrage collectif, aujourd'hui universellement connu comme les *Éléments de mathématiques* de Bourbaki. La composition du groupe Bourbaki varia selon les époques, même si H.

Cartan, C. Chevalley, J. Dieudonné et A. Weil en sont unanimement reconnus comme les fondateurs. L'influence que Bourbaki exerça sur les mathématiques non seulement françaises est enorme et difficile à évaluer. Les conceptions « formalistes » de Bourbaki, autant pour ce qui concerne la recherche que pour ce qui concerne l'enseignement des mathématiques ont trouvé et comptent encore nombreuses opposants ; même ceux-ci n'auraient pourtant pas pensé ou ne penseraient pas aujourd'hui les mathématiques de la même manière si les *Éléments* et les autres ouvrages de Bourbaki n'avaient jamais été écrits.

L'idée centrale de Bourbaki est que les mathématiques sont un édifice unitaire et que les liens entre les différentes parties de cet édifice ne peuvent se comprendre qu'à condition d'un effort d'abstraction capable de dégager, derrière les différentes théories qui y interviennent, des structures communes ; ces dernières deviennent, une fois découvertes, à leur tour, des objets d'étude et de recherche. Bien que Bourbaki ait largement utilisé le vocabulaire et les notions fondamentales de la théorie des ensembles, et qu'il se soit fait partisan d'une approche rigoureusement formaliste, il n'a jamais accepté l'idée que la théorie des ensembles, ou plus en général la logique, pouvaient fournir un fondement extérieur pour les mathématiques.

D'ailleur, le formalisme ne fut jamais pour Bourbaki qu'une manière d'atteindre un dégré d'abstraction suffisant pour comprendre et exprimer l'unité profonde de la connaissance mathématique. Une citation, aussi longue que suggestive, devrait servir à comprendre l'esprit de l'entreprise poursuivie par ce mathématicien polycéphale :

« On dit [...] « formalisme » ou « méthode formaliste » ; mais il faut dès le début mettre en garde contre le risque d'une confusion [...]. Chacun sait que le caractère externe des mathématiques est de se présenter sous l'aspect de cette « longue chaîne de raisons » dont parlait Descartes [...]. C'est donc un truisme banal de dire que ce « raisonnement déductif » est un principe d'unité pour la mathématique ; mais une remarque aussi superficielle ne peut certainement rendre compte de l'apparente complexité des diverses théories mathématiques [...]. Le mode de raisonnement par enchaînement de syllogismes n'est qu'un *mécanisme* transformateur, applicable indifféremment à toute sorte de prémisses, et qui ne saurait donc caractériser la nature de celles-ci. En d'autres termes, c'est la *forme* extérieure que le mathématicien donne à sa pensée [...], le *langage* propre à la mathématique ; mais il n'y faut pas chercher autre chose. Codifier ce langage, en ordonner le vocabulaire et en clarifier la syntaxe, c'est faire œuvre fort utile, et qui constitue effectivement une face de la méthode axiomatique [...]. Mais [...] *ce n'en est qu'une face*, et la moins intéressante.

« Ce que se propose pour but essentiel l'axiomatique, c'est précisément ce que le formalisme logique, à lui seul, est incapable de fournir, l'intelligibilité profonde des mathématiques. [...] la méthode axiomatique trouve son point d'appui dans la conviction que, si les mathématiques ne sont pas un enchaînement de syllogismes se déroulant au hasard, elles ne sont pas davantage une collection d'artifices plus ou moins « astucieux » [...]. Là où l'observateur superficiel ne voit que deux ou plusieurs théories en apparence très distinctes [...], la méthode axiomatique enseigne à rechercher les raisons profondes de cette découverte, à trouver les idées communes enfouies sous l'appareil extérieur de détails propres à chacune des théories considérées, à dégager ces idées et à les mettre en lumière ».

Cette longue citation est tirée d'un article, « L'architecture des mathématiques », que Bourbaki écrivit pour le célèbre recueil, *Les grands courants de la pensée mathématique*,

que F. Le Lionnais avait préparé, avec tant de difficultés, à l'époque de l'occupation allemande, et dont le projet l'avait accompagné au camp de concentration de Dora, avant d'aboutir, finalement, en 1948. Pour donner un exemple de la fonction de la méthode axiomatique à laquelle fait allusion la citation précédente, Bourbaki se réclame justement de la notion de groupe. Cela vaut la peine de lui laisser encore la parole :

« Considérons [...] les trois opérations suivantes : 1) l'addition des nombres réels [cf. le chapitre 6, mais, pour la suite de l'argument, on pourrait se limiter aux nombres rationnels] [...] ; 2) la multiplication des entiers « modulo un nombre premier » [cf. la suite du présent chapitre] [...] ; 3) la « composition » des déplacements dans l'espace euclidien à trois dimensions [cf. la note historique 5.4]. Dans chacune de ces trois théories, à deux éléments $x$, $y$ (pris dans cet ordre) de l'ensemble d'éléments considéré [...] on fait correspondre (par un procédé particulier à la théorie) un troisième élément bien déterminé, que nous conviendrons de désigner symboliquement dans les trois cas par $x \tau y$ [...]. Si maintenant on examine les propriétés de cette « opération » dans chacune des trois théories, on constate qu'elles présentent un remarquable parallélisme ; mais à l'intérieur de chacune de ces théories, ces propriétés dépendent les unes des autres, et une analyse de leurs connexions logiques amène à en dégager un petit nombre qui, elles, sont indépendantes (c'est-à-dire qu'aucune n'est conséquence logique de toutes les autres). On peut, par exemple, prendre les [...] suivantes [...] [suivent les conditions qui caractérisent un groupe]. On constate alors que les propriétés qui sont susceptibles de s'exprimer de la même manière dans les trois théories, à l'aide de la notation commune, sont des conséquences des [...] précédentes. »

Voici expliqué ce qu'est un groupe : une structure abstraite qui exprime la forme commune de plusieurs théories mathématiques ; dit en d'autres termes : l'expression formelle de ce que Bourbaki appelait « l'unité intrinsèque des mathématiques ».

**Lectures possibles** : F. Le Lionnais (éd.), *Les grands courants de la pensée mathématique*, Cahiers du sud, Paris, 1948 (réimpression : Rivages, Paris, Marseille, 1986) ; N. Bourbaki, *Éléments d'histoire des mathématiques*, Hermann, Paris, 1960 (nouv. éd., revue, corrigée et augmentée, 1974).

Remarque 5.6. Plus loin, on présentera les exemples d'un groupe de permutations et des groupes des classes de congruence modulo un nombre naturel quelconque, plus grand que 1. On expliquera de quoi il s'agit le moment venu, ici on peut présenter de manière bien plus rapide et informelle un autre exemple qui permettra au lecteur de comprendre la variété et la différence des objets mathématiques qui présentent la forme d'un groupe.

On imagine disposer d'un segment quelconque, gisant sur un plan euclidien, et d'une procédure apte à le déplacer sur ce plan. Peu importe ici la nature de cette procédure, ce qui est important est qu'elle permette de réaliser un tel déplacement et qu'elle soit indépendante de la position initiale du segment, en sorte qu'elle soit applicable plusieurs fois de suite au même segment qui sera ainsi successivement déplacé d'une position à une autre. On imagine maintenant qu'on dispose d'un moyen pour caractériser la position d'un segment donné dans le plan considéré. Les lecteurs qui sont familiers avec la méthode des coordonnées qui est à l'usage en géométrie analytique n'auront aucune difficulté à imaginer un tel moyen. Pour nos buts actuels, il n'est pourtant pas nécessaire de le spécifier. Posons seulement que si $p$ est la position du segment donné avant le déplacement, alors sa position après le déplacement est donnée par l'image de $p$ selon une application $f : P \to P$, dont les ensembles de départ et d'arrivée sont donnés par l'ensemble $P$ des positions possibles du segment donné sur notre plan. Cette application sera dite « déplacement ». Or, comme une application associe

à chaque élément de son ensemble de départ un et un seul élément de son ensemble d'arrivée, et qu'on peut supposer qu'un segment puisse prendre n'importe quelle position sur notre plan, il est naturel de caractériser l'application $f$ de sorte que : $i$) elle est telle que son ensemble d'arrivée coïncide avec l'image de son domaine, c'est-à-dire qu'elle est surjective ; $ii$) quel que soit la position $p$ qui est donnée, $f(p)$ n'est pas seulement déterminée de manière univoque, mais elle est aussi différente de toute autre position $f(q)$ que le segment aurait pris si on lui avait appliquée le même déplacement à partir d'une position $q$ différente de $p$ c'est-à-dire que $f$ est injective. L'application $f$ sera alors bijéctive.

La situation sera alors la suivante. Si un segment est donné dans une position $p$ quelconque, alors on pourra le déplacer dans n'importe quelle position sur le plan, chacune de ces positions étant caractérisée par une et une seule application bijective $f : P \to P$, dite justement « déplacement ». On imagine alors que $f$ et $g$ soient deux déplacements différents, et que notre segment soit donné dans la position $p$, et qu'on lui fasse subir d'abord le déplacement $f$ qui le conduit de la position $p$ à la position $q = f(p)$, et ensuite le déplacement $g$ qui le conduit de la position $q = f(p)$ à la position $r = g(q) = g(f(p))$. On aura alors composé entre eux deux déplacements. Et comme à la fin du processus on aura déplacé le segment de $p$ à $r$ et que $p$ et $r$ sont deux positions possibles de ce segment, il est naturel de penser que le résultat de cette composition est un nouveau déplacement $h$ qui, appliqué à la position $p$, conduit directement le segment dans la position $r$. Cette composition sera alors une loi de composition interne à l'ensemble de tous les déplacements possibles d'un segment sur un plan. Si on note cette loi par le symbole « $*$ », la composition précédente pourra alors être indiquée par l'opération $g * f = h$. Il est facile de voir que cette loi de composition interne des déplacements d'un segment sur un plan est associative. En effet, si on considère trois déplacements $f, g, h$ appliqués au segment pris dans la position $p$, on aura que la translation $k = (h * g) * f$ conduit le segment de la position $p$ à une position $r$ qu'on détermine ainsi : d'abord on déplace le segment de $p$ à $q = f(p)$, ensuite on le déplace de $q = f(p)$ à $r = \varphi(f(p)) = \varphi(q)$, où $\varphi = h * g$. Or le déplacement $\varphi$ étant composé des déplacements $h$ et $g$ est tel qu'il conduit de la position $q$ à la position $r$ si et seulement si $g$ conduit de la position $q$ à une position $s$ telle que $h$ conduit de la position $s$ à la position $r$, en sorte qu'on aura finalement $r = k(p) = h(g(f(p)))$. D'autre part, le déplacement $\tilde{k} = h * (g * f)$ conduit le segment de la position $p$ à une position $\tilde{r}$ qu'on détermine ainsi : d'abord on déplace le segment de $p$ à $\tilde{s} = \psi(p)$, où $\psi = g * f$, ensuite de $\tilde{s} = \psi(p)$ à $\tilde{r} = h(\psi(p))$. On aura alors $\tilde{r} = h(g(f(p))) = r$ et donc $\tilde{k} = k$, ou bien : $(h * g) * f = h * (g * f)$. Parmi tous les déplacements possibles, il devra y en avoir en outre un, qu'on pourrait noter par le symbole « $e$ », qui laisse inaltérée la position $p$ du segment, en sorte que, quel que soit $p$, $e(p) = p$ et donc, quel que soit le déplacement $f$, $f(e(p)) = e(f(p)) = f(p)$, ou bien $f * e = e * f = f$. L'ensemble des déplacements possibles d'un segment sur notre plan admet alors un élément neutre par rapport à $*$. Finalement, pour tout déplacements $f$ du segment, de la position $p$ à la position $q = f(p)$, il est possible d'imaginer un déplacement $g = f^{-1}$, qui conduit à nouveau le segment de $q = f(p)$ à $p$, en sorte que $p = g(f(p))$, ou bien $g * f = e$. Chaque déplacement de notre segment sur notre plan admet donc un inverse.

Si $D$ est alors l'ensemble des déplacements possibles de notre segment sur notre plan, le couple $< D, * >$ est un groupe. Mais, il est facile de comprendre que les arguments précédents ne dépendent pas de la nature particulière du segment considéré, ni du choix du plan euclidien sur lequel on opère les déplacements. On a démontré ainsi que l'ensemble des déplacements de tout segment sur n'importe quel plan euclidien forme un groupe par rapport à l'opération $*$ définie comme ci-dessus. C'est en généralisant cette observation à d'autres sortes d'objets géomètriques et d'opérations sur ces objets que F. Klein parvient

à une théorie, dite des « groupes de transformations » qui, permît, vers la fin du XIX$^{\text{ème}}$ siécle, de donner un aspect nouveau aux études de géomètrie.

Si la conception de cette théorie fut une des étapes cruciales de l'édification des mathématiques modernes, il est peut-être encore plus important d'observer ici qu'avec le raisonnement précédent on a montré que la nature logique de l'ensemble $\mathbb{Q}$ des nombres rationnels, considéré relativement à la multiplication définie sur ces nombres, est essentiellement la même que la nature logique de l'ensemble $D$ des déplacements de tout segment sur n'importe quel plan euclidien, considéré relativement à l'opération de composition $*$ définie sur ces déplacements. La théorie de ces deux objets, apparemment aussi différents, est donc formellement la même et ne diffère que par l'interprétation qu'on donne des éléments des ensembles considérés et des opérations définies sur eux, ou même, comme on le dit souvent, des symboles qui dénotent ces éléments et ces opérations. Deux théories mathématiques, apparemment aussi diverses et issues d'histoires et d'exigences fort différentes, résultent ainsi unifiées dans une seule théorie.

Note Historique 5.4. Un plan euclidien peut être conçu comme un espace particulier à deux dimensions, un segment tracé sur un plan euclidien n'est à son tour qu'une figure plane fort particulière de la géométrie euclidienne bidimensionnelle, les déplacements d'une figure sur un plan euclidien, peuvent enfin être considérés comme des transformations particulières qu'on fait subir aux figures tracées sur un plan euclidien. Ces simples observations nous font comprendre que la notion de déplacement d'un segment sur un plan euclidien peut être conçue comme une exemplification fort particulière d'une notion bien plus générale, que l'on pourra indiquer par le terme « transformation ».

Pour apprécier dans toute sa généralité la notion de transformation, qui est à la base des idées de Klein, il faut pourtant changer radicalement d'approche par rapport au raisonnement précèdent. Au cours de ce raisonnement, on n'a pas seulement décidé *a priori* de considérer certaines transformations, on a surtout fixé *a priori* la nature des figures géométriques qui subissaient ces transformations et de l'espace dans lequel celles-ci avaient lieu. En un mot, on s'est placé *a priori* dans une certaine géométrie, la géométrie des segments euclidiens tracés sur un seul plan, et on a raisonné à l'intérieur de cette géométrie. L'idée essentielle de Klein fut justement d'invertir l'ordre logique de l'argumentation et d'étudier les différentes géométries possibles, ou, comme on dit souvent, les différents espaces sur lesquels on peut définir une géométrie, à partir d'une classification et d'une étude des différentes transformations possibles de l'espace. La question cruciale, pour comprendre le point de vue de Klein, est donc de savoir comment on doit entendre, avant la spécification d'une géométrie de référence ou toute caractérisation de l'espace dans lequel on est supposé travailler, la notion de transformation de l'espace.

Pendant des siècles, les mathématiciens ont pensé qu'il n'y avait qu'une géométrie (encore maintenant, en « bon français » — c'est-à-dire dans cette langue inflexible, déterminée, cas unique parmi les langues vivantes, par les décrets d'une assemblée de savants —, le terme « géométrie » supporte très mal d'être mis au pluriel). La géométrie était en effet pensée comme la théorie des figures spatiales et son unicité dérivait de l'unicité de l'espace. La naissance des géométries non euclidiennes et la découverte de la possibilité de penser ces géométries, et donc aussi la géométrie euclidienne, comme des théories d'espaces particuliers, ne fut qu'un des épisodes majeurs qui conduisirent, dans la deuxième moitié du XIX$^{\text{ème}}$ siècle, à concevoir une

géométrie comme une théorie possible d'une structure reconnaissable comme un espace. D'un autre côté, la généralisation, de la part, entre autres, d'Arthur Cayley, de vieilles idées de Desargues, Pascal et Poncelet, indiquant la possibilité d'étudier une figure géométrique sous des déformations qui, tout en modifiant ses propriétés métriques, en gardaient d'autres caractéristiques essentielles (celles que, informellement, on pourrait caractériser comme des propriétés invariantes par projection), et la naissance successive de la moderne géométrie projective, conduisit à penser les objets habitant un espace comme des invariantes par rapport à certaines opérations, plutôt que comme des configurations stables déterminables dans cet espace.

L'idée de Klein fut alors de définir un espace comme un objet possible d'une transformation globale. Pour en avoir une idée un peu plus concrète, on pourrait le penser comme un ensemble, sur lequel on aura défini des relations convenables, dont les éléments, qu'on pourra appeler « points », pour se souvenir des vieilles idées, peuvent tous changer en même temps de place. Un changement de place de tous les points d'un espace vaudra alors comme une transformation de cet espace. Ceci étant dit, il s'agira alors de penser les transformations non pas comme des opérations possibles sur un espace donné, mais l'espace comme l'objet possible de certaines transformations, et de caractériser ce dernier sur la base des transformations qu'il est supposé pouvoir subir. Pour ce faire, Klein pensa une transformation comme un élément d'un ensemble contenant toute autre transformation, sur lequel il imagina avoir défini une loi de composition interne associative, unitaire et inversible. Il se donna alors, comme objet d'étude, une structure fort générale constituée par le groupe de transformations de l'espace. Son programme, qui devint ensuite célèbre comme « le programme d'Erlangen » — car il fut exposé dans une dissertation que Klein présenta en 1872, « à l'occasion de l'entrée à la Faculté de Philosophie et au Sénat de l'Université d'Erlangen » — consistait dans l'étude des sous-ensembles de l'ensemble des transformations de l'espace, donnant lieu, à leur tour, à des sous-groupes du groupe des transformations de l'espace. La notion de sous-groupe d'un groupe donné sera éclaircie ci-dessous, en général. Pour l'instant, le lecteur ne devrait pas avoir de difficulté à comprendre ce que cela signifie, dans le cas particulier qu'on examine ici. Pour l'aider avec un exemple, on dira que dans ce contexte, on peut penser les déplacements comme des transformations de l'espace caractérisées, entre autres, par le fait que tout ensemble de points formant une certaine configuration dans un espace va former, après une transformation de cette sorte d'un tel espace, la même configuration. Ainsi, le déplacement d'un segment n'est rien qu'une transformation de l'espace qui, en transformant tout l'espace, transforme le sous-ensemble des points de cet espace qu'on reconnaît comme ce segment dans un sous-ensemble transformé qu'on reconnaît encore comme un segment (en l'occurrence comme ce même segment). Il n'est pas difficile de montrer alors que l'ensemble des déplacements, se composant comme on l'a dit ci-dessus, forme un groupe, qui n'est donc qu'un sous-groupe du groupe des transformations de l'espace. Ceci étant dit, il ne sera plus trop difficile de comprendre Klein, lorsqu'il présente de manière très générale, son programme comme suit.

« Faisons [. . .] abstraction de la figure matérielle qui, au point de vue mathématique, n'est pas essentielle, et ne voyons plus dans l'espace qu'une multiplicité à plusieurs dimensions, par exemple, en nous en tenant à la représentation habituelle du point comme élément de l'espace, une multiplicité à trois dimensions. Par analogie avec les

transformations de l'espace, nous pouvons parler des transformations de la multiplicité : elles forment *des groupes*. Mais il n'y a plus, comme dans l'espace, un groupe qui se distingue des autres par sa signification ; un groupe quelconque n'est ni plus ni moins que tout autre. Comme généralisation de la Géométrie se pose ainsi la question générale que voici : *Étant donnés une multiplicité et un groupe de transformations de cette multiplicité, en étudier les êtres au point de vue des propriétés qui ne sont pas altérées par les transformations du groupe* ».

Une géométrie particulière n'est donc, de ce point de vue, que l'étude d'un groupe particulier de transformations de l'espace. C'est une des idées génératrices de la géométrie moderne, entendue non plus comme une théorie mathématique particulière, mais comme une branche des recherches mathématiques.

**Lectures possibles** : F. Klein, *Le programme d'Erlangen. Considérations comparatives sur les recherches géométriques modernes*, préface de J. Dieudonné, postface du Père F. Russo s.j., Gauthier- Villars, Paris, Bruxelles, Montréal, 1974 ; L. Boi, *Le problème mathématique de l'espace*, Springer Verlag, Berlin, Heildelberg, New York, 1995.

* * *

Felix Klein naquit à Düsseldorf, le 25 avril 1849 et mourut à Göttingen, le 22 juin 1925. Après avoir obtenu son baccalauréat au collège de Düsseldorf, il étudia la physique et les mathématiques à l'université de Bonn, où il obtint son doctorat en 1868. Après un court voyage d'études à Paris, interrompu par le début de la guerre franco-prussienne en 1870, il fut nommé lecteur à l'université de Göttingen et, en 1872, professeur à l'université de Erlangen. Lorsqu'il arriva à Erlangen, il avait déjà obtenu plusieurs résultats importants en géométrie. Devenu familier avec les conceptions de Cayley en géométrie projective, et après avoir appris la théorie des groupes du *Traité des substitutions et des équations algébriques* de Camille Jordan, publié à Paris en 1870 — qui fut à l'origine de la première véritable diffusion de cette théorie —, il profita de sa nomination à Erlangen pour rédiger la dissertation dont on a parlé ci-dessus, où il présente un nouveau programme pour le développement des études géométriques. Après avoir quitté l'université de Erlangen, il fut professeur à Munich, de 1875 à 1880, à Leipzig, de 1880 à 1886 et enfin à Göttingen, de 1886 jusqu'à 1913. En 1875, il épousa Anne Hegel, une petite-fille de G. Wilhelm Friedrich Hegel.

Bien qu'il soit surtout célèbre pour son « programme de Erlangen », Klein apporta des contributions importantes à peu près dans toutes les branches des mathématiques, de la théorie des équations algébriques, à la théorie des fonctions réelles et complexes, jusqu'à la physique mathématique et à l'ingénierie. Pendant son séjour à l'université de Göttingen, il fit de cette université le centre d'études mathématiques le plus fécond et influent d'Allemagne.

**Lectures possibles** : R. Tobies, *Felix Klein*, BSB B. G. Teubneur, Leipzig, 1981.

Jusqu'ici, on n'a considéré que des groupes où interviennent des ensembles infinis. Il est pourtant facile de voir que la condition d'infinité de $E$ n'est pas requise pour construire un groupe $< E, * >$. Un exemple simple et immédiat d'un groupe fini est donné par le couple $< \{-1, 1\}, \cdot >$, la multiplication $\cdot$ étant définie sur $\{-1, 1\}$ comme elle est définie sur $\mathbb{Z}$. Il est très facile de vérifier que $< \{-1, 1\}, \cdot >$ est un groupe, car, la multiplication est bien sur

associative, et on a les égalités :

$$\begin{aligned} 1 \cdot 1 &= (-1) \cdot (-1) = 1 \\ -1 \cdot 1 &= 1 \cdot (-1) = -1 \end{aligned}$$

qui vérifient en même temps les conditions $(i)$, ( $iii$), avec $e = 1$, et $(iv)$, avec $y_{1,\cdot} = 1$ et $y_{-1,\cdot} = -1$, de la définition 1.3. Comme la multiplication est dans ce cas commutative, ce groupe est en outre abélien.

Un groupe $< E, * >$ tel que l'ensemble $E$ est fini et contient $n$ éléments, est dit « d'ordre $n$ ». Ainsi $< \{-1, 1\}, \cdot >$ est un groupe abélien d'ordre 2.

Ce groupe est tel que l'ensemble $E = \{-1, 1\}$ qui y intervient est un sous-ensemble de l'ensemble $\mathbb{Z}$, qui est à son tour tel que le couple $< \mathbb{Z}, \cdot >$ est un groupe. On dira alors que $< \{-1, 1\}, \cdot >$ est un sous-groupe de $< \mathbb{Z}, \cdot >$. Plus en général, on dit qu'un groupe $\mathfrak{g}$ est un sous-groupe de $\mathfrak{G}$, si $\mathfrak{g}$ et $\mathfrak{G}$ sont l'un et l'autre des groupes, l'ensemble $\tilde{E}$ qui intervient dans le groupe $\mathfrak{g}$ est un sous-ensemble de l'ensemble $E$ qui intervient dans $\mathfrak{G}$ et l'opération $*$ qui intervient dans les deux groupes est la même (c'est-à-dire qu'elle est définie sur $\tilde{E}$ et sur $E$, de sorte que le résultat de son application à deux éléments quelconques de $\tilde{E}$ est le même que le résultat de son application aux mêmes éléments pris comme des éléments de $E$). Il sera alors facile de vérifier que $< \{1\}, \cdot >$ est en même temps un sous-groupe de $< \{-1, 1\}, \cdot >$ et de $< \mathbb{Z}, \cdot >$, tandis que $< \{-1\}, \cdot >$, qui n'est pas un groupe, n'est un sous-groupe d'aucun groupe.

Or, si $X$ est un sous-ensemble de $E$ et $\mathfrak{G} = < E, * >$ est un groupe, alors l'opération $*$ est définie sur $X$ et y est certainement associative. Imaginons maintenant que $X$ contienne l'inverse relativement à $*$, de chacun de ses éléments $x$. Alors, si $*$ est une loi de composition interne sur $X$ et $x$ appartient à $X$, $x * y_{x,*}$ aussi appartient à $X$. Mais, par définition, autant $x$ que $y_{x,*}$ appartiennent à $E$ et donc, comme $< E, * >$ est un groupe, $x * y_{x,*}$ appartient à $E$ et, comme $y_{x,*}$ est l'inverse de $x$, relativement à $*$, de sorte que $x * y_{x,*} = e$, $E$ contient aussi l'élément neutre $e$ de $*$. Ainsi, si $X \subseteq E$, $< E, * >$ est un groupe, $*$ est une loi de composition interne sur $X$ et $X$ contient l'inverse par rapport à $*$ de chacun de ses éléments, alors $< X, * >$ est certainement un groupe et il est en particulier un sous-groupe de $< E, * >$. Donc : $\mathfrak{g} = < X, * >$ est un sous-groupe d'un groupe $\mathfrak{G} = < E, * >$ si et seulement si $X \subseteq E$ et : $i)$ si $x$ et $y$ appartiennent à $X$, alors aussi $x * y$ appartient à $X$ ; $ii)$ si $x$ appartient à $X$, alors aussi l'inverse $y_{x,*}$ de $x$ par rapport à $*$ appartient à $X$. Il est facile de vérifier que $< \{-1, 1\}, \cdot >$ et $< \{1\}, \cdot >$ respectent ces conditions par rapport à $< \mathbb{Z}, \cdot >$, tandis que $< \{-1\}, \cdot >$ ne les respecte pas.

On imagine maintenant que $Y$ est un sous-ensemble fini ou dénombrable d'un ensemble $E$ qui intervient dans un groupe $\mathfrak{G} = < E, * >$. Rien n'empêche qu'il y ait des sous-groupes de $\mathfrak{G}$, tels que l'ensemble qui intervient en eux inclue $Y$ comme sous-ensemble. L' intersection de tous ces sous-groupes (c'est-à-dire le couple $< E_Y, * >$ , tel que l'ensemble $E_Y$ est l'intersection de tous les ensembles $\tilde{E}$, tels que $Y \subseteq \tilde{E}$ et $< \tilde{E}, * >$ est un sous-groupe de $\mathfrak{G}$) est évidemment un groupe. On dira que ce groupe est *généré* à partir de $Y$, ou, si on préfère s'exprimer ainsi, des éléments de $Y$ (relativement à l'opération $*$), et on appellera ces éléments « générateurs » du groupe $< E_Y, * >$.

On observe qu'on ne demande pas que $< Y, * >$ soit un groupe. Le groupe généré par $Y$ est ainsi le groupe $< E_Y, * >$, tel que $E_Y$ est la plus petite des extensions de $Y$, telle que le couple qu'elle forme avec l'opération $*$ est un groupe. On peut citer beaucoup de groupes $< E_Y, * >$ générés à partir d'une partie propre de $E_Y$. C'est par exemple le cas de $< \mathbb{Z}, + >$ qui peut être généré à partir de $\mathbb{N}$, ou de $< \mathbb{Q}_+^*, \cdot >$, qui peut l'être à partir de $\mathbb{N} - \{0\}$ ; $< \{-1, 1\}, \cdot >$ est en revanche généré à partir de $-1$ , et $< \{1\}, \cdot >$ est généré à partir de 1 lui-même.

Selon les définitions précédentes, rien ne s'oppose au fait qu'un même groupe $< E, * >$ soit généré en même temps à partir de deux ensembles distincts. C'est par exemple le cas du groupe $< \mathbb{Z}, + >$ qui est généré autant à partir de $\mathbb{N}$ que, tout simplement, de 1. Le cas de la génération de $< \mathbb{Z}, + >$ à partir de 1 est particulièrement intéressant. Il montre qu'un groupe infini peut être généré à partir d'un ensemble fini et même à partir d'un seul élément. Lorsqu'un groupe est généré à partir d'un seul élément, il est dit « monogène ». On pourra avoir ainsi des groupes monogènes infinis. $< \mathbb{Z}, + >$ est un de ces groupes.

Pour comprendre comment ceci est possible, considérons un ensemble $Y$ composé par un seul élément, disons $a$, et une opération associative $*$ qui s'applique à $a$. Alors il est clair que l'extension $E_Y$ de $Y$, qu'on pourra aussi noter « $E_a$ », telle que $< E_Y, * >$ est le groupe généré à partir de $a$, doit contenir, à côté de $a$ : *i*) tous les résultats des opérations $a * a$, $(a * a) * a$, $[(a * a) * a] * a$, ..., dites « puissances de $a$ (relativement à $*$) » ; *ii*) l'élément neutre de $*$ ; *iii*) l'inverse de toute puissance de $a$, relativement à l'opération $*$. Si on emploie la notation multiplicative, c'est-à-dire qu'on note les résultat de $a*a$ par « $a^2$ », celui de $(a*a)*a$ par « $a^3$ », et ainsi de suite, et on écrit « $a^1$ » pour $a$, « $a^0$ » pour l'élément neutre de $*$ et « $x^{-1}$ » pour l'inverse de $x$ relativement à $*$, alors on dira que $E_a$ doit contenir toutes les puissances entières,

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots \tag{52}$$

de $a$ par rapport à $*$. Il est possible que ces puissances soient toutes distinctes les unes des autres. Si $a = 1$ et $*$ est l'addition sur les entiers, ceci est justement le cas, car on aura

$$\begin{aligned} a^1 &= 1 \\ a^2 &= a + a = 2 \\ a^3 &= a^2 a = 2 + 1 = 3 \\ &\ldots \\ a^0 &= 0 \\ a^{-1} &= -1 \\ a^{-2} &= -2 \\ &\ldots \end{aligned}$$

et donc $E_a = E_1 = \mathbb{Z}$ et $< \mathbb{Z}, + >$ est, comme on l'a dit, un groupe monogène généré à partir de 1. Cette génération correspond à la définition de $\mathbb{Z}$ comme la fermeture minimale, par rapport à l'opération inverse de l'addition, de l'ensemble $\{1, 2, ...\}$, qui est, à son tour, défini récursivement à partir de l'objet 1 et au moyen des additions successives du même objet 1 à l'objet produit lors de l'étape précédente, ce qui est une manière courante de définir d'abord $\mathbb{N} - \{0\}$ et ensuite $\mathbb{N}$ et $\mathbb{Z}$ (le lecteur n'aura pas de difficultés à observer les analogies entre cette construction de $\mathbb{N} - \{0\}$ et la définition des nombres entiers positifs présentée dans le chapitre 1).

Il n'est pourtant pas nécessaire que les puissances (52) soient toutes distinctes les unes des autres. Si, par exemple,

$$a * a = a$$

alors elles coïncident toutes avec $a$, en sorte que $E_a = \{a\}$ et $< E_a, * >$ est un groupe d'ordre 1. Si $a = 1$ et l'opération $*$ est la multiplication sur les entiers, ceci est justement le cas, comme on vient de le voir. Si en revanche

$$a * a = a^2 \neq a$$

mais

$$a^2 * a = a^3 = a$$

alors

$$\begin{aligned} a * a^2 &= a * (a * a) = (a * a) * a = a^2 * a = a \\ a^2 * a^2 &= a^4 (a^2 * a) * a = a * a = a^2 \end{aligned}$$

et

$$\begin{aligned} a^5 &= a^4 * a = a^2 * a = a \\ a^6 &= a^5 * a = a * a = a^2 \\ a^7 &= a^6 * a = a^2 * a = a \\ &... \end{aligned}$$

$a^2$ sera alors l'élément neutre de $*$ (ou bien : $a^2 = a^0$), $a$ sera l'inverse de $a$ (ou bien : $a^{-1} = a$) et $a^2$ l'inverse de $a^2$ (ou bien : $a^{-2} = a^2$). On aura alors $E_a = \{a, a^2\}$ et $< E_a, * >$ sera un groupe d'ordre 2. Si $a = -1$ et $*$ est encore la multiplication sur les entiers, alors

$$\begin{aligned} a^2 &= (-1)(-1) = 1 \\ a^3 &= a^2(-1) = 1(-1) = -1 = a \end{aligned}$$

et $E_a = \{-1, 1\}$, comme on vient de voir.

Une situation analogue se produit si

$$\begin{aligned} a * a &= a^2 \neq a \\ a^2 * a &= a^3 \neq a \end{aligned}$$

mais

$$a^2 * a^2 = a^4 = a$$

Le lecteur pourra en effet vérifier que dans ce cas, on aura

$$\begin{aligned} a^5 &= a^8 = a^{11} = ... = a^2 \\ a^6 &= a^9 = a^{12} = ... = a^3 \\ a^7 &= a^{10} = a^{13} = ... = a^4 = a \\ &\dots \\ a^0 &= a^3 \\ a^{-1} &= a^2 \\ a^{-2} &= a \\ a^{-3} &= a^0 = a^3 \\ &\dots \end{aligned}$$

et $E_a = \{a, a^2, a^3\}$ ; $< E_a, * >$ sera donc un groupe d'ordre 3. Il sera alors facile de comprendre en général que si un nombre naturel $n$ est tel que $a^n = a$ et que pour aucun nombre naturel $m$, tel que $0 < m < n$, $a^m = a$, alors $E_a = \{a, a^2, ...a^{n-1}\}$ et $< E_a, * >$ est un groupe d'ordre $n - 1$.

On comprendra alors la raison pour laquelle, lorsque $< E_a, * >$ est un groupe monogène et $E_a$ est fini, on dit que $< E_a, * >$ est un groupe *cyclique*. En effet, dans ce cas, en partant de l'élément générateur et en opérant selon l'opération $*$, on retombera nécessairement, de manière cyclique, sur les mêmes éléments de $E_a$.

REMARQUE 5.7. Dans certains textes, on appelle directement « cycliques » les groupes qu'on a ici qualifiés de « monogènes », en distinguant ensuite, entre groupes cycliques finis et groupes cycliques infinis.

Un groupe monogène est donc par définition ou bien cyclique (et donc fini), ou bien dénombrable, c'est-à-dire que l'ensemble qui y intervient est au plus dénombrable. On peut montrer que, comme l'argument précédent le suggère, si $< E_a, * >$ est un groupe monogène, alors il est nécessairement abélien. Pour prouver ceci rigouresement, il suffit de noter que si $a$ est l'élément générateur de $< E_a, * >$, alors $a \in E_a$, et si $a * a = a$, alors, comme on l'a vu, $E_a = \{a\}$ et le groupe est fini, d'ordre 1 et certainement abélien, car $a * a = a * a$, tandis que si $a * a = b \neq a$, alors si $a * b = a * (a * a)$ était différent de $b * a = (a * a) * a$, l'opération $*$ ne serait pas associative sur $E_a$ et $< E_a, * >$ ne pourrait pas être un groupe. À partir de cette remarque, on pourrait exploiter le fait que $< E_a, * >$ est au plus dénombrable pour conclure la preuve par induction complète.

Pour permettre au lecteur de se familiariser un peu plus avec la notion de groupe, je vais présenter des exemples de groupes. Je construirai d'abord un groupe bien particulier, et je montrerai ensuite comment il est possible de construire autant de groupes que l'on veut, tous appartenant à une même famille de groupes, dont chaque élément est associé à un nombre naturel distinct.

**1.1. L'exemple d'un groupe de permutations.** Mon premier exemple est celui d'un groupe fini d'ordre 6, avec deux éléments générateurs. On verra plus tard qu'il s'agit d'un groupe de permutations, une espèce de groupes très intéressante, dont le champ d'application en mathématiques est très grand.

Considérons d'abord un ensemble $X$ composé de trois éléments quelconques $x_1$, $x_2$, $x_3$ : des nombres, des lettres de l'alphabet, des humains, tout simplement des symboles, ou quoi que ce soit d'autre. Définissons ensuite deux applications bijectives de $X$ sur $X$, disons $\phi$ et $\psi$, comme il suit :

$$\phi : \begin{cases} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_1 \\ x_3 \longrightarrow x_3 \end{cases} \qquad \psi : \begin{cases} x_1 \longrightarrow x_2 \\ x_2 \longrightarrow x_3 \\ x_3 \longrightarrow x_1 \end{cases}$$

Ces applications peuvent se composer entre elles, en accord à une opération (dite justement « composition » ) que, en général, on pourra définir de la manière suivante, pour tout couple d'applications telles que l'ensemble d'arrivée de la première coïncide avec l'ensemble de départ de la deuxième : si $\Phi$ et $\Psi$ sont deux applications, respectivement de $A$ vers $B$ et de $B$ vers $C$, telles que $\Phi$ associe l'élément $a_\varkappa$ de $A$ à l'élément $b_\varkappa$ de $B$ (en symboles : $\Phi : A \to B$ et $a_\varkappa \xrightarrow{\Phi} b_\varkappa$) et $\Psi$ associe l'élément $b_\varkappa$ de $B$ à l'élément $c_\varkappa$ de $C$ (en symboles : $\Psi : B \to C$ et $b_\varkappa \xrightarrow{\Psi} c_\varkappa$), alors la composition, notée « $\Psi \circ \Phi$ », de $\Phi$ et $\Psi$ est une application de $A$ vers $C$ qui associe l'élément $a_\varkappa$ de $A$ à l'élément $c_\varkappa$ de $C$ (en symboles : $\Psi \circ \Phi : A \to C$ et $a_\varkappa \xrightarrow{\Psi \circ \Phi} c_\varkappa$).

REMARQUE 5.8. Le lecteur n'aura aucune difficulté à observer que, ainsi définie, l'opération de composition de deux applications n'est qu'une généralisation de l'opération de composition de deux déplacements d'un segment sur un plan euclidien, qu'on a définie tout à l'heure (comme on l'a vu, un déplacement d'un segment sur un plan euclidien peut en effet être pensé comme une certaine application bijective, dont autant l'ensemble de départ que l'ensemble d'arrivée est donné par l'ensemble de positions possibles du segment sur ce plan). Pour s'en convaincre il suffit d'observer que, selon la définition qu'on vient de donner, $\Psi \circ \Phi(a_\varkappa) = \Psi(\Phi(a_\varkappa)) = \Psi(b_\varkappa) = c_\varkappa$. On n'aura donc aucune difficulté à comprendre que l'opération $\circ$ ainsi définie est associative.

À ce point, il s'agit de chercher l'extension minimale $E_{\{\phi,\ \psi\}}$ de l'ensemble de bijections de $X$ sur $X$ $\{\phi,\ \psi\}$, telle que $< E_{\{\phi,\ \psi\}}, \circ >$ soit un groupe. Commençons par nous demander si l'ensemble $\{\phi,\ \psi\}$ est fermé par rapport à $\circ$. Comme $\{\phi,\ \psi\}$ contient deux éléments (et que

rien ne nous assure que $\circ$ soit commutative), on aura d'abord quatre compositions possibles : $\phi\circ\psi$, $\psi\circ\phi$, $\phi\circ\phi=\phi^2$ et $\psi\circ\psi=\psi^2$. Il est facile de voir que ces compositions produisent quatre nouvelles applications bijectives de $X$ sur $X$, toutes distinctes entre elles et toutes distinctes de $\phi$ et $\psi$ ; les voici :

$$\psi\circ\phi:\begin{cases}x_1\longrightarrow x_3\\ x_2\longrightarrow x_2\\ x_3\longrightarrow x_1\end{cases}\qquad \phi\circ\psi:\begin{cases}x_1\longrightarrow x_1\\ x_2\longrightarrow x_3\\ x_3\longrightarrow x_2\end{cases}$$

$$\phi^2:\begin{cases}x_1\longrightarrow x_1\\ x_2\longrightarrow x_2\\ x_3\longrightarrow x_3\end{cases}\qquad \psi^2:\begin{cases}x_1\longrightarrow x_3\\ x_2\longrightarrow x_1\\ x_3\longrightarrow x_2\end{cases}$$

Une condition nécessaire pour que l'extension de $\{\phi,\ \psi\}$ que nous cherchons soit fermée par rapport à $\circ$ , est donc qu'elle contienne, en plus de $\phi$ et $\psi$, également ces quatre applications. On se demande si c'est aussi une condition suffisante.

La réponse est immédiate et évidemment positive. Il suffit d'observer qu'en composant des applications bijectives d'un ensemble $A$ sur lui-même, on ne peut obtenir que des applications bijectives de l'ensemble $A$ sur lui-même (la preuve est banale et le lecteur pourra s'exercer à la conduire seul), et que, si $X$ est un ensemble contenant trois éléments, il ne peut y avoir que six applications bijectives distinctes de $X$ sur $X$. Une application bijective de $X$ sur $X$ peut en effet être pensée comme une association qui associe l'ordre $\{x_1,x_2,x_3\}$ des éléments de $X$ avec un ordre quelconque de ces mêmes éléments, et il n'y a que six ordres distincts possibles sur un ensemble de trois éléments. Ces ordres sont évidemment les suivants :

| | | (1) | (2) | (3) | (4) | (5) | (6) |
|---|---|---|---|---|---|---|---|
| $x_1$ | $\longrightarrow$ | $x_1$ | $x_1$ | $x_2$ | $x_2$ | $x_3$ | $x_3$ |
| $x_2$ | $\longrightarrow$ | $x_2$ | $x_3$ | $x_1$ | $x_3$ | $x_1$ | $x_2$ |
| $x_3$ | $\longrightarrow$ | $x_3$ | $x_2$ | $x_3$ | $x_1$ | $x_2$ | $x_1$ |
| | | $(\phi^2)$ | $(\phi\circ\psi)$ | $(\phi)$ | $(\psi)$ | $(\psi^2)$ | $(\psi\circ\phi)$ |

et ils correspondent, comme il est facile de voir, et comme le tableau l'indique, aux six applications $\phi$, $\psi$, $\psi\circ\phi$, $\phi\circ\psi$, $\phi^2$ et $\psi^2$ qu'on a considérées jusqu'ici. Ainsi, en composant entre elles ces six applications, on ne pourra obtenir à nouveau, à chaque fois, qu'une de ces six bijections.

On a ainsi prouvé qu'aucune extension de $\{\phi,\ \psi\}$ plus petite que

$$\left\{\phi,\psi,\psi\circ\phi,\phi\circ\psi,\phi^2,\psi^2\right\}$$

peut aspirer à former un groupe avec l'opération $\circ$, et qu'aucune extension de $\{\phi,\ \psi\}$ plus grande que $\left\{\phi,\psi,\psi\circ\phi,\phi\circ\psi,\phi^2,\psi^2\right\}$ peut ne contenir que des applications bijectives de $X$ sur $X$. Il est donc naturel de se demander si le couple $<\left\{\phi,\psi,\psi\circ\phi,\phi\circ\psi,\phi^2,\psi^2\right\},\circ>$ est ou non un groupe. Comme on vient de voir que ce couple satisfait aux clauses $(i)$ et $(ii)$ de la définition 1.3, il ne reste qu'à se demander s'il satisfait aussi aux clauses $(iii)$ et $(iv)$ de cette même définition. Pour la condition $(iii)$, la réponse est facile, car la bijection $\phi^2$ est évidemment l'élément neutre de $\circ$ en $\left\{\phi,\ \psi,\ \psi\circ\phi,\ \phi\circ\psi,\ \phi^2,\ \psi^2\right\}$. Pour la condition $(iv)$, il s'agit de voir si chaque élément de $\left\{\phi,\ \psi,\ \psi\circ\phi,\ \phi\circ\psi\ ,\phi^2,\psi^2\right\}$ a un inverse en $\left\{\phi,\ \psi,\ \psi\circ\phi,\ \phi\circ\psi,\ \phi^2,\psi^2\right\}$ par rapport à $\circ$. Là aussi la réponse est facile et elle est évidemment positive, car l'élément neutre étant une bijection, l'inverse d'une bijection ne peut qu'être une bijection ; or dans $\left\{\phi,\psi,\psi\circ\phi,\phi\circ\psi,\phi^2,\psi^2\right\}$ il y a toutes les bijections possibles de $X$ sur $X$.

Pour expliciter cette réponse, le lecteur pourra facilement vérifier les égalités suivantes (ou, si $\Phi$ est une application, le symbole « $\Phi^{-1}$ » indique l'application inverse de $\Phi$ relativement à

$\circ$) :

$$(\phi^2)^{-1} = \phi^2 \qquad (\phi \circ \psi)^{-1} = \phi \circ \psi \qquad (\phi)^{-1} = \phi$$
$$(\psi)^{-1} = \psi^2 \qquad (\psi^2)^{-1} = \psi \qquad (\psi \circ \phi)^{-1} = (\psi \circ \phi)$$

Le tableau suivante (dite « table de groupe » ) résume alors la situation :

| $\circ$ | $\phi^2$ | $\phi$ | $\psi$ | $\psi \circ \phi$ | $\phi \circ \psi$ | $\psi^2$ |
|---|---|---|---|---|---|---|
| $\phi^2$ | $\phi^2$ | $\phi$ | $\psi$ | $\psi \circ \phi$ | $\phi \circ \psi$ | $\psi^2$ |
| $\phi$ | $\phi$ | $\phi^2$ | $\phi \circ \psi$ | $\psi^2$ | $\psi$ | $\psi \circ \phi$ |
| $\psi$ | $\psi$ | $\psi \circ \phi$ | $\psi^2$ | $\phi \circ \psi$ | $\phi$ | $\phi^2$ |
| $\psi \circ \phi$ | $\psi \circ \phi$ | $\psi$ | $\phi$ | $\phi^2$ | $\psi^2$ | $\phi \circ \psi$ |
| $\phi \circ \psi$ | $\phi \circ \psi$ | $\psi^2$ | $\psi \circ \phi$ | $\psi$ | $\phi^2$ | $\phi$ |
| $\psi^2$ | $\psi^2$ | $\phi \circ \psi$ | $\phi^2$ | $\phi$ | $\psi \circ \phi$ | $\psi$ |

Du fait que la matrice qui forme cette table n'est pas symétrique, il suit que le groupe $< E_{\{\phi,\psi\}}, \circ >$, où, comme, l'on vient de voir,

$$E_{\{\phi,\psi\}} = \left\{\phi, \psi, \psi \circ \phi, \phi \circ \psi, \phi^2, \psi^2\right\}$$

n'est pas abélien, et du fait que $E_{\{\phi,\psi\}}$ contient six éléments, il suit qu'il s'agit d'un groupe d'ordre 6.

On pourrait se demander si le même groupe ne pourrait pas être généré à partir d'un autre sous-ensemble de $E$ différent de $\{\phi, \psi\}$ et en particulier d'un seul des éléments de $E$. Le dernier tableau fournit la réponse à cette question, car il nous montre : que si on part d'un seul élément choisi parmi $\phi^2$, $\phi$, $\phi \circ \phi$ et $\phi \circ \psi$ de $E$ et qu'on le compose avec lui-même selon $\circ$, on n'obtient rien d'autre que l'élément neutre de $\circ$ dans $E$, qui, composé à son tour, dans n'importe quel ordre, avec l'élément de départ donne ce même élément de départ, et composé avec lui-même donne encore une fois soi-même ; tandis que si on part d'un seul parmi les éléments $\psi$ et $\psi^2$ et qu'on le compose avec lui-même selon $\circ$, on obtient l'autre de ces deux éléments, qui, composé avec l'élément de départ, dans n'importe quel ordre, donne l'élément neutre de $\circ$ dans $E$, c'est-à-dire $\phi^2$. Donc, dans le premier cas on s'arrêterait à un ensemble de deux éléments composé par l'élément donné et $\phi^2$, tandis que dans le deuxième on ne parviendrait qu'à l'ensemble à trois éléments $\left\{\psi, \psi^2, \phi^2\right\}$. Le groupe $< \left\{\phi, \psi, \psi \circ \phi, \phi \circ \psi, \phi^2, \psi^2\right\}, \circ >$ n'est donc certainement pas monogène, ce qui dérive d'ailleurs, beaucoup plus facilement, du fait qu'il n'est pas abélien.

Le lecteur motivé pourrait s'exercer à répéter la même construction à partir des ensembles $X$ de $i = 2, 4, 5, ...$ éléments, et vérifier qu'il obtiendrait : dans le premier cas, un groupe monogène (et donc abélien) d'ordre 2 ; et, dans les autres cas, des groupes non abéliens d'ordre $i!$.

L'ensemble $E_X$ qui entre dans tous ces groupes est un ensemble d'applications bijectives d'un ensemble sur lui-même. Or il est facile de voir qu'une application bijective d'un ensemble sur lui même ne fait, pour ainsi dire, que changer la place des éléments de l'ensemble sur lesquels elle opère, en mettant chacun de ces éléments à la place d'un autre. Une telle application s'appelle « permutation », de sorte que les groupes en question sont des groupes finis de permutations et gèrent les transformations possibles qu'un ensemble peut subir, sans acquérir ni perdre des éléments. Les applications de la théorie des groupes de permutations sont variées autant en mathématiques (par exemple dans la théorie des équations algébriques), qu'ailleurs.

NOTE HISTORIQUE 5.5. Dans la nuit du 29 au 30 mai 1832, un jeune homme de vingt ans (né le 25 octobre 1811 à Bourg-la-Reine) écrivit une lettre à un cher ami, un dénommé Auguste Chevalier. Ce jeune homme avait échoué deux fois à son concours d'entrée à l'École polytechnique ; il était ensuite entré à l'École préparatoire, mais il avait été expulsé après avoir publié une lettre où il attaquait violemment le

directeur de cette école ; il avait envoyé deux manuscrits mathématiques à l'Académie des Sciences, tous deux perdus, d'abord par Cauchy et ensuite par Fourier ; il avait recomposé le deuxième manuscrit et l'avait envoyé à Poisson qui l'avait jugé incompréhensible ; il avait pris part aux émeutes contre Louis-Philippe et il était détenu sur parole dans une maison de santé (à cause de sa santé incertaine) ; il s'était épris d'une femme et mu par sa passion il avait accepté de se battre en duel le matin du 30 mai ; il savait qu'il serait tué par son adversaire. Dans sa lettre, il résumait les découvertes mathématiques qu'il était sûr d'avoir faites, mais que personne n'avait su comprendre. Le jour suivant le jeune homme fut atteint d'une balle au ventre et il mourut le 31 mai, à deux heures du matin.

Après la morte du jeune homme et la publication de la lettre à Chevalier, des mathématiciens commencèrent à lire les papiers mathématiques que ce dernier avait laissé. Ils se rendirent finalement compte que les découvertes mathématiques de ce jeune homme, dénommé Évariste Galois, étaient en mesure de changer en profondeur la physionomie des mathématiques connues. Aujourd'hui, les mathématiciens sont unanimes en considérant Galois comme l'un des plus extraordinaires mathématiciens de tous les temps.

Dans sa lettre à Chevalier, Galois esquissait la preuve qu'il avait obtenue pour la conjecture que Ruffini avait avancée une trentaine d'années plus tôt, d'après laquelle les racines d'une équation algébrique dont le dégré est supérieur à quatre ne sont pas généralement des fonctions algébriques des coefficients de cette équation [cf. la note historique 5.2]. Pour obtenir cette preuve, il avait construit et puis étudié des groupes de permutations constitués par les racines d'une équation algébriques, en essayant de définir les conditions sous les quelles des racines d'une équation donnée sont permutables sans que cela comporte des variations dans certaines fonctions de ces racines. L'idée d'étudier les permutations possibles des racines d'une équation avait déjà été avancée une cinquantaine d'années plus tôt par Lagrange, mais Galois était désormais en mesure de parvenir à un niveau d'abstraction et de généralité que Lagrange était bien loin d'avoir atteint. Sa lettre enseigna à jamais aux mathématiciens comment traiter avec des structures algébriques générales et fait de Galois le véritable père de l'algèbre moderne.

**Lectures possibles** : G. Verriest, *Évariste Galois et la théorie des équations algébriques*, Gauthier-Villars, Paris, 1934 ; R. Bourgne et J.-P. Ayra (éd.), *Écrits et mémoires mathématiques d'Évariste Galois*, Gauthier-Villars, Paris, 1962. A. Dalmas, *Évariste Galois. Révolutionnaire et géométre*, Le nouveau commerce, s.h., 1982. A. Astruc, Evariste Galois, Flammarion, Paris, 1994.

**1.2. Les groupes des classes de congruence modulo $n$.** Revenons maintenant à nos ensembles $\mathbb{N}$ et $\mathbb{Z}$. Ceci nous permettra de découvrir une variété assez intéressante de groupes finis. Choisissons d'abord deux éléments quelconques $n$ et $p$ de $\mathbb{N}$, tels que $n > 1$ et $0 \leq p < n$, et considérons tous les éléments $\kappa_\zeta$ de $\mathbb{Z}$ qu'on peut écrire sous la forme

$$\kappa_\zeta = \zeta n + p$$

$\zeta$ étant un nombre relatif quelconque (c'est-à-dire un élément quelconque de $\mathbb{Z}$). Si $n = 7$ et $p = 3$, alors :

$$..., \kappa_{-2} = -11, \kappa_{-1} = -4, \kappa_0 = 3, \kappa_1 = 10, \kappa_2 = 17, ...$$

On voit facilement que, quel que soit $p$, ces nombres sont tous tels que

$$\kappa_{\zeta+1} - \kappa_\zeta = n$$

et que le reste de leur division pour $n$ est toujours égal à $p$ (dans notre exemple, on aura : ... ; $\frac{-11}{7} = -2 + \frac{3}{7}$ ; $\frac{-4}{7} = -1 + \frac{3}{7}$ ; $\frac{3}{7} = 0 + \frac{3}{7}$ ; $\frac{10}{7} = 1 + \frac{3}{7}$ ; $\frac{17}{7} = 2 + \frac{3}{7}$ ;...). On peut noter l'ensemble $\{\kappa_\zeta\}_{\zeta\in\mathbb{Z}}$ de ces nombres par le symbole « $\overset{n}{p}$ » (de sorte que $\overset{7}{3}$ est par exemple l'ensemble $\{...,-11,-4,3,10,17,...\}$).

Considérons maintenant le nombre naturel $n$ comme étant fixe, et faisons varier $p$ entre 0 et $n-1$. Il est clair qu'à chaque choix de $p$ correspondra un ensemble ${}_p\{\kappa_\zeta\}_{\zeta\in\mathbb{Z}} = \overset{n}{p}$ différent. On aura ainsi $n$ ensembles de nombres relatifs, $\overset{n}{0}, \overset{n}{1}, \overset{n}{2}, ..., \overset{n}{n-1}$ différents entre eux, qui seront bien sûr tels que chaque nombre relatif appartiendra à un et un seul de ces ensembles, en sorte que l'intersection de ces ensembles sera la classe vide et leur union coïncidera avec $\mathbb{Z}$. Pour se convaincre de ceci, il suffira d'observer que dans chacun de ces ensembles entreront tous les nombres relatifs qui peuvent s'écrire respectivement sous les formes :

$$\begin{aligned}&\zeta n\\&\zeta n+1\\&\zeta n+2\\&...\\&\zeta n+(n-1)\end{aligned}$$

$\zeta$ étant un nombre relatif quelconque.

Le choix de n'importe quel nombre naturel $n$ plus grand que 1 nous permet donc de partager $\mathbb{Z}$ en $n$ parties, mutuellement disjointes : $\overset{n}{0}, \overset{n}{1}, \overset{n}{2}, ...,$ et $\overset{n}{n-1}$. Il est aussi facile de vérifier que la différence entre deux éléments quelconques du même ensemble $\overset{n}{p}$ ne dépend ($n$ étant fixé) que de la différence des nombres relatifs $\zeta$. Quels que soient ces éléments, ils pourront en fait s'écrire ainsi

$$\kappa_{\zeta'} = \zeta' n + p \qquad \text{et} \qquad \kappa_{\zeta''} = \zeta'' n + p$$

où $\zeta'$ et $\zeta''$ sont deux valeurs de $\zeta$, c'est-à-dire deux nombres relatifs, et leur différence sera ainsi, quel que soit $p$,

$$\zeta' n + p - \zeta'' n - p = (\zeta' - \zeta'')n$$

Or, imaginons qu'on commence à compter les nombres relatifs à partir d'un nombre quelconque et que, après en avoir compté $n$, on recommence à partir de 1. Ainsi si on part de $-9$ et qu'on pose $n = 7$, on aura ce décompte :

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $-9$ | $-8$ | $-7$ | $-6$ | $-5$ | $-4$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ | $4$ | ... |
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | |
| $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ | $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ | ... |

Il est facile de constater que les nombres de la première ligne qui correspondent à des nombres égaux entre eux dans la deuxième sont exactement ceux qui appartiennent au même ensemble $\overset{n}{p}$. C'est la raison pour laquelle on dit que les éléments d'un même ensemble $\overset{n}{p}$ (quel que soit $p$) sont congruents modulo $n$ (c'est-à-dire qu'en certaines circonstances, ils peuvent être pris comme égaux). Les ensembles $\overset{n}{0}, \overset{n}{1}, \overset{n}{2}, ..., \overset{n}{n-1}$ sont ainsi des classes d'équivalence, c'est-à-dire que la relation $x\mathbf{R}y$ qui a lieu entre deux nombres relatifs $x$ et $y$ si et seulement si $x$ et $y$ appartiennent au même ensemble $\overset{n}{p}$ (quel que soit $p$) est une relation d'équivalence : le lecteur n'aura aucune difficulté à s'exercer en le montrant. Cela revient à dire qu'à chaque choix de $n$ correspond une partition de $\mathbb{Z}$ en $n$ classes d'équivalence dites « classes de congruence modulo $n$ ». Or, si l'union de ces classes coïncide avec $\mathbb{Z}$, cela ne signifie pas que l'ensemble $\left\{\overset{n}{0}, \overset{n}{1}, \overset{n}{2}, ..., \overset{n}{n-1}\right\}$ de

ces classes coïncide, lui aussi, avec $\mathbb{Z}$. On appellera ce dernier ensemble « ensemble des classes de congruence modulo $n$ », et on le notera par le symbole « $\mathbb{Z}/n\mathbb{Z}$ ».

REMARQUE 5.9. Comme on l'a déjà noté, implicitement, dans le chapitre 1, la différence qu'on fait en théorie des ensembles entre union de plusieurs ensembles et ensemble dont ces ensembles sont les éléments est profonde et absolument fondamentale (on pourrait même dire que la théorie des ensembles naît, aux alentours de 1880, grâce à des mathématiciens tels Dedekind ou Cantor et, en partie, à Frege, lorsqu'on parvient à saisir cette différence). En effet, si deux ensembles $A$ et $B$ sont donnés, par exemple l'ensemble $A$ des nombres naturels pairs et l'ensemble $B$ des nombres naturels impairs, une chose est de rassembler tous les éléments de ces ensembles dans un seul ensemble, en effaçant, pour ainsi dire, les frontières entre $A$ et $B$, et une autre chose est de former l'ensemble $\{A, B\}$, dont les deux seuls éléments sont les ensembles $A$ et $B$. Dans le premier cas on a l'ensemble $\{1, 2, 3, ...\}$ composé d'une infinité d'éléments, dans le deuxième cas, on a justement l'ensemble $\{A, B\}$ qui n'est composé que de deux éléments.

Bien qu'à chaque nombre naturel $n$ plus grand que 1 corresponde un ensemble $\mathbb{Z}/n\mathbb{Z}$ différent, chacun de ces ensembles est fini et ne contient que $n$ éléments. Cela ne nous empêche pas de définir sur cet ensemble, quel que soit $n$, deux lois de composition internes, qu'on pourra respectivement identifier avec une addition et une multiplication. Pour ce faire, on commence par observer que, si $\zeta'$ et $\zeta''$ sont deux nombres relatifs quelconques et $h$ et $k$ deux nombres naturels plus petits que $n$, alors les nombres relatifs $\zeta' n + h$ et $\zeta'' n + k$ appartiennent respectivement aux classes $\overset{n}{h}$ et $\overset{n}{k}$ , tandis que leur somme et leur produit,

$$\begin{aligned} \zeta' n + h + \zeta'' n + k &= (\zeta' + \zeta'')\, n + (h + k) \\ (\zeta' n + h) \cdot (\zeta'' n + k) &= (\zeta' \zeta'' n + \zeta' k + \zeta'' h)\, n + hk \end{aligned}$$

appartiennent respectivement aux classes $(\overset{n}{h + k})$ et $(\overset{n}{hk})$, le symbole « $\overset{n}{q}$ » indiquant, par extension, quel que soit le nombre naturel $q$, la classe de congruence modulo $n$ à laquelle appartient $q$. Il est donc tout à fait naturel de définir l'addition et la multiplication sur l'ensemble des classes de congruence modulo $n$, en termes de l'addition et de la multiplication sur les nombres naturels, comme il suit :

$$\overset{n}{h} + \overset{n}{k} = (\overset{n}{h + k}) \qquad \text{et} \qquad \overset{n}{h} \cdot \overset{n}{k} = (\overset{n}{h \cdot k}) \tag{53}$$

quels que soient les nombres naturels $h$ et $k$. Par exemple si $n = 7$, comme tout à l'heure, on aura les tables suivantes pour l'addition et la multiplication sur l'ensemble des classes de

congruence modulo 7 :

(54)

| $+$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ |
|---|---|---|---|---|---|---|---|
| $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ |
| $\overset{7}{1}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ | $\overset{7}{0}$ |
| $\overset{7}{2}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{1}$ |
| $\overset{7}{3}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ |
| $\overset{7}{4}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ |
| $\overset{7}{5}$ | $\overset{7}{5}$ | $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ |
| $\overset{7}{6}$ | $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ |

| $\cdot$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ |
|---|---|---|---|---|---|---|---|
| $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ | $\overset{7}{0}$ |
| $\overset{7}{1}$ | $\overset{7}{0}$ | $\overset{7}{1}$ | $\overset{7}{2}$ | $\overset{7}{3}$ | $\overset{7}{4}$ | $\overset{7}{5}$ | $\overset{7}{6}$ |
| $\overset{7}{2}$ | $\overset{7}{0}$ | $\overset{7}{2}$ | $\overset{7}{4}$ | $\overset{7}{6}$ | $\overset{7}{1}$ | $\overset{7}{3}$ | $\overset{7}{5}$ |
| $\overset{7}{3}$ | $\overset{7}{0}$ | $\overset{7}{3}$ | $\overset{7}{6}$ | $\overset{7}{2}$ | $\overset{7}{5}$ | $\overset{7}{1}$ | $\overset{7}{4}$ |
| $\overset{7}{4}$ | $\overset{7}{0}$ | $\overset{7}{4}$ | $\overset{7}{1}$ | $\overset{7}{5}$ | $\overset{7}{2}$ | $\overset{7}{6}$ | $\overset{7}{3}$ |
| $\overset{7}{5}$ | $\overset{7}{0}$ | $\overset{7}{5}$ | $\overset{7}{3}$ | $\overset{7}{1}$ | $\overset{7}{6}$ | $\overset{7}{4}$ | $\overset{7}{2}$ |
| $\overset{7}{6}$ | $\overset{7}{0}$ | $\overset{7}{6}$ | $\overset{7}{5}$ | $\overset{7}{4}$ | $\overset{7}{3}$ | $\overset{7}{2}$ | $\overset{7}{1}$ |

En observant ces tables, on comprend que l'ensemble $\mathbb{Z}/7\mathbb{Z}$ est fermé par rapport à l'addition et à la multiplication et que ces deux opérations sont commutatives sur cet ensemble et admettent chacune un élément neutre, égal respectivement à $\overset{7}{0}$ et $\overset{7}{1}$. Il n'est pas difficile de comprendre que c'est le cas de tous les ensembles $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo $n$ ($n = 2, 3, ...$), les éléments neutres étant respectivement $\overset{n}{0}$ et $\overset{n}{1}$. Il n'est ensuite pas difficile de comprendre que l'addition et la multiplication ainsi définies sur les ensembles $\mathbb{Z}/n\mathbb{Z}$ sont aussi associatives (le lecteur pourra s'exercer à le vérifier). Ainsi, on peut dire avoir défini, sur chacune de ces ensembles, une addition et une multiplication associatives et commutatives, qui admettent un élément neutre, et par rapport auxquelles ces ensembles sont fermées. Il reste à savoir si tous les élément de ces ensembles sont inversibles par rapport à ces opérations. Dans ce cas, la réponse est facile : c'est vrai pour l'addition — car dans la table ci-dessus, ainsi que dans toutes les tables analogues relatives à d'autres valeurs de $n$, l'élément neutre figure dans chaque ligne et chaque colonne (et donc, pour tout élément de n'importe quel ensemble $\mathbb{Z}/n\mathbb{Z}$, il y a un éléments du même ensemble qui, additionné à celui-ci, produit l'élément neutre de l'addition dans cet ensemble : dans le cas $n = 7$, on aura, par exemple, comme il est facile de vérifier sur la première des deux tables précédentes, $\left(\overset{7}{0}\right)^{-1} = \overset{7}{0}$; $\left(\overset{7}{1}\right)^{-1} = \overset{7}{6}$; $\left(\overset{7}{2}\right)^{-1} = \overset{7}{5}$; $\left(\overset{7}{3}\right)^{-1} = \overset{7}{4}$; $\left(\overset{7}{4}\right)^{-1} = \overset{7}{3}$; $\left(\overset{7}{5}\right)^{-1} = \overset{7}{2}$; $\left(\overset{7}{6}\right)^{-1} = \overset{7}{0}$) —, mais ça ne l'est pas pour la multiplication — car dans aucun ensemble $\mathbb{Z}/n\mathbb{Z}$ l'élément $\overset{n}{0}$ n'est inversible (c'est-à-dire qu'en aucun ensemble $\mathbb{Z}/n\mathbb{Z}$, il y a un élément $\overset{n}{p}$, tel que $\overset{n}{0} \cdot \overset{n}{p} = \overset{n}{1}$). Ainsi, les couples $< \mathbb{Z}/n\mathbb{Z}, + >$ et $< \mathbb{Z}/n\mathbb{Z}, \cdot >$, se comportent, par rapport à la propriété de former un groupe, comme les couples $< \mathbb{Z}, + >$ et $< \mathbb{Z}, \cdot >$, les premiers (c'est-à-dire $< \mathbb{Z}/n\mathbb{Z}, + >$, pour $n = 2, 3, ...$ ) forment des groupes abéliens, les seconds (à savoir $< \mathbb{Z}/n\mathbb{Z}, \cdot >$, pour $n = 2, 3, ...$ ) ne forment que des monoïdes commutatifs unitaires. Pourtant, entre les couples $< \mathbb{Z}/n\mathbb{Z}, + >$ et $< \mathbb{Z}/n\mathbb{Z}, \cdot >$ et les couples $< \mathbb{Z}, + >$ et $< \mathbb{Z}, \cdot >$ il y a une différence essentielle : tous les ensembles $\mathbb{Z}/n\mathbb{Z}$ sont finis et ne contiennent que $n$ éléments. On reviendra plus loin sur le comportement des ensembles $\mathbb{Z}/n\mathbb{Z}$ par rapport à la multiplication définie sur ces ensembles. Pour l'instant, on se limitera à observer que l'argument précédent nous montre comment construire autant de groupes abéliens, qu'on veut : tous ceux qui appartiennent à la famille $\{< \mathbb{Z}/n\mathbb{Z}, + >\}$ ($n = 2, 3, ...$), dits « groupes (additifs) des classes de congruence modulo $n$ ».

## 2. Anneaux

Jusqu'ici, on n'a considéré que les comportements de certains ensembles relativement à une seule opération définie sur ces ensembles. La pratique arithmétique nous enseigne pourtant qu'il est souvent nécessaire de combiner entre elles des opérations diverses et nous fait comprendre que les propriétés de $\mathbb{N}$, de $\mathbb{Z}$ et de $\mathbb{Q}$ dépendent justement de la manière selon laquelle les deux opérations d'addition et de multiplication se combinent entre elles. Cela nous pousse à définir et étudier des structures algébriques constituées non plus par des couples formés par un ensemble et une opération définie sur cet ensemble, mais par des triplets composés par un ensemble et deux opérations définies sur cet ensemble. Il s'agit alors de classer ces structures sur la base de trois sortes de conditions : les conditions qui doivent être satisfaites relativement à la première opération, considérée isolément ; les conditions qui doivent être satisfaites relativement à la deuxième opération considérée isolément ; les conditions que ces opérations doivent satisfaire l'une relativement à l'autre.

La plus simple des structures de ce genre, qu'on va présenter ici et qu'on étudie généralement en algèbre, combine ces conditions de la manière suivante : le couple formé par l'ensemble et la première opération définie sur cet ensemble est un groupe abélien ; le couple formé par l'ensemble et la deuxième opération définie sur cet ensemble est un magma associatif ; la deuxième opération est distributive sur la première dans l'ensemble considéré. Un telle structure s'appelle « anneau » et est donc définie comme suit :

DÉFINITION 2.1. *On appelle « anneau » un triplet $< E, *, \star >$ composé par un ensemble $E$ quelconque et deux opérations $*$ et $\star$ définies sur l'ensemble $E$, telles que le couple $< E, * >$ est un groupe abélien, le couple $< E, \star >$ est un magma associatif (ce qu'on appelle quelques fois un « demi-groupe » ) et l'opération $\star$ est distributive sur l'opération $*$ dans $E$. En d'autres termes, un triplet $< E, *, \star >$ est un anneau si et seulement si :*

*i.i) pour tout $x$ et $y$ appartenant à $E$, $x * y$ appartient à $E$ ;*

*i.ii) pour tout $x$ et $y$ appartiennent à $E$, $x * y = y * x$ ;*

*i.iii) pour tout $x$, $y$ et $z$ appartenant à $E$, $(x * y) * z = x * (y * z)$ ;*

*i.iv) il y a dans $E$ un (et un seul) élément $e$ (l'élément neutre de $*$), tel que pour tout $x$ appartenant à $E$, $x * e (= e * x) = x$ ;*

*i.v) pour tout $x$ appartenant à $E$, il y a dans $E$ un et un seul élément $y_{x,*}$ (l'élément inverse de $x$ relativement à $*$), tel que $x * y_{x,*} (= x * y_{x,*}) = e$ ;*

*ii.i) pour tout $x$ et $y$ appartenant à $E$, $x \star y$ appartient à $E$ ;*

*ii.ii) pour tout $x$, $y$ et $z$ appartenant à $E$, $(x \star y) \star z = x \star (y \star z)$ ;*

*iii.i) pour tout $x$, $y$ et $z$ appartenant à $E$, $x \star (y * z) = (x \star y) * (x \star z)$.*

*Si l'opération $\star$ est de surcroît commutative dans $E$, c'est-à-dire que pour tout $x$ et $y$ appartenant à $E$, $x \star y = y \star x$, alors l'anneau est dit lui-même « commutatif » ; si enfin l'opération $\star$ admet, elle-aussi, un élément neutre en $E$, distinct de l'élément neutre de $*$, alors l'anneau est dit « unitaire ».*

REMARQUE 5.10. La condition qui exige que l'éventuel élément neutre de $\star$ soit distinct de l'élément neutre de $*$ sert à garantir l'univocité des opérations sur un anneau. En effet, si $e$ était l'élément neutre autant de $*$ que de $\star$, alors, grâce à la distributivité de $\star$ sur $*$, on aurait, pour tous éléments $x$ et $y$ de $E$ :

$$\begin{aligned} x \star y &= (x \star e) \star (y * e) \\ &= [(x \star e) \star y] * [(x \star e) \star e] \\ &= (x \star y) * x \end{aligned}$$

et donc, quel que soit $x$ dans $E$, si $z = x \star y$ ($z$ et $y$ étant deux éléments de $E$), alors $z = z * x$.

REMARQUE 5.11. Quels que soient $x$ et $y$ appartenant à $E$, on aura, pour la définition de l'élément neutre de $*$ sur un anneau et la distributivité de $*$ sur $\star$,

$$x \star y = x \star (y * e) = (x \star y) * (x \star e)$$

et, donc, comme l'élément neutre de $*$ est unique,

$$(x \star e) = e \tag{55}$$

La distributivité de $*$ sur $\star$, a donc comme conséquence que dans n'importe quel anneau le résultat de l'application de l'opération $\star$ à tout élément de $E$ et à l'élément neutre de $*$ est l'élément neutre de $*$ lui-même.

Il est facile de trouver, parmi les structures dont on a parlé dans les chapitres précédents, des exemples d'anneaux. Si $E$ est l'ensemble $\mathbb{Z}$ des nombres relatifs et $*$ et $\star$ sont respectivement l'addition et la multiplication sur ces nombres, on a évidemment l'anneau commutatif unitaire $< \mathbb{Z}, +, \cdot >$. Il est en revanche facile de voir que le triplet $< \mathbb{Z}, \cdot, + >$ n'est pas un anneau, car dans $\mathbb{Z}$ l'addition n'est pas distributive sur la multiplication (ce triplet ne satisfait donc pas à la condition ( *iii.i*) et aucun élément de $\mathbb{Z}$ différent de 1 n'a un inverse dans $\mathbb{Z}$ relativement à $\cdot$ (donc ce triplet ne satisfait pas à la condition (*i.iv*) non plus). Quant aux nombres rationnels, il est facile de voir que $< \mathbb{Q}, +, \cdot >$ est aussi un anneau commutatif unitaire. On verra pourtant tout à l'heure que cette structure respecte aussi des conditions significativement plus fortes que celles imposées à un anneau commutatif.

Pour avoir des exemples d'anneaux finis, considérons en revanche l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo $n$, pour un nombre naturel quelconque plus grand que 1. Il n'est pas difficile de montrer que si l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ sont définies comme ci-dessus, alors le triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$ est, quel que soit $n$, un anneau commutatif unitaire d'ordre $n$ (de même qu'un groupe, un anneau est dit « d'ordre $n$ » si l'ensemble $E$ est fini et ne contient que $n$ éléments).

On pourrait finalement montrer, entre autres choses, que si $< E, +, \cdot >$ est un anneau commutatif et $a, b \in E$, alors la formule du développement binomial présentée dans le chapitre 3 est sans doute valable pour tout exposant naturel, de quelque manière qu'on définisse l'addition $+$ et la multiplication $\cdot$ sur les éléments de $E$ (à condition évidemment que pour tout $x \in E$, le symbole $x^m$, $m$ étant un nombre naturel différent de 0 , indique le produit $x^{m-1} \cdot x$ et que $x^0$ soit l'élément neutre de $E$ par rapport à $\cdot$). On laissera cette démonstration aux lecteurs les plus motivés.

REMARQUE 5.12. Cette dernière remarque rend claire une des raisons qui font l'intérêt de la structure algébrique qu'on appelle « anneau ». Celle-ci est, en effet, la plus simple des structures algébriques sur laquelle la formule du développement binomial démontrée dans le chapitre 3 est valable. En qualifiant, lors de la démonstration de cette formule, les termes $a$ et $b$ de « quantités quelconques » et en parlant, en rapport à ces quantités, d'addition et de multiplication au sens habituel de ces termes, on a implicitement supposé travailler, non pas sur un anneau quelconque, mais sur une structure bien définie, qui satisfait à des conditions plus fortes que celles qui définissent un anneau. Pourtant, le lecteur pourra revenir sur les deux démonstrations qu'on a données de cette formule pour vérifier qu'elles ne demandent aucune condition plus forte que l'appartenance de $a$, $b$ à un ensemble $E$ qui forme, avec les deux opérations y notées « $+$ » et « $\cdot$ » un anneau commutatif.

## 3. Corps

Revenons maintenant à la définition 2.1, et essayons de voir s'il n'y a pas moyen de renforcer de manière intéressante les conditions qui y interviennent, en parvenant, par exemple, à saisir

les propriétés structurelles profondes et distinctives de l'ensemble $\mathbb{Q}$ des nombres rationnels. Une possibilité nous apparaît dès le début : elle consiste à renforcer les conditions demandées pour le couple $< E, \star >$ ; ne pourrait-on pas demander que ce couple soit plus qu'un simple magma associatif ? Voyons. Il est clair que si, allant au-delà de cette condition minimale, on demande par exemple que l'opération $\star$ admette un élément neutre dans $E$, on reste encore à des conditions qui sont satisfaites autant par le triplet $< \mathbb{Z}, +, \cdot >$, que par le triplet $< \mathbb{Q}, +, \cdot >$, qui sont justement des anneaux (commutatifs) unitaires. En revanche, si on demande que le couple $< E, \star >$ soit carrément un groupe, alors on tombe d'emblée au-delà des conditions que $< \mathbb{Z}, +, \cdot >$ autant que $< \mathbb{Q}, +, \cdot >$ respectent, car, sauf 1, aucun des éléments de $\mathbb{Z}$ n'admet un inverse dans $\mathbb{Z}$ relativement à $\cdot$, et même dans $\mathbb{Q}$ il y a un élément, 0, qui n'admet pas d'inverse relativement à $\cdot$. Pourtant, la situation est dans ces deux cas fort différente, car, dans le second, il y a non seulement une seule exception (au lieu d'une infinité) à la règle de l'inversibilité, mais cette exception est en plus bien définie, car il s'agit justement de l'élément neutre de l'addition. Cette remarque nous suggère la définition suivante, caractérisant une nouvelle structure algébrique :

DÉFINITION 3.1. *On appelle « corps » un anneau unitaire $< E, *, \star >$, tel que $< E - \{e_*\}, \star >$ ($e_*$ étant l'élément neutre de $*$ dans $E$) soit un groupe. Comme il est clair que si l'élément neutre de $\star$ dans $E$ était égal à celui de $*$, alors $< E - \{e_*\}, \star >$ ne pourrait pas être un groupe (car il lui manquerait l'élément neutre), cela revient à dire qu'un corps est un anneau unitaire $< E, *, \star >$, tel que tous les éléments de $E$, sauf l'élément neutre de $*$, sont inversibles relativement à $\star$ ; c'est-à-dire un triplet $< E, *, \star >$ composé d'un ensemble $E$ quelconque et de deux opérations $*$ et $\star$ définies sur les éléments de $E$, telles que le couple $< E, * >$ soit un groupe abélien, le couple $< E, \star >$ un magma associatif unitaire, le couple $< E - \{e_*\}, \star >$ ($e_*$ étant l'élément neutre du groupe $< E, * >$) un groupe, et que l'opération $*$ soit distributive sur l'opération $\star$ dans $E$. En d'autres termes, un triplet $< E, *, \star >$ est un corps si et seulement si :*

*i.i) pour tout $x$ et $y$ appartenant à $E$, $x * y$ appartient à $E$ ;*

*i.ii) pour tout $x$ et $y$ appartenant à $E$, $x * y = y * x$ ;*

*i.iii) pour tout $x$, $y$ et $z$ appartenant à $E$, $(x * y) * z = x * (y * z)$ ;*

*i.iv) il y a dans $E$ un (et un seul) élément $e_*$ (l'élément neutre de $*$), tel que pour tout $x$ appartenant à $E$, $x * e_* (= e_* * x) = x$ ;*

*i.v) pour tout $x$ appartenant à $E$, il y a en $E$ un et un seul élément $y_{x,*}$ (l'élément inverse de $x$ relativement à $*$), tel que $x * y_{x,*} (= y_{x,*} * x) = e_*$ ;*

*ii.i) pour tout $x$ et $y$ appartenant à $E$, $x \star y$ appartient à $E$ ;*

*ii.ii) pour tout $x$, $y$ et $z$ appartenant à $E$, $(x \star y) \star z = x \star (y \star z)$ ;*

*ii.iii) il y a dans $E$ un (et un seul) élément $e_\star$ (l'élément neutre de $\star$), différent de $e_*$, tel que pour tout $x$ appartenant à $E$, $x \star e_\star = e_\star \star x = x$ ;*

*ii.iv) pour tout $x$ appartenant à $E$ et différent de $e_*$, il y a dans $E$ un et un seul élément $y_{x,\star}$ (l'élément inverse de $x$ relativement à $\star$ ), tel que pour tout $x$ appartenant à $E$, $x \star y_{x,\star} = y_{x,\star} \star x = e_\star$ ;*

*iii.i) pour tout $x$, $y$ et $z$ appartenant à $E$, $x \star (y * z) = (x \star y) * (x \star z)$.*

*Si l'opération $\star$ est de surcroît commutative en $E$, c'est-à-dire que pour tout $x$ et $y$ appartenant à $E$, $x \star y = y \star x$, alors le corps est dit lui-même « commutatif ».*

Il est alors facile de vérifier que le triplet $< \mathbb{Q}, +, \cdot >$ (mais évidemment pas le triplet $< \mathbb{Q}, \cdot, + >$) est un corps, et en particulier un corps commutatif, tandis que $< \mathbb{Z}, +, \cdot >$ ne l'est pas. Voici donc ce qui, d'un point de vue formel distingue $\mathbb{Q}$ de $\mathbb{Z}$ : le fait que $< \mathbb{Q}, +, . >$ est un corps nous dit que $\mathbb{Q}$ est un substrat bien plus confortable que $\mathbb{Z}$ pour le développement d'une algèbre. Il est facile de voir que la raison qui fait que beaucoup de théorèmes sont démontrables sur $\mathbb{Q}$,

une fois qu'on y a défini l'addition et la multiplication, est justement le fait que la structure $< \mathbb{Q}, +, \cdot >$ est un corps (commutatif). Cela signifie que ces théorèmes peuvent d'emblée être référés à n'importe quel corps (commutatif). On a déjà vu un exemple de cette circonstance pour les anneaux avec le théorème du développement binomial pour un exposant naturel quelconque. Pour exhiber des exemples comparables pour les corps (mais notons que tout corps étant un anneau, le théorème du développement binomial pour un exposant naturel vaut aussi pour tout corps), on devrait développer ici une mathématique un peu plus sophistiquée ; on devrait par exemple introduire la notion d'équation algébrique définie sur un corps $\mathbf{K}$. On ne s'aventurera pas sur ces chemins, que le lecteur motivé pourra pourtant suivre avec bonheur en s'appuyant sur des textes plus élaborés. Ici on se limitera à observer que tout triplet $< E, *, \star >$ qui satisfait aux conditions imposées à un corps est tel que $E$ est fermé par rapport à $*, *^{-1}$ et $\star$ , et $E - \{e_*\}$ est fermé relativement à $\star^{-1}$. C'est exactement cette quadruple fermeture qui fait la puissance algébrique d'un corps et motive l'intérêt pour une telle structure.

Pour ce qui est des dimensions de l'ensemble $E$, il est facile d'observer qu'il n'est pas nécessaire qu'il soit infini et qu'il est même facile de construire des corps finis, même si un ensemble $E$ qui intervient dans un corps doit contenir au moins deux éléments distincts (les deux éléments neutres de $*$ et $\star$).

Pour trouver des exemples simples de corps finis, revenons pour un instant aux tableau (54) exhibant l'addition et la multiplication sur l'ensemble $\mathbb{Z}/7\mathbb{Z}$ des classes de congruence modulo 7. Il est facile de voir que ces tables sont symétriques (ce qui est dû à la commutativité de $+$ et $\cdot$ dans tous les ensembles $\mathbb{Z}/n\mathbb{Z}$) et que dans la deuxième, toutes les lignes, sauf la première (qui relève, comme la première table le montre, de l'élément neutre de l'addition), contiennent l'élément $\overset{7}{1}$, qui (comme le montre la deuxième table) est l'élément neutre de la multiplication. Cela signifie que pour tout élément $\overset{7}{i}$ de $\mathbb{Z}/7\mathbb{Z}$, il est possible de trouver un autre élément $\overset{7}{j}$, du même ensemble, tel que $\overset{7}{i} \cdot \overset{7}{j} = \overset{7}{1}$. Donc tout élément de $\mathbb{Z}/7\mathbb{Z}$ différent de l'élément neutre de l'addition est inversible dans $\mathbb{Z}/7\mathbb{Z}$, relativement à la multiplication définie sur $\mathbb{Z}/7\mathbb{Z}$. Or, comme $< \mathbb{Z}/7\mathbb{Z}, +, \cdot >$ est sans doute un anneau commutatif (car, comme on l'a vu, tout triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$ est un anneau commutatif), cela revient à dire que le triplet $< \mathbb{Z}/7\mathbb{Z}, +, \cdot >$ est un corps commutatif fini d'ordre 7.

La question se pose alors de savoir s'il en est de même pour tout triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$, quel que soit le nombre naturel $n$ plus grand que 1. La réponse à cette question est connue et fort claire : le triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$, est un corps si et seulement si $n$ est un nombre premier (et, si c'est un corps, il est un corps commutatif). Pour qui n'est pas accoutumé aux mathématiques, il n'est pourtant pas si facile de prouver que cette réponse est correcte. Essayons quand même.

Si $n = 2$ et $n = 3$, les tables de la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ sont respectivement les suivantes :

| $\cdot$ | $\overset{2}{0}$ | $\overset{2}{1}$ |
|---|---|---|
| $\overset{2}{0}$ | $\overset{2}{0}$ | $\overset{2}{0}$ |
| $\overset{2}{1}$ | $\overset{2}{0}$ | $\overset{2}{1}$ |

| $\cdot$ | $\overset{3}{0}$ | $\overset{3}{1}$ | $\overset{3}{2}$ |
|---|---|---|---|
| $\overset{3}{0}$ | $\overset{3}{0}$ | $\overset{3}{0}$ | $\overset{3}{0}$ |
| $\overset{3}{1}$ | $\overset{3}{0}$ | $\overset{3}{1}$ | $\overset{3}{2}$ |
| $\overset{3}{2}$ | $\overset{3}{0}$ | $\overset{3}{2}$ | $\overset{3}{1}$ |

et il suffit de raisonner sur ces tables comme on l'a fait sur la deuxième des tables (54) pour conclure que $< \mathbb{Z}/2\mathbb{Z}, +, \cdot >$ et $< \mathbb{Z}/3\mathbb{Z}, +, \cdot >$ sont deux corps commutatifs (qu'on se rappelle que pour tout $n$ différent de 0, l'élément $\overset{n}{0}$ est l'élément neutre de l'addition définie sur $\mathbb{Z}/n\mathbb{Z}$).

Pour trouver des ensembles $\mathbb{Z}/n\mathbb{Z}$, avec $n > 1$, tels que les triplets $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$ ne forment pas un corps, il suffit pourtant de considérer le cas où le nombre naturel $n$ n'est pas un nombre premier. En fait, si c'est le cas, il est toujours possible de trouver deux nombres naturels $h$ et $k$ différents de 1 et de $n$ tels que $n = h \cdot k$. Et comme cela n'est possible que si $1 < h \leq n-1$, $1 < k \leq n-1$ et $n > 3$, il s'ensuit, que les deux classes de congruence modulo $n$ notées « $\overset{n}{h}$ » et « $\overset{n}{k}$ » sont des éléments de $\mathbb{Z}/n\mathbb{Z}$, et sont l'une et l'autre distinctes de la classe $\overset{n}{0}$. Mais, comme $h \cdot k = n$, le produit $h \cdot k$ appartient à la classe $\overset{n}{0}$, et donc, selon la définition de la multiplication entre classes de congruence modulo $n$, $\overset{n}{h} \cdot \overset{n}{k} = \overset{n}{0}$, la classe $\overset{n}{0}$ étant l'élément non inversible de $\mathbb{Z}/n\mathbb{Z}$, relativement à $\cdot$. Donc si $\overset{n}{k}$ admettait un inverse en $\mathbb{Z}/n\mathbb{Z}$, relativement à $\cdot$, alors (en notant par « $\overset{n}{k^{-1}}$ » cet inverse) on aurait autant :

$$\left(\overset{n}{h} \cdot \overset{n}{k}\right) \cdot \overset{n}{k^{-1}} = \overset{n}{h} \cdot \left(\overset{n}{k} \cdot \overset{n}{k^{-1}}\right) = \overset{n}{h} \cdot \overset{n}{1} = \overset{n}{h}$$

que

$$\left(\overset{n}{h} \cdot \overset{n}{k}\right) \cdot \overset{n}{k^{-1}} = \overset{n}{0} \cdot \overset{n}{k^{-1}} = \overset{n}{0}$$

bien qu'on ait montré que $\overset{n}{h} \neq \overset{n}{0}$. Comme en $\mathbb{Z}/n\mathbb{Z}$ la multiplication est commutative, le même raisonnement peut être répété pour $h$. Il s'ensuit que si $n$ n'est pas premier, alors il y a dans $\mathbb{Z}/n\mathbb{Z}$ au moins un élément (car il est bien possible que $h = k$) qui n'est pas inversible.

La table suivante, relative à la multiplication en $\mathbb{Z}/6\mathbb{Z}$ éclaire la situation :

| $\cdot$ | $\overset{6}{0}$ | $\overset{6}{1}$ | $\overset{6}{2}$ | $\overset{6}{3}$ | $\overset{6}{4}$ | $\overset{6}{5}$ |
|---|---|---|---|---|---|---|
| $\overset{6}{0}$ | $\overset{6}{0}$ | $\overset{6}{0}$ | $\overset{6}{0}$ | $\overset{6}{0}$ | $\overset{6}{0}$ | $\overset{6}{0}$ |
| $\overset{6}{1}$ | $\overset{6}{0}$ | $\overset{6}{1}$ | $\overset{6}{2}$ | $\overset{6}{3}$ | $\overset{6}{4}$ | $\overset{6}{5}$ |
| $\overset{6}{2}$ | $\overset{6}{0}$ | $\overset{6}{2}$ | $\overset{6}{4}$ | $\overset{6}{0}$ | $\overset{6}{2}$ | $\overset{6}{4}$ |
| $\overset{6}{3}$ | $\overset{6}{0}$ | $\overset{6}{3}$ | $\overset{6}{0}$ | $\overset{6}{3}$ | $\overset{6}{0}$ | $\overset{6}{3}$ |
| $\overset{6}{4}$ | $\overset{6}{0}$ | $\overset{6}{4}$ | $\overset{6}{2}$ | $\overset{6}{0}$ | $\overset{6}{4}$ | $\overset{6}{2}$ |
| $\overset{6}{5}$ | $\overset{6}{0}$ | $\overset{6}{5}$ | $\overset{6}{4}$ | $\overset{6}{3}$ | $\overset{6}{2}$ | $\overset{6}{1}$ |

On y voit que, $n$ étant égal à $2 \cdot 3$, les éléments $\overset{n}{2}$ et $\overset{n}{3}$ de $\mathbb{Z}/n\mathbb{Z}$ n'ont pas d'inverse (et divisent $\overset{n}{0}$). La même chose est d'ailleurs vraie pour $\overset{n}{4}$, car si $n = 6$, alors $2n = 3 \cdot 4$ et donc $\overset{n}{3} \cdot \overset{n}{4} = 3 \cdot \overset{n}{4} = \overset{n}{0}$.

On a donc montré que si le nombre naturel $n$ n'est pas premier, alors le triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$ n'est pas un corps. Il reste à comprendre ce qui se passe lorsque $n$ est un nombre premier. Imaginons donc que $n$ soit un nombre premier (qu'on pourra prendre plus grand que 3, car on a déjà réglé les cas des nombres premiers 2 et 3). Comme il est clair que pour tout $n$ $\overset{n}{1}$ est l'élément neutre de $*$ dans $\mathbb{Z}/n\mathbb{Z}$, il s'agit de savoir si, un nombre naturel $h$ étant donné, tel que $1 \leq h \leq n-1$, il y a un autre nombre naturel $k$, tel que $1 \leq k \leq n-1$ et que $\overset{n}{h} \cdot \overset{n}{k} = \overset{n}{(h \cdot k)} = \overset{n}{1}$, $\overset{n}{(h \cdot k)}$ étant comme dans (53) la classe de congruence modulo $n$ à laquelle appartient le produit $h \cdot k$. Or, $n$ étant premier, si $q, \nu$ et $\mu$ sont trois nombres naturels tels que $1 \leq q \leq n-1$,

$1 \leq \mu \leq n-1$ et $q \cdot \mu = \nu n$, c'est-à-dire $q = \frac{\nu}{\mu} n$, alors, comme il n'est possible, ni que $\mu = n \cdot s$, pour quelque nombre naturel $s$ (car $\mu < n$), ni que $\frac{n}{\mu}$ soit un nombre naturel, car $n$ est premier et $\mu$ ne peut être égal ni à $n$ (car par hypothèse, $\mu \leq n-1$), ni à 1 (car si $\mu = 1$, alors $q = \nu n$ et il ne serait Ddonc pas possible que $q \leq n-1$), il faut que $\frac{\nu}{\mu}$ soit un nombre naturel, disons $\nu'$. De là il s'ensuit que si $q, \nu$ et $\mu$ sont trois nombres naturels tels que $2 \leq q \leq n-1$, $1 \leq \mu \leq n-1$ et $q \cdot \mu = \nu \cdot n$, alors il y a un nombre naturel $\nu'$, tel que $q = \nu' \cdot n$ et donc :

$$q \cdot \mu \in \overset{n}{0} \Rightarrow q \in \overset{n}{0} \tag{56}$$

Ceci prouvé, considérons les classes

$$\overset{n}{h}, \overset{n}{2h}, ..., \overset{n}{(n-1)h}$$

Il est clair que tout produit entre le nombre $h$ donné et un nombre naturel $k$, tel que $1 \leq k \leq n-1$ appartient à une de ces classes. Comme $n$ est tel que $1 \leq h \leq n-1$, et $n > 3$, il est clair que $h$ n'appartient pas à $\overset{n}{0}$, donc d'après 56, il n'y a pas de nombre naturel $\mu$, tel que $1 \leq \mu \leq n-1$ et $h \cdot \mu \in \overset{n}{0}$. D'où il suit qu'aucune des classes $\overset{n}{h}, \overset{n}{2h}, ..., \overset{n}{(n-1)h}$ n'est égale à $\overset{n}{0}$. Imaginons maintenant que $\mu$ et $\mu'$ soient deux nombres naturels, tels que $1 \leq \mu < \mu' \leq n-1$ et $\overset{n}{\mu \cdot h} = \overset{n}{\mu' \cdot h}$. On aurait alors que : $[(\mu' - \mu) \cdot h] = 0$, ce qui, comme on vient de le voir, ne peut se produire. Il s'ensuit aussi que les classes $\overset{n}{h}, \overset{n}{2h}, ..., \overset{n}{(n-1)h}$ sont toutes différentes. Donc, chacune de ces classes est égale à une et une seule des classes $\overset{n}{1}, \overset{n}{2}, ..., \overset{n}{(n-1)}$ et il n'y en aura qu'une et une seule égale à $\overset{n}{1}$, de sorte qu'il y a un et un seul nombre naturel $k$, tel que $1 \leq k \leq n-1$ et $\overset{n}{k \cdot h} = \overset{n}{1}$.

On a donc prouvé le théorème suivant :

THÉORÈME 3.1. *Le triplet $< \mathbb{Z}/n\mathbb{Z}, +, \cdot >$ est un corps si et seulement si $n$ est un nombre premier, et s'il est un corps, alors il est un corps commutatif fini d'ordre $n$.*

REMARQUE 5.13. Une conséquence immédiate de ce résultat est que tous les théorèmes qu'on démontre sur $\mathbb{Q}$ en ne se servant que du fait que $< \mathbb{Q}, +, \cdot >$ est un corps commutatif, peuvent aussi être démontrés sur l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$, ou l'addition et la multiplication sont définies comme ci-dessus, si et seulement si $n$ est un nombre premier qu'on note généralement par la lettre « $p$ ».

Ceci est le point de départ d'une mathématique abstraite, qu'on peut développer sur les classes de congruence modulo $p$, ainsi que sur toute autre structure qui satisfait aux conditions caractérisant un corps.

## 4. Corps et ordre

Dans les paragraphes précédents, on a graduellement reconnu que l'ensemble $\mathbb{Q}$ des nombres rationnels, sur lesquels sont définies les opérations d'addition et de multiplication, possède les propriétés distinctives d'un corps commutatif. Parmi les propriétés fondamentales qu'on assigne à $\mathbb{Q}$ dans la pratique mathématique, il y en a pourtant une, dont on a longuement discuté dans le chapitre 4, qui n'a fait l'objet d'aucune stipulation propre à la notion de corps, et qui ne peut donc pas être déduite du fait que le triplet $< \mathbb{Q}, +, \cdot >$ est un corps commutatif. Il s'agit naturellement de la propriété d'ordre, que nous avons assignée à $\mathbb{Q}$ en étendant à cet ensemble l'ordre total défini sur $\mathbb{N}$. Ainsi, si on veut procéder à rebours et, au lieu de chercher dans $\mathbb{Q}$ les propriétés d'un corps commutatif, définir $\mathbb{Q}$ comme un corps commutatif particulier, il faut ajouter une stipulation qui assure que l'ensemble intervenant dans ce corps est totalement

ordonné relativement à une certaine relation d'ordre $\leq$, et indiquer les relations qui doivent lier entre elles les opérations définies sur cet ensemble, intervenant dans la structure de corps, et cette relation d'ordre. Pour ce faire, on peut partir de la définition suivante :

DÉFINITION 4.1. *Un corps $< E, *, \star >$ est dit « totalement ordonné relativement à la relation d'ordre $\mathbf{R}$ » si et seulement si l'ensemble $E$ est totalement ordonné relativement à la relation $\mathbf{R}$ et :*

**(*i*):** *pour tout $x, y$ et $z$ appartenant à $E$,*

$$x\mathbf{R}y \Rightarrow (x * z)\mathbf{R}(y * z)$$

**(*ii*):** *pour tout $x$ et $y$ appartenant à $E$,*

$$(e_*\mathbf{R}x) \wedge (e_*\mathbf{R}y) \Rightarrow e_*\mathbf{R}\,(x \star y)$$

*$e_*$ étant, comme ci-dessus, l'élément neutre de $*$ dans $E$.*

*Pour tout $x$ appartenant à $E$, si $e_*\mathbf{R}x$, on dira que $x$ est positif, tandis que si $x\mathbf{R}e_*$ et $x \neq e_*$, on dira que $x$ est négatif. Si $e_*\mathbf{R}x$ et $x \neq e_*$, on dira que $x$ est strictement positif.*

REMARQUE 5.14. Si $x$ et $y$ sont deux éléments de $E$, tels que $x\mathbf{R}y$, et $x^*$ est l'inverse de $x$ par rapport à $*$, alors, d'après la clause $(i)$, on aura, en posant $z = x^*$

$$e_*\mathbf{R}(y * x^*).$$

Si $a$ est ensuite un élément quelconque de $E$, tel que $e_*\mathbf{R}a$, on aura donc, d'après la clause $(ii)$, et la distributivité de $\star$ sur $*$,

$$e_*\mathbf{R}\,[(a \star y) * (a \star x^*)]$$

De là, si $(a \star x^*)^*$ est l'inverse de $(a \star x^*)$ par rapport à $*$, on tire, encore d'après la clause $(i)$ et par l'associativité de $*$,

$$(a \star x^*)^*\,\mathbf{R}\,(a \star y)$$

Mais, en accord à la distributivité de $*$ sur $\star$ et d'après 55 on aura aussi,

$$e_* = a \star e_* = a \star (x * x^*) = (a \star x) * (a \star x^*)$$

et donc, par l'unicité de l'élément neutre, $(a \star x^*)^* = (a \star x)$, et donc

$$(a \star x)\,\mathbf{R}\,(a \star y)$$

Donc, les clauses $(i)$ et $(ii)$ impliquent ensemble la condition suivante

$$a \in E \Rightarrow \{e_*\mathbf{R}a \Rightarrow [x\mathbf{R}y \Rightarrow (a \star x)\,\mathbf{R}\,(a \star y)]\} \tag{57}$$

qui est souvent donnée à la place de la clause $(ii)$, dans la définition d'un corps ordonné. Le lecteur pourra en fait démontrer comme exercice que, si on suppose (57), on peut, à son tour, démontrer cette dernière clause. Il ne trouvera aucune difficulté pour le faire.

Il est facile de voir, grâce à cette définition, que le quadruplet $< \mathbb{Q}, \leq, +, \cdot >$ est un corps commutatif totalement ordonné, tandis que, quel que soit le nombre premier $p$, et, de quelque manière que l'on définisse la relation d'ordre $\leq$ sur $\mathbb{Z}/p\mathbb{Z}$, le quadruplet $< \mathbb{Z}/p\mathbb{Z}, \leq, +, \cdot >$ n'est pas un corps commutatif totalement ordonné.

Une fois cette définition donnée, il sera possible de construire directement $\mathbb{Q}$ comme l'ensemble minimal qui intervient dans un corps commutatif totalement ordonné, généré à partir des éléments 0 et 1 sur lesquels on a défini l'addition, la multiplication et une relation d'ordre articulée sur ces opérations. En revanche, on ne peut pas agir comme on l'a fait dans le cas de la définition axiomatique de $\mathbb{N}$, si on veut limiter les axiomes aux conditions qui définissent un corps commutatif ordonné, car on verra dans le prochain chapitre qu'il est possible de construire

au moins un corps commutatif totalement ordonné, où intervient un ensemble essentiellement différent de $\mathbb{Q}$, c'est-à-dire tel qu'il ne peut pas être mis en bijection avec $\mathbb{Q}$ (ou, comme on le dit, qu'il n'est pas *isomorphe* à $\mathbb{Q}$). C'est la tâche à laquelle il faut donc se consacrer dès maintenant.

CHAPITRE 6

# Nombres réels

Dans le chapitre 4, on a défini les nombres fractionnaires, puis les nombres rationnels, en se réclamant de l'exigence de mesurer d'autres objets que les nombres entiers positifs. Le moment est venu de comprendre pourquoi les nombres rationnels ne peuvent pas suffire, à eux seuls, à satisfaire à cette exigence.

## 1. L'insuffisance des rationnels pour la mesure des segments

Imaginons que deux segments soient donnés et qu'il s'agisse de savoir si l'un des deux mesure l'autre au sens d'Euclide, c'est-à-dire si le deuxième de ces segments peut être obtenu en additionnant le premier à lui-même, un certain nombre des fois. Pour cela, il faudra avoir d'abord défini une addition sur les segments. Si, en suivant Euclide, on suppose que la somme de deux segments quelconques est le segment qui résulte en juxtaposant de manière rectiligne ces segments l'un à l'autre, il suffira, pour parvenir à une définition convenable, de disposer d'une procédure géométrique permettant de construire un ou plusieurs segments égaux à tout segment donné, pouvant être pris comme des répliques de ce même segment, dans n'importe quelle position du plan. La mise au point de cette procédure est l'un des objectifs les plus fondamentaux des *Éléments* d'Euclide et il a fait, dans l'histoire, l'objet de nombreuses discussions. Comme il ne s'agit pas ici de parler de géométrie, on laissera ce point de côté, et on supposera qu'on sait additionner un segment à lui-même, en le reportant de surcroît sur un autre, de sorte à vérifier d'emblée si la somme ainsi obtenue est plus petite, plus grande ou égale à ce dernier segment (si on veut un support intuitif pour cette opération, on peut imaginer que l'on dispose d'un compas à ouverture fixe, chose que d'ailleurs Euclide s'interdit d'utiliser).

Note Historique 6.1. On a souvent affirmé que la géométrie euclidienne, comme elle est exposée par Euclide dans les *Éléments*, présuppose, entre autres choses, la possibilité de déplacer un segment donné sur le plan auquel il appartient. Cette possibilité serait par exemple à la base de la définition de l'égalité entre deux segments en tant que congruence de ces segments : si l'on admet que pour Euclide deux segments sont égaux si et seulement s'ils sont exactement superposables l'un à l'autre, alors on doit supposer qu'il est possible, pour Euclide, de poser un segment sur un autre et, pour ce faire, de le déplacer. Celle-ci me semble pourtant une manière fort imprécise de décrire la situation.

Il faut observer d'abord que pour Euclide, cela n'aurait eu aucun sens de supposer la possibilité d'un déplacement d'un segment sur le plan sans spécifier la manière dont ce déplacement pouvait être obtenu. Pour Euclide, il ne suffisait pas de définir définition/existence d'un objet dans la géométrie d'Euclide un objet géométrique, pour pouvoir en disposer, c'est-à-dire pour s'assurer de son existence ; une définition n'est que la présentation d'une condition à laquelle un objet doit satisfaire, et une fois que cette condition est présentée, rien ne nous assure qu'elle puisse être satisfaite par un certain objet ; seulement si on peut s'assurer de cette possibilité, on peut

affirmer que la définition donnée est celle d'un objet géométrique. Cela signifie que, pour Euclide, il y a une modalité de donation d'objets géométriques essentiellement distincte de leur simple définition. Une définition n'est qu'un outil de classification des objets géométriques donnés indépendamment. Pour être utile, il faut qu'elle caractérise un objet qui peut effectivement être donné. Ainsi, on pourrait de la même manière définir un triangle et un biangle ; ce n'est pas la nature de la définition qui fait que le premier est un objet de la géométrie euclidienne et le deuxième ne l'est pas : c'est que dans cette géométrie on peut donner un objet qu'on reconnaît, d'après la première définition, comme un triangle, tandis qu'on ne peut donner aucun objet qu'on reconnaîtrait, d'après la deuxième définition, comme un biangle.

Or, si on se limite à la géométrie du plan, donner un objet géométrique signifie pour Euclide parvenir à construire cet objet à partir de la donnée originelle d'un nombre fini de segments quelconques et en opérant en accord avec un nombre fini de clauses constructives déterminées à l'avance. Le fait qu'Euclide suppose, comme point de départ de ses constructions, la donation préalable d'un nombre fini de segments quelconques ne signifie pas que pour Euclide tout segment peut être supposé comme donné, sans qu'il résulte d'une construction. Les segments qui sont donnés originellement sont des segments quelconques, et non pas des segments qui satisfont à certaines conditions. Si on veut se donner un segment qui satisfait à une certaine condition, il faut le construire à partir d'autres segments qui sont supposés être donnés préalablement, de manière totalement indépendante de cette condition.

L'exemple le plus typique de cette situation est justement celui qu'on décrit souvent, de façon un peu trop sommaire, en parlant de déplacements. Imaginons qu'un segment quelconque est donné originellement, et que l'on ait, d'une manière qu'il ne sera pas nécessaire ici de préciser, fixé un point sur le plan auquel appartient ce segment qui ne coïncide pas avec une des deux extrémités du segment donné. On se demande si l'on peut donner un segment, égal au segment déjà donné, dont une des extrémités coïncide avec ce point. Pour Euclide, la réponse à cette question — qui n'est autre que le problème posé par la deuxième proposition du premier livre des *Éléments* — consiste dans l'exhibition d'une procédure qui, en n'appliquant que les clauses constructives préalablement acceptées et à partir de la donné du premier segment, conduit à la construction d'un segment satisfaisant à la condition indiquée. Déplacer un segment donné signifie donc, pour Euclide, construire un autre segment, dans une certaine position du plan, qu'on puisse reconnaître comme étant égal au segment donné.

Pour préciser dans les détails comment ceci pourrait être fait, il faudrait présenter les clauses constructives dont Euclide se réclame dans ses constructions, et éclairer la manière selon laquelle Euclide définit la relation d'égalité entre deux segments. Ceci nous conduirait assez loin dans l'examen de la structure logique-déductive du livre I des *Éléments*. Il suffira ici de décrire la situation en termes plutôt généraux.

D'abord, il devrait apparaître clairement, de ce que je viens de dire, que la relation d'égalité entre deux segments ne peut se réclamer, d'aucune manière, de la possibilité de déplacer un de ces segments en le posant sur l'autre, car c'est au contraire la caractérisation de l'opération de déplacement d'un segment qui se réclame de la possibilité de déclarer deux segments comme égaux. Pour comprendre comment Euclide définit, d'ailleurs implicitement, la relation d'égalité entre deux segments, il faut commencer par la considération des clauses constructives qu'il s'autorise à employer. Même si une analyse plus fine des arguments avancés par Euclide nous montre la

présence d'autres clauses constructives implicites, qu'on ne pourra pas préciser ici, on peut dire que, pour l'essentiel, les constructions d'Euclide se réclament de trois clauses constructives, respectivement énoncées par les trois premiers des cinq postulats qui précèdent le déroulement du premier livre des *Éléments* (un discours un peu plus complexe devrait concerner le cinquième postulat, qui, à mon opinion, énonce une quatrième clause constructive ; pour ce qui est des buts de la note présente, on peut toutefois laisser ce discours de côté). Ces clauses sont les suivantes : i) deux points étant donnés, on peut tracer un segment qui joint ces points ; ii) un segment étant donné, on peut le prolonger (jusqu'à rencontrer une ligne donnée) ; iii) un segment étant donné, on peut tracer un cercle dont ce segment est le rayon et une des extrémités de ce segment est le centre. Cette dernière clause constructive assigne au cercle un rôle assez particulier. Bien qu'Euclide ne se donne pas la liberté de supposer qu'un cercle puisse être donné originellement, comme peut être un segment, il se garantit la possibilité de construire un cercle, pour ainsi dire, par un acte élémentaire qui ne tient qu'à une application d'une clause constructive acceptée : toutes les fois qu'un segment est donné, on peut passer d'emblée de ce segment à un cercle dont ce segment est le rayon. Un cercle est d'ailleurs défini, dans la définition 15 du livre I, comme « une figure plane contenue par une ligne unique par rapport à laquelle toutes les droites [qu'on lise : les segments] menées à sa rencontre à partir d'un unique point parmi ceux qui sont placés à l'intérieur de la figure, sont égales entre elles ». Pourtant, d'après Euclide, ce n'est pas l'égalité des segments qui définit le cercle ; c'est au contraire le cercle qui définit l'égalité des segments. Si un segment est donné, nous dit Euclide, on peut tracer, grâce à la clause (iii), le cercle dont ce segment est le rayon ; si, ensuite, en appliquant soit la clause (i), soit la clause (ii), on peut tracer un segment qui joint le centre du cercle à sa circonférence, alors on pourra se réclamer de la définition du cercle pour en conclure que le segment ainsi tracé est égal au segment à partir duquel on avait tracé le cercle. Si deux segments sont rayons du même cercle, ils sont donc égaux. Ceci n'est pourtant qu'une condition suffisante pour l'égalité entre deux segments. Pour parvenir à une condition nécessaire et suffisante, il faut se réclamer de la transitivité de la relation d'égalité et de sa stabilité par rapport à l'addition et la soustraction d'égaux, deux conditions générales, valables pour toute sorte de relation d'égalité, que Euclide énonce dans les trois premières notions communes (des axiomes de nature générale que Euclide fait suivre aux postulats, au début du livre I des *Éléments*). Pour s'assurer que deux segments, qui ne sont pas rayons du même cercle, sont égaux, il faut donc s'arranger pour montrer que ces segments sont, tous les deux, égaux au même segment, ou résultent de l'addition ou de la soustraction de segments égaux à deux segments égaux, et ceci en partant évidemment d'une ou plusieurs égalités entre deux segments, garanties pas le fait que ces segments sont rayons du même cercle.

Cette dernière stratégie est justement celle qui permet à Euclide de reconnaître comme égaux deux segments, dont un est donné et l'autre résulte, à partir de celui-ci, d'une construction particulière qui est exhibée lors de la solution du problème posé par la proposition I.2. De là Euclide en conclut que, un segment étant donné, on peut en construire un autre, égal à celui-ci, dans une autre position du plan. Évidemment, s'il ne s'agit que de sommer un segment à lui-même, les choses sont beaucoup plus simples. Il suffit, le segment en question étant donné, d'appliquer la clause (iii) pour tracer le cercle dont ce segment est le rayon et, ensuite, la clause (ii) pour prolonger le segment donné jusqu'à la circonférence du cercle ainsi construit. On aura ainsi en

même temps deux nouveaux segments : un nouveau rayon de ce cercle, qui sera, de ce fait, égal au segment donné ; et le segment résultant de la juxtaposition de ce rayon avec le segment donné, qui sera justement la somme cherchée.

**Lectures possibles** : Ian Mueller, *Phylosophy of Mathematics and Deductive Structure in Euclid's* Elements, MIT Press, Cambridge (Mass.), London, 1981.

Soient alors PQ et MN deux segments (non nuls), qu'on sait reporter l'un sur l'autre (par la suite, sauf indication contraire, je parlerai toujours de « segments » pour me référer à des segments non nuls), et qu'il s'agisse de savoir combien de fois un de ces segments, disons PQ, peut être reporté sur l'autre. En traduisant ce problème en termes arithmétiques, il s'agit de déterminer un nombre naturel $n$, tel que

$$n(\mathsf{PQ}) \leq \mathsf{MN} < (n+1)(\mathsf{PQ}) \tag{58}$$

(pourvu que, quels que soient le nombre naturel $s$ et le segment $K$, on ait, comme dans le chapitre 4, $\underbrace{K+K+...+K}_{s \text{ fois}} = sK$).

Il y a un sens dans lequel la détermination du nombre naturel $n$ qui satisfait à (58) nous renseigne à elle seule sur la relation de mesure qui lie entre eux les segments MN et PQ, car de (58) il suit que le segment PQ peut être reporté sur le segment MN tout au plus $n$ fois. Il est pourtant facile de comprendre que cette même relation de mesure a lieu entre l'un quelconque des deux segments MN et PQ et une infinité de segments différents entre eux. Si l'un des deux segments MN et PQ est déterminé, il ne suffit donc pas de supposer ou de savoir qu'il est dans cette relation de mesure avec un certain segment, pour que ce dernier segment soit à son tour déterminé. On dira alors que le nombre naturel $n$ ne fournit qu'une « mesure approximative » du segment MN en termes du segment PQ . Si on veut parvenir à la détermination d'une mesure précise du segment MN en termes du segment PQ, c'est-à-dire d'une relation $\mathbf{M}$ entre ces deux segments — qui dépende du résultat de la procédure consistant à reporter le segment PQ sur le segment MN autant de fois qu'il est possible de le faire, et qui soit telle que, lorsque le segment PQ est déterminé, le segment MN soit à son tour déterminé de manière univoque par son seul être dans la relation $\mathbf{M}$ avec le segment PQ —, il faut, ou bien s'assurer que $n(\mathsf{PQ}) = \mathsf{MN}$ (ce qui entraïne évidemment que $n \neq 0$), si ceci n'était pas le cas, continuer à raisonner comme il suit.

D'abord, on devrait se demander combien de fois une certaine partie $\mathsf{PQ}_1$ de PQ — c'est-à-dire un segment $\mathsf{PQ}_1$ qui mesure PQ au sens d'Euclide — peut être reporté sur la différence $\mathsf{MN} - n(\mathsf{PQ})$. Soit alors, par hypothèse, $\mathsf{PQ} = m_1(\mathsf{PQ}_1)$, $m_1$ étant évidemment un nombre naturel plus grand que 1. Il s'agirait alors de déterminer un nombre naturel $n_1$, tel que :

$$n_1(\mathsf{PQ}_1) \leq \mathsf{MN} - n(\mathsf{PQ}) < (n_1+1)(\mathsf{PQ}_1)$$

ou bien

$$n_1(\mathsf{PQ}_1) \leq \mathsf{MN} - n \cdot m_1(\mathsf{PQ}_1) < (n_1+1)(\mathsf{PQ}_1)$$

Si $n_1$ était différent de 0 et tel que

$$\mathsf{MN} - n(\mathsf{PQ}) = \mathsf{MN} - n \cdot m_1(\mathsf{PQ}_1) = n_1(\mathsf{PQ}_1)$$

ou bien, en posant $n = n_0$ et $\mathsf{PQ} = \mathsf{PQ}_0$

$$\begin{aligned} \mathsf{MN} &= n_0(\mathsf{PQ}_0) + n_1(\mathsf{PQ}_1) \\ &= n_0 \cdot m_1(\mathsf{PQ}_1) + n_1(\mathsf{PQ}_1) \\ &= (n_0 \cdot m_1 + n_1)\,(\mathsf{PQ}_1) \end{aligned}$$

alors le problème serait résolu, car on pourrait dire que le segment $\mathsf{PQ}_1$ peut être reporté exactement $n_0 \cdot m_1 + n_1$ fois sur le segment $\mathsf{MN}$, d'où il suit que

$$\mathsf{MN} = \left(n_0 + \frac{n_1}{m_1}\right)(\mathsf{PQ}) = \left(\frac{n_0 \cdot m_1 + n_1}{m_1}\right)(\mathsf{PQ})$$

Mais si ce n'était pas ainsi, on devrait se demander combien de fois une certaine partie $\mathsf{PQ}_2$ de $\mathsf{PQ}_1$, et donc de $\mathsf{PQ}$, peut être reportée sur la différence

$$[\mathsf{MN} - n(\mathsf{PQ})] - n_1(\mathsf{PQ}_1) = \mathsf{MN} - [n \cdot m_1(\mathsf{PQ}_1) + n_1(\mathsf{PQ}_1)]$$

On posera alors par hypothèse $\mathsf{PQ}_1 = m_2(\mathsf{PQ}_2)$, ou bien $\mathsf{PQ} = m_1 \cdot m_2(\mathsf{PQ}_2)$, $m_1$ étant un nombre naturel plus grand que 1, et on cherchera un nombre naturel $n_2$, tel que ;

$$n_2(\mathsf{PQ}_2) \leq [\mathsf{MN} - n(\mathsf{PQ})] - n_1(\mathsf{PQ}_1) < (n_2 + 1)(\mathsf{PQ}_2)$$

ou bien

$$n_2(\mathsf{PQ}_2) \leq \mathsf{MN} - [n \cdot m_1(\mathsf{PQ}_1) + n_1(\mathsf{PQ}_1)] < (n_2 + 1)(\mathsf{PQ}_2)$$

ou encore

$$n_2(\mathsf{PQ}_2) \leq \mathsf{MN} - [n \cdot m_1 \cdot m_2(\mathsf{PQ}_2) + n_1 \cdot m_2(\mathsf{PQ}_2)] < (n_2 + 1)(\mathsf{PQ}_2)$$

Si $n_2$ était différent de 0 et tel que

$$[\mathsf{MN} - n(\mathsf{PQ})] - n_1(\mathsf{PQ}_1) = n_2(\mathsf{PQ}_2)$$

ou bien, en posant encore $n = n_0$ et $\mathsf{PQ} = \mathsf{PQ}_0$,

$$\begin{array}{rcl} \mathsf{MN} & = & n_0(\mathsf{PQ}_0) + n_1(\mathsf{PQ}_1) + n_2(\mathsf{PQ}_2) \\ & = & n_0 \cdot m_1 \cdot m_2(\mathsf{PQ}_2) + n_1 \cdot m_2(\mathsf{PQ}_2) + n_2(\mathsf{PQ}_2) \\ & = & (n_0 \cdot m_1 \cdot m_2 + n_1 \cdot m_2 + n_2) \cdot (\mathsf{PQ}_2) \\ & = & \frac{n_0 \cdot m_1 \cdot m_2 + n_1 \cdot m_2 + n_2}{m_1 m_2}(\mathsf{PQ}) \end{array}$$

on aurait évidemment fini ; sinon, on devrait recommencer de la même manière.

Sans multiplier les exemples, on imagine que, au bout de $\nu+1$ réitérations de cette opération ($\nu$ étant évidemment un nombre naturel), on arrive à l'égalité

$$\mathsf{MN} = \sum_{i=0}^{\nu} n_i(\mathsf{PQ}_i) \tag{59}$$

c'est-à-dire

$$\begin{array}{rcl} \mathsf{MN} & = & [n_0(m_1 \cdot ... \cdot m_\nu) + n_1(m_2 \cdot \ldots \cdot m_\nu) + ... \\ & & \ldots + n_{\nu-1} \cdot (m_\nu) + n_\nu](\mathsf{PQ}_\nu) \\ & = & \left[n_\nu + \sum_{i=0}^{\nu-1} n_i(m_{i+1} \cdot m_{i+2} ... \cdot m_\nu)\right](\mathsf{PQ}_\nu) \\ & = & \left[n_\nu + \sum_{i=0}^{\nu-1} n_i \left(\prod_{j=i+1}^{\nu} m_j\right)\right](\mathsf{PQ}_\nu) \qquad (60) \\ & = & \left[\frac{n_\nu + \sum\limits_{i=0}^{\nu-1} n_i \left(\prod\limits_{j=i+1}^{\nu} m_j\right)}{\prod\limits_{j=1}^{\nu} m_j}\right](\mathsf{PQ}) \end{array}$$

où $m_1$, $m_2$, ..., $m_\nu$ sont tous des nombres naturels plus grands que 1. C'est à ce point, et seulement à ce point, qu'on aura définitivement résolu le problème sans aucune approximation.

Or, la nouvelle question qui se pose, tout naturellement, est la suivante : est-on sûr que, pour tout couple donné de segments $\mathsf{PQ}$ et $\mathsf{MN}$, on peut arriver, au bout un certain nombre $\nu + 1$ d'étapes (aussi grand que l'on veut), à des égalités comme (59) et (60) ? On va chercher une réponse à cette question.

Observons d'abord que, quel que soit le nombre naturel $\nu$, l'addition

$$n_\nu + \sum_{i=0}^{\nu-1} n_i \left( \prod_{j=i+1}^{\nu} m_j \right)$$

qui intervient dans la (60) est une addition de produits de nombres naturels, c'est-à-dire une addition de nombres naturels. Sa somme est donc sans doute un nombre naturel, et, dans le cas en question, ce nombre sera évidemment différent de 0. Indiquons ce nombre naturel par le symbole « $p_\nu$ ». L'égalité (60) pourra alors s'écrire ainsi :

$$\mathsf{MN} = p_\nu(\mathsf{PQ}_\nu) \tag{61}$$

où $p_\nu$ est un nombre naturel différent de 0. De là il suit que si la réponse à notre question est positive, c'est-à-dire qu'on peut, pour tout couple donné de segments $\mathsf{PQ}$ et $\mathsf{MN}$, et au bout d'un certain nombre $\nu+1$ d'étapes, parvenir à des égalités comme (59) et (60), alors, pour tout couple de segments $\mathsf{PQ}$ et $\mathsf{MN}$, il y a un nombre naturel $p_\nu \neq 0$, qui satisfait à (61), pourvu que

$$\begin{aligned} \mathsf{PQ} &= m_0(\mathsf{PQ}) = m_0 \cdot m_1(\mathsf{PQ}_1) = m_0 \cdot m_1 \cdot m_2(\mathsf{PQ}_2) = ... = \\ &= m_0 \cdot m_1 \cdot ... \cdot m_\nu(\mathsf{PQ}_\nu) \end{aligned} \tag{62}$$

où $m_0 = 1$ et $m_1$, $m_2$, ..., $m_\nu$ sont tous des nombres naturels plus grands que 1.

Or, comme le produit d'un nombre quelconque de nombres naturels est un nombre naturel, on pourra poser $m_0 \cdot m_1 \cdot ... \cdot m_\nu = q_\nu$ et écrire (63) comme suit

$$\mathsf{PQ} = q_\nu(\mathsf{PQ}_\nu)$$

$q_\nu$ étant évidemment un nombre naturel différent de 0. La (61) peut alors s'écrire sous la forme

$$\mathsf{MN} = \frac{p_\nu}{q_\nu}(\mathsf{PQ}) \qquad \text{ou bien} \qquad q_\nu(\mathsf{MN}) = p_\nu(\mathsf{PQ}) \tag{63}$$

où $p_\nu$ et $q_\nu$ sont deux nombres naturels différents de 0, et $\frac{p_\nu}{q_\nu}$ est donc un nombre rationnel strictement positif. Il s'ensuit que si la réponse à notre question est positive, c'est-à-dire si on peut, pour tout couple de segments $\mathsf{PQ}$ et $\mathsf{MN}$ qu'on peut prendre au départ, et au bout d'un certain nombre $\nu + 1$ d'étapes, parvenir à des égalités comme (59) et (60), alors, pour tout couple de segments $\mathsf{PQ}$ et $\mathsf{MN}$, il y a deux nombres naturels $p_\nu$ et $q_\nu$ différents de 0, et, donc, un nombre rationnel strictement positif $\frac{p_\nu}{q_\nu}$, qui satisfont à (63).

Mais nous nous étions posé la question de savoir s'il est possible de parvenir à des égalités comme (59) et (60), parce que nous avions remarqué que cette possibilité, et elle seule, garantissait que notre problème originaire, celui de la relation de mesure entre deux segments quelconques, pouvait à son tour être résolu, de manière exacte, selon la procédure exhibée. On est arrivé donc au résultat suivant : le problème de la relation de mesure entre deux segments quelconques peut être résolu de manière exacte, selon la procédure qu'on a exhibée, seulement si pour tout couple de segments $\mathsf{PQ}$ et $\mathsf{MN}$, il y a un nombre rationnel strictement positif, qu'on pourrait indiquer par « $\frac{p}{q}$ », tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$.

Réfléchissons maintenant à la différence entre les deux sens selon lesquels on a parlé de solution pour le problème de la mesure d'un segment en termes d'un autre segment. Il est clair

que se limiter à résoudre ce problème dans le premier sens, c'est-à-dire par approximation, signifie accepter, comme on l'a déjà observé, qu'il soit possible que deux segments distincts et différents entre eux, $\mathsf{MN}$ et $\mathsf{MN}'$, entretiennent avec un autre segment $\mathsf{PQ}$ la même relation de mesure. Il suffit en fait qu'il y ait un nombre naturel $n$ tel que

$$n(\mathsf{PQ}) \leq \mathsf{MN} < (n+1)(\mathsf{PQ}) \qquad \text{et} \qquad n(\mathsf{PQ}) \leq \mathsf{MN}' < (n+1)(\mathsf{PQ})$$

pour que les segments $\mathsf{MN}$ et $\mathsf{MN}'$ entretiennent, dans le premier sens du terme, la même relation de mesure avec le segment $\mathsf{PQ}$, c'est-à-dire que ce dernier segment ne peut être reporté, autant sur le segment $\mathsf{MN}$ que sur le segment $\mathsf{MN}'$, que $n$ fois. Le passage au deuxième sens correspond au désir d'éviter cette ambiguïté et de donner à la relation de mesure entre deux segments $\mathsf{MN}$ et $\mathsf{PQ}$ un sens tel que deux segments distincts $\mathsf{MN}$ et $\mathsf{MN}'$ entretiennent avec le même segment $\mathsf{PQ}$ la même relation de mesure si et seulement s'ils sont égaux entre eux. On a donc conclu ceci : si $\mathbf{M}$ est une certaine relation de mesure entre deux segments quelconques, telle que, si $\mathsf{XY}$, $\mathsf{XY}'$ et $\mathsf{HK}$ sont trois segments, alors

$$(\mathsf{XY})\mathbf{M}(\mathsf{HK}) \qquad \text{et} \qquad (\mathsf{XY}')\mathbf{M}(\mathsf{HK})$$

si et seulement si $\mathsf{XY} = \mathsf{XY}'$, alors la procédure précédente nous permet d'établir la relation $\mathbf{M}$, que deux segments donnés quelconques $\mathsf{MN}$ et $\mathsf{PQ}$ entretiennent entre eux, seulement s'il y a un nombre rationnel strictement positif $\frac{p}{q}$, tel que

$$\mathsf{MN} = \frac{p}{q}(\mathsf{PQ}) \tag{64}$$

Or — comme si $\mathsf{MN} \neq \mathsf{MN}'$ et $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, alors $\mathsf{MN}' \neq \frac{p}{q}(\mathsf{PQ})$ — il est naturel d'associer à une égalité comme (64) une relation de mesure déterminée entre les segments $\mathsf{MN}$ et $\mathsf{PQ}$ qui satisfait à la condition indiquée et dire donc que si $\mathsf{MN}$ et $\mathsf{PQ}$ sont deux segments tels qu'il y a un nombre rationnel strictement positif $\frac{p}{q}$ pour lequel $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, alors le segment $\mathsf{MN}$ est dans la relation $\mathbf{M}_{\frac{p}{q}}$ avec $\mathsf{PQ}$, c'est-à-dire que

$$(\mathsf{MN})\mathbf{M}_{\frac{p}{q}}(\mathsf{PQ})$$

Notre raisonnement nous conduit alors à dire que la méthode indiquée fournit une relation de mesure déterminée $\mathbf{M}_\alpha$ entre deux segments quelconques $\mathsf{MN}$ et $\mathsf{PQ}$ seulement s'il y a un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$.

Remarque 6.1. Le lecteur aura compris comment, en passant du premier au second sens de la relation de mesure entre deux segments et, en introduisant les nombres rationnels comme outils, on est passé *de facto* de l'idée euclidienne de mesure à une idée beaucoup plus proche de l'idée moderne. Car, il suffit de décider que le segment $\mathsf{PQ}$ est une unité de mesure universelle pour interpréter un éventuel résultat de la procédure précédente, qui pourra s'écrire sous la forme de l'égalité $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, comme une condition suffisante pour pouvoir réécrire l'autre égalité $\mathsf{MN} = \frac{p}{q}$.

Le lecteur le plus attentif aura aussi compris que le choix des nombres $m_i$ détermine la valeur des nombres $n_i$ $(i = 1, 2, ..., \nu)$. Cela ne signifie pas pourtant que, s'il existe un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, alors on peut choisir les nombres $m_i$ de n'importe quelle manière et parvenir toujours, au bout d'un nombre fini $\nu$ d'étapes, à la détermination du nombre $\frac{p}{q}$ et donc à la fixation de la relation de mesure exacte que les deux segments $\mathsf{PQ}$ et $\mathsf{MN}$ entretiennent entre eux. Imaginons par exemple que $\mathsf{MN} = 10a$ et $\mathsf{PQ} = 3a$, $a$ étant un segment quelconque. Alors on aura $n_0 = 3$ ; et si on pose $m_1 = m_2 = ... = 10$, la procédure ne s'arrêtera jamais, tandis qu'il suffit de poser $m_1 = 3$ pour avoir $\mathsf{PQ}_1 = a$ et donc $n_1 = 1$, ce qui permettra d'arrêter la procédure avec le résultat

$\mathsf{MN} = \left[3 + \frac{1}{3}\right] \mathsf{PQ} = \frac{10}{3}\mathsf{PQ}$, qui satisfera aux conditions définissant une relation de mesure exacte.

Mais, il est clair aussi que ceci ne signifie pas que le premier choix ($m_1 = m_2 = \ldots = 10$) aboutit à un résultat différent du second ; cela serait pour nous fort inattendu, car ce résultat consiste, en définitive, dans la détermination d'une relation entre les segments $\mathsf{MN}$ et $\mathsf{PQ}$ qui ne devrait dépendre en rien de la méthode de mesure choisie, et ne tenir qu'à la nature relative de ces segments.

La situation deviendra plus claire quand on aura observé que si on pose $m_1 = m_2 = \ldots = 10$, on a, dans le cas de notre exemple, les égalités $n_1 = n_2 = \ldots = 3$, qui donnent successivement les résultats

$$\begin{aligned} \mathsf{MN} &= 3\,(\mathsf{PQ}) + a \\ &= 3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + \frac{1}{10}a \\ &= 3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + 3\,(\mathsf{PQ}_2) + \frac{1}{100}a \\ &\ldots \end{aligned}$$

ou bien

$$\begin{aligned} \mathsf{MN} &= 3\,(\mathsf{PQ}) + a \\ &= \left(3 + \frac{3}{10}\right)(\mathsf{PQ}) + \frac{1}{10}a \\ &= \left(3 + \frac{3}{10} + \frac{3}{100}\right)(\mathsf{PQ}) + \frac{1}{100}a \\ &\ldots \end{aligned}$$

Or, pour pouvoir s'assurer que cette suite de résultats ne contredit pas le tout simple résultat obtenu en posant $m_1 = 3$, il faut pouvoir s'assurer que les sommes des additions

(65)
$$\begin{aligned} &3\,(\mathsf{PQ}) + a \\ &3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + \frac{1}{10}a \\ &3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + 3\,(\mathsf{PQ}_2) + \frac{1}{100}a \\ &\ldots \end{aligned}$$

sont toutes égales à $\frac{10}{3}\,(\mathsf{PQ})$. On peut penser que ceci est très aisé, car, selon notre hypothèse, on aura $a = \frac{1}{3}\,(\mathsf{PQ})$ et donc, successivement :

$$\begin{aligned} 3\,(\mathsf{PQ}) + a &= \left(3 + \frac{1}{3}\right)(\mathsf{PQ}) = \frac{10}{3}\,(\mathsf{PQ}) \\ 3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + \frac{1}{10}a &= \left(3 + \frac{3}{10} + \frac{1}{30}\right)(\mathsf{PQ}) = \frac{10}{3}\,(\mathsf{PQ}) \\ 3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + 3\,(\mathsf{PQ}_2) + \frac{1}{100}a &= \left(3 + \frac{3}{10} + \frac{3}{100} + \frac{1}{300}\right)(\mathsf{PQ}) = \frac{10}{3}\,(\mathsf{PQ}) \\ &\ldots \end{aligned}$$

Il suffit pourtant de réfléchir un seul instant sur la manière dont ces résultats sont obtenus pour comprendre que le succès des calculs précédents dépend du fait qu'on connaît *a priori* la relation de mesure entre les segments $\mathsf{PQ}$ et $\mathsf{MN}$, grâce aux hypothèses $\mathsf{PQ} = 3a$ et

$\mathsf{MN} = 10a$. Si ces hypothèses n'avaient pas été avancées, et si l'on travaillait sur des segments quelconques $\mathsf{PQ}$ et $\mathsf{MN}$, dont la relation de mesure n'était pas connue, alors les termes $a, \frac{1}{10}a, \frac{1}{100}a, \ldots$ des additions (65) ne pourraient être déterminés que par approximation et toujours lors de l'étape successive à celle dans laquelle ils apparaissent. Ces additions devraient alors s'écrire ainsi :

$$\begin{aligned} &3\,(\mathsf{PQ}) + R_0 \\ &3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + R_1 \\ &3\,(\mathsf{PQ}) + 3\,(\mathsf{PQ}_1) + 3\,(\mathsf{PQ}_2) + R_2 \\ &\ldots \end{aligned}$$

où $R_0, R_1, R_2, \ldots$ sont des restes indéterminés, qui se déterminent, par approximation, en avançant dans la procédure. On comprendra alors que la différence entre les deux choix précédents des nombres $m_i$ $(i = 1, 2, \ldots)$ tient à ce que d'après le second choix, le résultat correct ne peut être obtenu, par le biais de notre procédure, que s'il était déjà connu, car à aucune étape de cette procédure, les résultats obtenus permettent de prévoir les résultats qui seront obtenus lors des étapes suivantes.

Tout ce qu'on peut dire est donc que si les deux segments $\mathsf{MN}$ et $\mathsf{PQ}$ sont tels qu'il y a un nombre rationnel $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, alors il est toujours possible de choisir les nombres $m_i$ $(i = 1, 2, \ldots)$, de manière à obtenir, grâce à notre procédure, et au bout d'un nombre fini d'étapes, le résultat cherché.

De tout ce qu'on a dit, il suit que la procédure précédente ne peut fournir une méthode pour déterminer la relation de mesure exacte entre deux segments $\mathsf{MN}$ et $\mathsf{PQ}$ que si ces segments sont entre eux dans un rapport rationnel et que, s'il en est ainsi, alors cette procédure peut toujours fournir cette méthode (pourvu que le choix des nombres $m_1$, $m_2, \ldots$ soit convenable). Tout notre raisonnement nous conduit alors à la conclusion suivante : la procédure précédente permet d'assigner à un segment quelconque $\mathsf{MN}$ une valeur numérique déterminée (relativement à l'unité de mesure $\mathsf{PQ}$) seulement si on a choisi l'unité de mesure $\mathsf{PQ}$ de manière qu'il existe un nombre rationnel positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$.

Remarque 6.2. Arrivés à ce point, il est nécessaire de s'arrêter un instant pour réfléchir sur la forme logique de l'argument précédent. On est partis d'une constatation facile : si la procédure précédente s'arrête au bout d'un nombre fini $\nu+1$ d'étapes, avec la détermination d'une égalité telle que (60), alors il existe un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$. On a ensuite exprimé cette implication sous une forme équivalente, en disant que la procédure précédente s'arrête au bout d'un nombre fini $\nu + 1$ d'étapes, avec la détermination d'une égalité telle que (60) seulement s'il existe un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$. Cette nouvelle formulation est évidemment logiquement équivalente à la première, mais, à la différence de celle-ci, suggère qu'il y a un sens à affirmer l'existence d'un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$, indépendamment de la détermination de ce nombre par une procédure telle que la précédente.

On peut pourtant se demander ce que cette hypothèse d'existence pourrait vouloir dire, lorsqu'elle est prise comme une hypothèse préalable et donc indépendante de la considération du résultat obtenu par une procédure telle que la précédente. La remarque précédente semble suggérer une réponse, qui découle d'ailleurs, tout naturellement, des considérations contenues dans le chapitre 4 : l'existence d'un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$ équivaut à l'existence d'une mesure commune (au sens d'Euclide), disons $a$,

aux segments PQ et MN. On pourrait pourtant ne pas être satisfait de cette réponse, car elle se réclame à son tour d'une existence qu'on ne sait pas comment assurer, sauf par la constatation de deux égalités telles que $\mathsf{PQ} = qa$ et $\mathsf{MN} = pa$, qui, si, elles ne dépendent pas de l'application d'une procédure telle que la précédente, rendent la mise en oeuvre de cette procédure tout à fait inutile. On pourrait donc soupçonner que si les deux segments PQ et MN sont donnés, sans qu'on connaisse leurs respectives relations de mesure avec un segment (tel que $a$, dans l'exemple précédent) qui en est une mesure commune (au sens d'Euclide), alors les différentes implications qu'on a établies prennent un sens mathématique précis seulement lorsqu'on interprète la condition d'existence d'un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$, comme la possibilité de déterminer ce nombre par le bais d'une procédure telle que la précédente. Nos implications ne seraient alors que des formes masquées de la plus banale des tautologies : la procédure précédente s'arrête au bout d'un nombre fini $\nu + 1$ d'étapes, avec la détermination d'une égalité telle que (60) seulement si la procédure précédente s'arrête au bout d'un nombre fini $\nu+1$ d'étapes, avec la détermination d'une égalité telle que (60).

Cet argument me semble correct, sauf pour sa conclusion, car s'il est vrai, il me semble, que la seule manière mathématiquement acceptable d'interpréter la condition d'existence d'un nombre rationnel strictement positif $\frac{p}{q}$ tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$, lorsque les deux segments PQ et MN sont donnés sans qu'on connaisse leurs respectives relations de mesure avec un segment qui en est une mesure commune (au sens d'Euclide), est de penser cette condition comme la possibilité de déterminer ce nombre par le biais d'une procédure telle que la précédente, il est aussi vrai que la formulation de la seconde condition sous la forme d'une condition d'existence, telle que la première, permet de soumettre cette condition au contrôle d'une preuve par l'absurde visant à répondre à la question qui nous paraît à ce point cruciale : si deux segments quelconques sont donnés, est-il toujours le cas qu'un choix convenable de nombres $m_i$ $(i = 1, 2, ...)$ conduise à la détermination d'un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$ ? dit en d'autres termes, les segments respectent-ils tous la condition de la mesure commune ; sont-ils tous commensurables entre eux ?

C'est à cette question qu'il faut maintenaint répondre. On verra qu'il sera fort facile de parvenir à une réponse en pensant la condition de commensurabilité de deux segments quelconques PQ et MN en termes d'existence, et donc de possibilité de déterminer, d'une manière ou d'une autre, d'un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}\mathsf{PQ}$.

Si un segment MN est donné, il est certainement toujours possible de choisir un segment PQ, de sorte qu'il y ait un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$. Il suffit par exemple de prendre $\mathsf{PQ} = \mathsf{MN}$ pour avoir $\frac{p}{q} = 1$, ou, pour éviter cette banalité, de diviser MN en $h$ parties ($h$ étant un nombre naturel différent de 0) et de prendre PQ égal à la $h$-ième partie de MN pour avoir $\frac{p}{q} = h$. Ceci n'est pourtant pas ce qui nous intéresse. La question intéressante est ailleurs : à condition que PQ ait été fixé *a priori* (bien que de manière complètement arbitraire), est-on sûr que pour tout segment MN, il y ait un nombre rationnel positif $\frac{p}{q}$, tel que $\mathsf{MN} = \frac{p}{q}(\mathsf{PQ})$, et que la procédure précédente nous permette donc (à condition de bien choisir les nombres $m_1, m_2, ...$) de calculer ce nombre ? C'est bien à cette question qu'on n'a pas encore répondu, et c'est à celle-ci qu'il faut répondre maintenant.

Pour prouver qu'il n'en est pas ainsi, il suffit d'exhiber un couple de segments qui ne satisfont pas à la condition indiquée, ou, pour être plus précis, qui ne peuvent pas la satisfaire à cette condition. C'est exactement ce qu'on va faire ici, en adaptant un argument très ancien. Voici comment on peut procéder.

Figure p. 311

Le segment PQ étant donné, on commence par construire le carré dont PQ est le côté et, ceci fait, on tire une diagonale, disons PR, de ce carré qui le coupe en deux triangles égaux. Encore une fois, on suppose ici que nos connaissances en géométrie élémentaire nous permettent de procéder ainsi. On n'aura pourtant pas besoin de pousser plus loin la supposition, et de faire l'hypothèse qu'on dispose du théorème que tout le monde connaît sous le nom de « théorème de Pythagore », car dans le cas d'un triangle rectangle isocèle, comme celui qui résulte de la partition d'un carré par une de ses diagonales, ce théorème se lit sur la figure elle-même : il suffit de reconnaître que les deux triangles isocèles, dans lesquels une diagonale partage un carré, sont égaux entre eux. Si on examine la figure ci-dessous, on voit que le carré PSTR, construit sur la diagonale PR, est le double du carré PQRV, construit sur le segment donné PQ (et il est donc égal à la somme des deux carrés égaux construits respectivement sur les deux côtés du triangle rectangle PQR ). En indiquant par « $Q(x)$ » le carré construit sur un segment $x$, on aura alors

$$2Q(\mathsf{PQ}) = Q(\mathsf{PR}) \tag{66}$$

Note Historique 6.2. En dépit du nom habituel de ce théorème, la formulation classique du théorème de Pythagore se trouve dans le livre I des *Éléments* d'Euclide, où il constitue la proposition 47. Ce théorème fut pourtant connu bien avant Euclide ; apparemment, il l'était déjà à Babylone, sous le royaume de Hammourabi, et il est probable que Pythagore l'apprît pendant son voyage à Babylone, et l'emportât en Grèce, même s'il n'est pas sûr qu'il en donnât lui-même une démonstration. Dans le premier livre des *Éléments*, ce théorème occupe une place cruciale et on peut même dire que ce livre culmine avec ce théorème qui en est d'ailleurs l'avant-dernier.

Naturellement, Euclide ne se réclame ni des puissances, ni des racines carrées pour énoncer ce théorème. Comme on l'a déjà observé, pour Euclide deux segments ne peuvent pas être multipliés entre eux et cela n'a donc pas de sens de parler de puissance carrée d'un segment. Dans la version d'Euclide, le théorème de Pythagore nous dit tout simplement que le carré qu'on peut construire sur l'hypoténuse d'un triangle rectangle est égal à la somme des carrés qu'on peut construire sur les côtés de ce même triangle. Selon la conception d'Euclide cela ne signifie pas que l'aire du premier carré est égale à la somme des aires de ces derniers carrés. La notion d'aire d'un polygone est étrangère à la conception d'Euclide. Ce que nous dit le théorème, dans le contexte des *Éléments*, est plutôt que le rectangle construit sur l'hypoténuse d'un triangle carré peut être décomposé de telle manière qu'en composant différemment ses composants on obtient les deux carrés construits sur les côtés de ce triangle.

Ainsi conçu, ce théorème nous fournit une procédure standard pour additionner deux carrés : on forme, avec les côtés de ces carrés, un angle droit ; on ferme l'angle ainsi obtenu par un segment qui joint les extrémités libres de ses côtés en obtenant ainsi un triangle rectangle ; et on construit enfin un carré sur l'hypothénuse de ce triangle. Les carrés peuvent donc être additionnés, et comme tout polygone peut être décomposé et recomposé dans un carré, de là il suit que les polygones de toute sorte peuvent être additionnés entre eux ; ils se comportent donc comme des quantités, ils sont des quantités. Voici la raison qui fait du théorème de Pythagore le résultat culminant du premier livre des *Éléments*, dont le but final est justement de montrer que les segments, les angles et les polygones sont des quantités.

Depuis Euclide, on a trouvé d'innombrables preuves du théorème de Pythagore, dont plusieurs sont même plus simples que celle d'Euclide. En voici une qui ne tient au fond qu'à une figure.

## Figure p. 313

Le carré PQRS est construit sur l'hypoténuse QR du triangle rectangle OQR et il est égal à la différence entre le carré ABCD et les triangles PSD, PAQ, QBR et SRC. Mais ces triangles sont égaux entre eux et leur somme est égale à la somme des rectangles DMON et OQBR. Or, si on soustrait ces deux derniers rectangles au carré ABCD on obtient les deux carrés MAQO et NORC, dont la somme est donc égale au carré PQRS. Il suffit alors d'observer, pour conclure la preuve, que ces derniers carrés sont construits respectivement sur les côtés OR et OQ du triangle QBR.

**Lectures possibles** : J. Gray, *Ideas of Space. Euclidian, Non Euclidian and Relativistic*, Clarendon Press, Oxford, 2nd ed., 1989.

Imaginons maintenant qu'il y ait un nombre rationnel strictement positif $\frac{p}{q}$, tel que

$$\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$$

alors, on aura aussi

$$q(\mathsf{PR}) = p(\mathsf{PQ})$$

et donc, si $\mathsf{PW}$ est le segment qui résulte en additionnant le segment $\mathsf{PR}$ à lui-même $q$ fois, c'est-à-dire que $\mathsf{PW} = q\mathsf{PR}$, alors le carré $Q(\mathsf{PW})$ construit sur $\mathsf{PW}$ contient $p^2$ carrés de côté $\mathsf{PQ}$ et naturellement $q^2$ carrés de côté $\mathsf{PR}$. On en conclut donc que

$$\begin{aligned} Q(\mathsf{PW}) &= p^2 Q(\mathsf{PQ}) \\ Q(\mathsf{PW}) &= q^2 Q(\mathsf{PR}) \end{aligned}$$

et donc

$$p^2 Q(\mathsf{PQ}) = q^2 Q(\mathsf{PR})$$

ou bien

$$\frac{p^2}{q^2} Q(\mathsf{PQ}) = Q(\mathsf{PR})$$

En comparant cette égalité avec (66), on aura donc

$$\frac{p^2}{q^2} = 2 \tag{67}$$

S'il y a un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$, alors le nombre rationnel strictement positif $\frac{p^2}{q^2}$ est égal à 2. Il s'agit alors de comprendre si cela est possible, c'est-à-dire s'il est possible qu'un nombre rationnel strictement positif tel que $\frac{p^2}{q^2}$ soit égal à 2.

Pour cela, on observe d'abord que si $\frac{m}{n}$ est un nombre rationnel strictement positif, alors $m$ et $n$ sont deux nombres relatifs qu'on peut prendre, ou bien tous les deux négatifs, ou bien tous les deux strictement positifs. Comme les deux choix sont équivalents, supposons que $m$ et $n$ soient deux nombres naturels strictement positifs. Imaginons qu'autant $m$ que $n$ soient pairs. On aura alors quatre nombres naturels strictement positifs, $i$, $j$, $h$ et $k$, tels que

$$m = 2^i h \qquad \text{et} \qquad n = 2^j k$$

les nombres $h$ et $k$ étant tous les deux impairs. De là, il suit que

$$\frac{m}{n} = \frac{2^i h}{2^j k} = 2^{i-j} \frac{h}{k}$$

ou bien

$$\frac{m}{n} = \begin{cases} \frac{2^\mu h}{k} & \text{si } j < i \text{ et } i - j = \mu \\ \frac{h}{2^\mu k} & \text{si } i < j \text{ et } j - i = \mu \\ \frac{h}{k} & \text{si } i = j \end{cases} \tag{68}$$

($\mu$ étant, évidemment, un nombre naturel strictement positif). Cela nous fait comprendre que pour tout nombre rationnel positif $\frac{m}{n}$, il y a deux nombres naturels positifs, $m'$ et $n'$, tels que

$$\begin{cases} \frac{m}{n} = \frac{m'}{n'} \\ (m' \text{ est pair}) \Rightarrow (n' \text{ est impair}) \end{cases}$$

(c'est-à-dire que tout nombre rationnel positif $\frac{m}{n}$ est égal à un nombre rationnel positif $\frac{m'}{n'}$, tel que les nombres naturels $m'$ et $n'$ ne sont pas pairs à la fois). Poser $\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$ est donc équivalent à poser

$$\begin{cases} \mathsf{PR} = \frac{p'}{q'}(\mathsf{PQ}) \\ p', q' \in \{\mathbb{N} - 0\} \text{ et } [(p' \text{ est pair}) \Rightarrow (q' \text{ est impair})] \end{cases}$$

En répetant l'argument qui nous a conduit à (67), on en déduit que s'il y a un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$, alors :

$$\begin{cases} 2 = \frac{(p')^2}{(q')^2} \\ p', q' \in \{\mathbb{N} - 0\} \text{ et } [(p' \text{ est pair}) \Rightarrow (q' \text{ est impair})] \end{cases} \tag{69}$$

En effet : si $h$ est un nombre naturel (strictement positif) pair, alors il y aura un nombre naturel $k$, différent de zéro, tel que $h = 2k$, et donc $h^2 = 4k^2 = 2(k^2)$, c'est-à-dire que $h^2$ est aussi pair ; d'autre part, si $h$ est un nombre naturel (strictement positif) impair, alors il y a un nombre naturel $k$ différent de 0, tel que $h = 2k - 1$ et donc $h^2 = 4k^2 - 2k + 1 = 2(2k^2 - k) + 1$, c'est-à-dire que $h^2$ est aussi impair. Donc : si $h$ est pair, alors $h^2$ est aussi pair, et, de là, si $h^2$ n'est pas pair, c'est-à-dire qu'il est impair, alors $h$ n'est pas non plus pair, c'est-à-dire qu'il est impair ; en revanche, si $h$ est impair, alors $h^2$ est aussi impair, et, de là, si $h^2$ n'est pas impair, c'est-à-dire qu'il est pair, alors $h$ n'est pas non plus impair, c'est-à-dire qu'il est pair. Pour résumer : tout nombre naturel $h$ est pair si et seulement si $h^2$ est pair, et il est impair si et seulement si $h^2$ est impair.

Remarque 6.3. Quelqu'un pourrait penser que la condition $(m' \text{ est pair}) \Rightarrow (n' \text{ est impair})$ n'exprime qu'une partie du contenu de (68). Cette triple égalité nous dit que chaque nombre rationnel strictement positif $\frac{m}{n}$ est égal à un nombre rationnel strictement positif $\frac{m'}{n'}$, où $m'$ et $n'$ sont deux nombres naturels strictement positifs qui ne sont pas pairs à la fois. Et on pourrait penser que pour exprimer cette condition dans le langage logique de l'implication, il faudrait ajouter à la condition $(m' \text{ est pair}) \Rightarrow (n' \text{ est impair})$, l'autre condition $(n' \text{ est pair}) \Rightarrow (m' \text{ est impair})$. Il est pourtant clair que dire d'un nombre naturel strictement positif qu'il est impair équivalent, à dire qu'il n'est pas pair et dire qu'il est pair équivalent à dire qu'il n'est pas impair. Les deux implications précédentes sont donc équivalentes, en logique classique (car, en logique classique, l'implication $A \Rightarrow B$ est équivalente à l'implication $\neg B \Rightarrow \neg A$) et, bien que prises séparément, elles expriment toutes les deux la condition énoncée en d'autres termes par la (68) : comme les deux nombres $m'$ et $n'$ ne sont pas pairs à la fois, si l'un des deux est pair, alors l'autre est impair, c'est-à-dire qu'il n'est pas pair.

Dire qu'un certain énoncé qu'il est équivalent, dans une certaine logique, à un autre énoncé, signifie dire que le premier énoncé peut être déduit du deuxième, en conjonction avec les axiomes de la logique considérée, et que le deuxième peut être déduit du premier, toujours en conjonction avec les axiomes de la logique considérée.

Or, si pour passer de $A \Rightarrow B$ à $\neg B \Rightarrow \neg A$, il suffit d'observer que de $A \Rightarrow B$ et $\neg B$ il suit $\neg A$, pour passer de $\neg B \Rightarrow \neg A$ à $A \Rightarrow B$, il faut observer que, de la même manière, de $\neg B \Rightarrow \neg A$ et $\neg(\neg A)$ il suit $\neg(\neg B)$, et ajouter que $\neg(\neg A)$ et $\neg(\neg B)$ sont respectivement équivalents à $A$ et $B$. Pourtant, quel que soit $H$, pour déduire $H$ à partir de $\neg(\neg H)$, il faut présupposer le principe du tiers exclu, qui affirme que, quel que soit $H$, ou bien il est le cas que $H$ ou bien il est le cas que non $H$, en symboles : $H \vee \neg H$. En effet de $H \vee \neg H$ et $\neg(\neg H)$, il suit évidemment $H$. On sait pourtant qu'il est parfaitement possible de construire une logique cohérente dans laquelle le principe du tiers exclu ne vaut pas. Cette logique est dite généralement « intuitionniste » et s'oppose à la logique dite « classique », dans laquelle ce principe est parfaitement valable. En logique intuitionnisme $\neg(\neg H)$ n'est donc pas équivalent à $H$ et donc $\neg B \Rightarrow \neg A$ n'est pas équivalent à $A \Rightarrow B$, car de $\neg B \Rightarrow \neg A$ et des axiomes de la logique intuitionniste ne dérive pas $A \Rightarrow B$.

Si on regarde les choses de prés, on s'aperçoit pourtant assez aisément que cela n'affecte pas notre argument précédent, car pour s'assurer que l'implication ($m'$ est pair) $\Rightarrow$ ($n'$ est impair) exprime le contenu entier de (68), il suffit de s'assurer que de ($m'$ est pair) $\Rightarrow$ ($n'$ est impair) on puisse tirer ($n'$ est pair) $\Rightarrow$ ($m'$ est impair), ce qui, comme on vient de voir, est parfaitement possible autant en logique classique qu'en logique intuitionniste. Notre argument est donc valide autant dans une logique que dans l'autre.

NOTE HISTORIQUE 6.3. Bien que les idées fondatrices de la mouvance intuitionniste soient dues au mathématicien hollandais Luityen Egbertus Jan Brouwer (né à Overschie-Rotterdam en 1881 et mort à Blaricum, en Hollande, en 1966), la première formalisation de la logique intuitionniste est due à A. Heyting (Amsterdam, 9 mai 1898 – Lugano, 9 juillet 1980) et date de 1928.

La formalisation de Heyting dérive pourtant, dans un certain sens, d'une trahison des idées originelles de Brouwer, pour lequel les mathématiques n'étaient qu'une libre activité de l'esprit, construisant des objets nouveaux à l'aide d'une intuition primordiale et irréductible à toute sorte de logique. Fortement influencé par la philosophie de Kant, Brouwer ne distingua jamais son travail mathématique d'une réflexion sur la nature des mathématiques et sur les sources de légitimité de l'argumentation mathématique. Toujours soucieux d'éviter toute inférence non fondée sur une exhibition effective de l'objet mathématique, il n'hésita pas à déclarer comme dépourvus de fondements de nombreux résultats communément acceptés dans la communauté mathématique. Si ses conceptions, souvent polémiques, le conduisirent jusqu'à la construction d'une analyse mathématique par certains aspects assez différente de celle qui a aujourd'hui l'approbation de la plupart des mathématiciens, elles furent aussi à l'origine d'une réflexion sur la nature de la preuve mathématique et contribuèrent, à côté de conceptions de Hilbert (en réalité moins lointaines de celles de Brouwer qu'on le dit d'habitude), à la naissance de la théorie moderne de la démonstration.

**Lectures possibles** : A. Heyting, *Intuitionism. An Introdution*, North-Holland Pub. Comp., Amsterdam, New York, Oxford, 3rd ed., 1971 ; W. P. van Stigt, *Brouwer's Intuitionism*, North- Holland, Pub. Comp., Amsterdam, New York, Oxford, Tokyo, 1990 ; J. Largeault, *L'intuitionisme*, PUF, Paris, 1992.

Or, si $2 = \frac{(p')^2}{(q')^2}$, alors $(p')^2 = 2(q')^2$ et donc $(p')^2$ est pair de même que $p'$. De là il suit qu'il y a un nombre naturel $r$, différent de 0, tel que

$$p' = 2r$$

De (69), il suit alors que

$$\begin{cases} 2 = \frac{4r^2}{(q')^2} \\ q' \in \{\mathbb{N} - 0\} \text{ et } q' \text{ est impair} \end{cases}$$

Mais c'est clairement impossible, car si $2 = \frac{4r^2}{(q')^2}$ alors $(q')^2 = 2r^2$ et donc $(q')^2$ est pair et par conséquent $q'$ est pair aussi.

La position $\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$ qui a déclenché ce raisonnement est donc impossible, et de là, il suit qu'il ne peut pas y avoir un nombre rationnel strictement positif $\frac{p}{q}$, tel que $\mathsf{PR} = \frac{p}{q}(\mathsf{PQ})$. Les segments $\mathsf{PR}$ et $\mathsf{PQ}$ sont donc incommensurables : littéralement, ils n'ont pas de mesure commune.

Remarque 6.4. L'argument qu'on a employé pour parvenir à cette conclusion est mathématiquement primordial. Il emploie pourtant une technique très puissante qui n'a nullement été abandonnée par les mathématiciens modernes. Ces derniers l'ont plutôt généralisée et la qualifient aujourd'hui de technique du « contrôle de parité ». De plus, cet argument est une preuve par l'absurde. Généralement, on dit qu'une preuve par l'absurde suit le schéma suivant : on veut prouver $A$, on suppose non $A$ (c'est-à-dire : $\neg A$) et on montre que $\neg A \Rightarrow B$ et qu'il n'est certainement pas le cas que $B$. De là, il suit qu'il ne peut pas non plus être le cas que $\neg A$, et donc qu'il doit être le cas que $A$.

Ci-dessus on a parlé de logique intuitionniste. Il est clair que l'intérêt de cette logique ne dépend pas, tout simplement, de sa cohérence. Si une logique de la sorte a été formalisée, c'est qu'il y a des mathématiciens, dits justement « intuitionnistes », qui pensent que, quand on raisonne en mathématiques, c'est cette logique, plutôt que la logique classique, qu'il faut employer. Une manière habituelle pour soutenir ceci est d'observer que la logique classique est une logique du vrai et du faux, c'est-à-dire qu'elle formalise les propriétés de l'être vrai et de l'être faux. Le principe du tiers exclu est un exemple très clair de ceci : si on pense l'affirmation d'un énoncé $H$, ou, si on préfère, la supposition qu'il est le cas que $H$, comme la supposition de la vérité de $H$, alors il est fort naturel de penser que s'il n'est pas le cas que $H$, alors il doit être le cas que non $H$, c'est-à-dire que si $H$ n'est pas vrai, alors est vrai $\neg H$. C'est de là qui dérive justement le principe du tiers exclu : ou bien $H$, ou bien non $H$ (ou bien il est vrai $H$, ou bien il est vrai non $H$) ; en symboles, $H \vee \neg H$. Mais, un intuitionniste dirait, quand on fait des mathématiques il n'est pas question du vrai et du faux, mais du prouvé et du non prouvé, ou, si on préfère, du prouvable et du non prouvable, et la logique du prouvé et du non prouvé, ou du prouvable et du non prouvable, n'est pas la même que celle du vrai et du faux. Ainsi, si on pense l'affirmation d'un énoncé $H$, ou, si on préfère, la supposition qu'il soit le cas que $H$, comme la supposition que $H$ a été prouvé, ou qu'il est prouvable, rien ne nous autorise à conclure, du fait qu'il n'est pas le cas que $H$, qu'il est le cas que non $H$ : du fait qu'on n'a pas prouvé $H$, ou que $H$ n'est pas prouvable, il ne semble pas suivre qu'on a prouvé $\neg H$, ou que $\neg H$ soit prouvable. Le principe du tiers exclu ne règle donc pas les relations du prouvé et du non prouvé, ou du prouvable et du non prouvable, et il doit donc être rejeté lorsqu'il est question, comme dans les mathématiques, du prouvé et du non prouvé, ou du prouvable et du non prouvable, et non pas du vrai et du faux.

Évidemment ceux qui acceptent de travailler en mathématiques avec la logique classique n'affirment pas, contre les intuitionnistes, que le principe du tiers exclu règle les relations

du prouvé et du non prouvé, ou celles du prouvable et du non prouvable ; même si les choses semblent être assez différentes selon que l'on parle de prouvé et de non prouvé, ou du prouvable et du non prouvable, sur ce point, l'argument intuitionniste semble imparable. Ceux qui acceptent de travailler en mathématiques avec la logique classique soutiennent, tout simplement, qu'en mathématiques il est, comme ailleurs, surtout question du vrai et du faux. Le débat entre ces deux points de vue a occupé une très large partie des discussions sur les fondements des mathématiques au XX$^{\text{ème}}$ siècle, et il n'est pas question de le résumer ici ou de prendre un parti (bien que j'aie naturellement mes opinions sur la question, des opinions qui sont assez proches du point de vue intuitionniste).

Je me limiterai à observer qu'un intuitionniste ne peut pas accepter, sans condition, une preuve par l'absurde qui prenne la forme présentée ci-dessus, car un argument de la sorte semble être justement vicié par une confusion entre vérité et démontrabilité. En effet son schéma logique étant le suivant :

$$\dfrac{\dfrac{\neg A \Rightarrow B \qquad \neg B}{\neg(\neg A)}}{A} \tag{70}$$

cet argument se réclame du passage de $\neg(\neg A)$ à $A$, même si rien ne nous assure que si $\neg A$ ne peut pas être démontré, alors $A$ doit pouvoir l'être.

Il suffit pourtant de réfléchir un instant pour comprendre que la preuve précédente de l'incommensurabilité du côté et de la diagonale d'un carré ne suit le schéma (70) qu'à condition qu'on pose : $A =$ « il n'y a pas de nombres naturels $p$ et $q$, tels que $q(\mathsf{PR}) = p(\mathsf{PQ})$ » ; si on pose, en revanche, $A =$ « il y a deux nombres naturels $p$ et $q$, tels que $q(\mathsf{PR}) = p(\mathsf{PQ})$ », alors la structure logique de la preuve précédente sera :

$$\dfrac{A \Rightarrow B \qquad \neg B}{\neg A} \tag{71}$$

de sorte que cette preuve ne demandera aucunement de passer de $\neg(\neg A)$ à $A$, n'employant que le *modus tollens* (c'est-à-dire, justement, le principe qui permet de passer de $A \Rightarrow B$ et $\neg B$ à $\neg A$).

On aura donc deux sortes de preuves par l'absurde : une qui suit le schéma (70), et qu'aucun intituionniste ne pourra accepter sans conditions ; une autre qui suit le schèma (71), et qu'aucun intuitionniste ne pourra en revanche réfuser, car elle ne demande pas de recours au tiers exclu (qui, comme on l'a vu ci-dessus, est justement ce qui permet de passer de $\neg(\neg A)$ à $A$). Les preuves de cette deuxième sorte ne sont généralement pas contestées, ni par les intuitionnistes, ni par d'autres mathématiciens.

Il en résulte que l'incommennsurabilité du côté et de la diagonale d'un carré peut être démontrée par l'absurde de deux manières distinctes, dont une n'est pas admise par certains mathématiciens, qui n'ont pourtant pas de problèmes à admettre l'autre.

Qu'on observe d'ailleurs qu'une preuve (par l'absurde) qu'on peut interpréter comme un exemple du premier schéma ne peut pas toujours être aussi interprétée comme un exemple du deuxième. Pour ce faire, il faut que le théorème qu'on veut démontrer se laisse énoncer sous la forme de la négation d'un énoncé qui implique un autre énoncé dont la négation peut être prouvée. Et ceci n'est clairement pas toujours le cas. Ainsi il est possible de rencontrer des preuves par l'absurde qui, quelle que soit la manière selon laquelle on les interprète, ne sont pas valides en logique intuitionniste. C'est la raison essentielle de la large discussion

autour des preuves par l'absurde, qui a occupé et occupe les philosophes et les historiens des mathématiques.

On ne continuera pas ici avec ces subtilités logico-mathématiques (qui sont pourtant loin d'être anodines) et on s'alignera sur l'opinion générale qui interprète l'argument précédent comme une preuve parfaitement légitime. On observera simplement que si $q(\mathsf{PR}) = p(\mathsf{PQ})$, alors, comme on l'a vu, $\left(\frac{p}{q}\right)^2 = 2$ et donc $\frac{p}{q} = \sqrt{2}$, de sorte que ce qu'on a prouvé est au fond que $\sqrt{2}$ n'est pas un nombre rationnel.

NOTE HISTORIQUE 6.4. Dans le *Ménon*, Platon cherche à définir la vertu. Ceci est l'objet d'un dialogue entre Socrate et Ménon (un élève du sophiste Gorgias). Au cours de la discussion, Socrate est amené à exposer la théorie de la réminiscence et à fournir un exemple de maïeutique (l'art de réveiller la connaissance cachée dans l'âme, par le biais du questionnement). Cet exemple est constitué par un dialogue entre Socrate et un esclave de Ménon ; le questionnement de Socrate conduit l'esclave à se rendre compte (à se souvenir, dit Platon) du fait que le carré construit sur la diagonale d'un carré est le double de ce dernier carré. L'argument de Socrate est le même que celui qui nous a conduits à la (1.10).

L'argument qui suit cette égalité est repris pour l'essentiel de la preuve de la proposition 27 de l'appendice au livre $X$ des *Éléments*, dans l'édition classique de Heiberg (l'édition, datée de 1886, qui fournit le texte des *Éléments* qu'on considère aujourd'hui comme canonique). Dans d'autres éditions des *Éléments*, précédant celle de Heiberg, cette proposition, avec sa démonstration, compte comme la proposition 117 du livre $X$. Si Heiberg la rejette hors du corps des *Éléments*, c'est qu'il la considère comme un ajout de quelque copiste, emprunté à des textes précédent la rédaction, de la part d'Euclide, du livre $X$. La preuve qui y est exposée semble d'ailleurs avoir été conçue au sein de l'école pythagoricienne, où elle aurait eu des effets desctructeurs. En montrant que le côté et la diagonale d'un carré sont incommensurables, cette preuve aurait bloqué en effet tout espoir de parvenir à une explication du monde en termes de seuls nombres entiers (strictement positifs), ce qui semble par contre avoir été le programme de Pythagore, un programme qui l'aurait porté à la défense d'une sorte de mystique numérique, autour de laquelle les adeptes de Pythagore constituèrent une véritable secte. On raconte même que l'incommensurabilité de la diagonale et du côté d'un carré fut gardée longtemps comme un secret à l'intérieur de la secte des pythagoriciens, et que Hippase de Métapont, qui révéla le premier ce secret, fut chassé du groupe et mourut dans un naufrage provoqué par la colère de Jupiter.

Dans un de ses essais, *Le raisonnement par l'absurde*, Jean-Louis Gardies s'est réclamé de cette preuve pour illustrer, sur un exemple, une thèse de nature générale : toute preuve par l'absurde peut se convertir en une preuve « ostensive » ou directe. Si je le comprends bien, l'argument général avec lequel Gardies supporte cette thèse peut être formulé, en bref, de la manière suivante : toute implication telle que $A \Rightarrow B$ peut être convertie dans l'implication $\neg B \Rightarrow \neg A$ (on vient de voir que c'est ainsi autant en logique classique qu'en logique intuitionniste), donc les deux schémas

$$\begin{array}{ll} \neg A \Rightarrow B & A \Rightarrow B \\ \neg B & \neg B \\ \neg\neg A & \neg A \end{array}$$

parmi lesquels Gardies ne semble voir aucune différence essentielle, peuvent se convertir respectivement dans les deux schémas

$$\begin{array}{ll} \neg B & \neg B \\ \neg B \Rightarrow \neg\neg A & \neg B \Rightarrow \neg A \\ \neg\neg A & \neg A \end{array}$$

qui correspondent justement à deux preuves ostensives, logiquement équivalentes aux preuves par l'absurde dont ces preuves se présentent comme des conversions.

L'argument de Gardies est, naturellement, parfaitement correct, mais il ne me semble pas concerner la question de la validité d'une preuve par l'absurde. Autant une preuve par l'absurde qui suit le premier des quatre schémas précédents, qu'une preuve ostensive qui suit le troisième de ces schémas, demande en effet, pour qu'on puisse en tirer le théorème $A$, que le passage de $\neg\neg A$ à $A$ soit permis, et c'est bien ce passage, et non pas la nature apagogique d'une preuve par l'absurde de la première sorte, qui pose un problème concernant la validité d'une telle preuve. La question qui est concernée par la thèse de Gardies est plutôt celle de la nature analytique d'une preuve par l'absurde (cf. la note historique 3.1).

En se fondant sur cette thèse, Gardies soutient que, en dépit de sa forme logique typiquement analytique, la preuve par l'absurde est historiquement solidaire des démarches dans l'ensemble synthétiques. La question est plutôt complexe et je ne peux pas la discuter ici. Il me semble pourtant nécessaire d'observer que les formes ostensives qui dérivent par conversion des formes apagogiquées qu'on a distinguées ci-dessus demandent toutes les deux de partir d'une prémisse ($\neg B$) qui pourrait ne pas être suggérée d'emblée par l'énoncé de la proposition que l'on veut prouver. La rédaction d'une preuve ostensive qui suit l'une ou l'autre de ces formes demande donc un argument heuristique préalable (typiquement analytique) apte à déterminer son point de départ. Or, la preuve apagogique dont cette preuve ostensive se présente comme la conversion semble fournir justement cet argument, et elle le fait de manière à rendre logiquement inutile la rédaction de la preuve ostensive, car la suggestion de cette prémisse est déjà, *ipso facto*, dans ces cas, une preuve du même théorème que la preuve ostensive permet de prouver.

**Lectures possibles** : A. Szabó, *Les débuts des mathématiques grecques*, Vrin, Paris, 1977 ; J.-L. Gardies, *Le raisonnement par l'absurde*, P.U.F., Paris, 1991.

Si l'on revient maintennait à la preuve précédente, et si on l'analyse de près, on se rend aisément compte que cet argument ne prouve pas seulement que les segments PQ et PR sont incommensurables. Cet argument prouve aussi quelque chose de plus fort : on a montré que si un segment quelconque est donné, alors il est toujours possible de construire, à partir de ce segment, un autre segment qui est incommensurable avec le segment donné. On comprendra facilement que cela signifie que pour tout segment donné, on peut construire autant de segments que l'on veut qui soient incommensurables avec le segment donné. Donc, quel que soit le segment PQ que l'on ait choisi comme unité de mesure, la classe des segments qu'on peut considérer et qui ne peuvent pas être mesurés, relativement à ce segment, par un nombre rationnel est aussi grande que l'on veut. Pour tout segment PQ, on peut donc exhiber autant de segments que l'on veut qui ne sont pas avec PQ dans une relation de mesure déterminable par la procédure que l'on a exposée ci-dessus. Si on ne pouvait assigner une mesure à un segment que par l'entremise de cette procédure, alors il n'existerait pas, pour les segments, d'unité de mesure universelle possible.

Qu'on l'ait exprimé ou non de cette manière, ce qu'on vient d'exposer est un fait mathématique connu dès les temps de Pythagore (au V$^{e}$ siècle avant J. C.). Pourtant une solution vraiment satisfaisante de la difficulté qu'il manifeste n'a été trouvée que dans la seconde moitié du XIX$^{e}$ siècle (par des mathématiciens tels que Cantor, Dedekind ou Weierstrass). Ceci ne signifie évidemment pas qu'avant cette date les mathématiciens ne savaient pas traiter avec d'autres nombres que les rationnels, capables de fournir une mesure pour tout segment (quel que fût le segment choisi comme unité de mesure). Toujours est-il pourtant que la pratique mathématique portant sur ces nombres n'a fait l'objet d'une justification tenue pour satisfaisante qu'à la date tardive qu'on a indiquée. Pour pouvoir exposer les idées essentielles autour desquelles cette solution s'organise, il faut d'abord introduire une notion nouvelle qui joue dans cette solution un rôle essentiel, c'est la notion de convergence d'une suite. C'est le but du prochain paragraphe.

NOTE HISTORIQUE 6.5. Si on réfléchit sur la preuve qu'on vient de donner du fait que le côté d'un carré et la diagonale de ce carré sont incommensurables, on comprend que ce qu'on a au fond montré est que l'ensemble des nombres rationnels positifs n'est pas en bijection avec l'ensemble des segments : il y a plus de segments que de nombres rationnels positifs.

On reviendra plus loin sur cette conséquence de la preuve précédente, ici il suffira d'observer que la découverte de cette circonstance, qu'on formulait de manière plus ou moins précise, fut une autre des raisons qui conduisirent à une séparation, qui persista pendant de longs siècles, entre la théorie des grandeurs et la théorie des nombres (cf. les notes historiques 3.3 et 4.3). Pourtant, les mathématiciens comprirent, bien avant Descartes, que l'argument précédent pouvait être interprété, en même temps, comme une preuve de l'égalité $\mathsf{PQ} = r(\mathsf{PQ})$, où $r$ devait être tel que $r^2 = 2$, et comme une preuve du fait que le facteur $r$ entrant dans cette égalité n'est pas un nombre rationnel. Ils commencèrent ainsi, déjà pendant le Moyen âge arabe, et ensuite à la Renaissance, à parler d'une nouvelle sorte de nombres, non entiers et non réductibles à des rapports d'entiers, dont on savait pourtant que certaines de leurs puissances étaient des entiers. Si ce ne fut que très tardivement (et précisément avec Descartes) que le symbole « $\sqrt{2}$ », éventuellement accompagné d'un exposant, fut introduit pour désigner ces nombres, l'usage du terme « racine » pour les dénommer remonte à une période bien antérieure. Graduellement, on commença même à travailler avec ces nombres et à les associer à des algorithmes qui définissaient des opérations les concernant.

Ces nombres continuèrent pourtant, même après Descartes, à être conçus plus comme des résultats inconnus de certaines opérations que comme des nombres parfaitement déterminés. Le symbole « $\sqrt{2}$ » utilisé pour noter un de ces nombres, est, à lui seul, une preuve de ceci : ce symbole indique en fait plus une opération appliquée à un nombre connu et bien déterminé (la racine carrée de 2), que le résultat de cette opération. On pouvait certes parvenir à des approximations de ce résultat au moyen des nombres fractionnaires (qu'on savait évidemment bien écrire en forme décimale), mais on ne pouvait pas l'indiquer exactement en termes de nombres entiers, autrement qu'en indiquant l'opération qui aurait dû conduire jusqu'à lui, à partir du nombre 2. Des approximations de cette sorte permettaient pourtant de donner à ces nombres une place, plus au moins précise, dans l'ordre des rationnels, et la possibilité d'employer ces nombres pour indiquer le rapport non rationnel entre deux segments incommensurables poussa les mathématiciens, même avant Descartes (le cas de Bombelli est par exemple fort instructif), à leur assigner une place sur une droite, dans laquelle on avait fixé un point, valant comme origine (étant associé au nombre zéro).

Lentement, on commençait à comprendre que d'autres nombres, comme les nombres indiqués aujourd'hui par les symboles « $\pi$ » et « $e$ », correspondant respectivement au rapport fixe entre le diamètre et la circonférence d'un cercle et à la base d'un logarithme naturel, se comportaient plus ou moins de la même manière. Après maints efforts pour exprimer ces nombres, d'abord comme des rapports de nombres entiers, et ensuite comme des racines, on parvint à se convaincre que ces nombres n'étaient pas rationnels et qu'ils ne pouvaient pas non plus être identifiés avec des radicaux (des preuves définitives de ces dernières impossibilités furent données très tard, respectivement en 1882 par Lindemann, pour le nombre $\pi$, et en 1873 par Hermite, pour le nombre $e$, mais les mathématiciens majeurs commençaient à en être convaincus à partir de la deuxième moitié du XVII$^{\text{ème}}$ siècle, et en particulier après l'*Arithmetica infinitorum*, de J. Wallis, publiée à Oxford en 1656). On pouvait pourtant, comme pour les radicaux, en donner des approximations par le biais de nombres fractionnaires et les positionner ainsi, avec une précision suffisante, sur une droite. C'est bien de cette manière, comme des valeurs correspondant à des points sur une droite, que les mathématiciens, après Descartes et Newton, commencèrent à concevoir ces nombres et à traiter avec eux.

Cette pratique était largement satisfaisante à plusieurs égards, et fut maintenue pendant plus de deux siècles. Pourtant, elle ne répondait pas à une question fondamentale : comment pouvait-on définir précisément ces nombres (plus tard on dira le domaine ou l'ensemble de ces nombres) sans faire intervenir aucun outil externe à l'arithmétique ? C'est exactement à cette question que les mathématiciens ne trouvèrent de réponse satisfaisante qu'à la fin du XIX$^{\text{ème}}$ siècle. La suite du présent chapitre servira justement à présenter et à justifier cette réponse.

**Lectures possibles** : O. Perron, *Irrationalzahlen*, Walter de Gruyter & Co., Berlin, 1939 ; J. Klein, *Greek Mathematical Thought and the Origin of Algebra*, MIT Press, Cambridge (Mass.), 1968.

## 2. Suites, séries et convergence vers une (certaine) limite dans un (certain) ensemble

Dans les deux premiers paragraphes du chapitre 4, on a parlé assez informellement de séries. Bien que cela n'ait pas fait l'objet d'une définition précise, le lecteur aura compris qu'en général une série est une addition réitérée à l'infini. Normalement, les mathématiciens ne s'occupent que des séries dont les termes successifs répondent à une loi de formation connue (ou si cette loi est inconnue, le but de la recherche est souvent de déterminer cette loi). Si $\mathfrak{T}$ est l'ensemble des termes d'une série, il faut naturellement que tous les éléments de $\mathfrak{T}$ soient aussi des éléments d'un autre ensemble, disons $E$, dont $\mathfrak{T}$ est donc un sous-ensemble, sur lequel on a défini une addition associative. Bien qu'une série soit une addition avec une infinité de termes, il n'est pas nécessaire que $\mathfrak{T}$ soit un ensemble infini, car il est possible qu'un même élément de $\mathfrak{T}$ entre dans la série plusieurs fois, et même une infinité de fois. Ceci est par exemple le cas de la série

$$\sum_{i=0}^{\infty}(-1)^i = 1 - 1 + 1 - 1 + 1 - ...$$

que les mathématiciens appellent « série de Grandi », se référant aux mathématicien italien Guido Grandi qui, au tout début du XVII$^{\text{ème}}$ siècle, avança (avec l'accord de Leibniz) des idées qu'aujourd'hui on considère assez bizarres à propos de cette série. L'ensemble $\mathfrak{T}$ des termes de cette série n'est constitué que par deux éléments, 1 et $-1$, qui sont, les deux, des nombres relatifs, de sorte que dans ce cas : $\mathfrak{T} \subset \mathbb{Z}$.

Note Historique 6.6. Supposons que $a$, $x$ et $z$ soient trois éléments d'un ensemble $E$, sur lequel on a défini une addition, une multiplication et les opérations inverses respectives. Pour rendre les choses plus simples, imaginons que le triplet $< E, +, \cdot >$ soit un corps totalement ordonné relativement à la relation $\leqslant$ et que $a$, $x$ et $z$ appartiennent à $E$, qu'on pourra, par exemple, identifier avec $\mathbb{Q}$. Proposons-nous, alors, de calculer le résultat de la division $a : (x - z)$. Pour ce faire, on peut procéder ainsi : on divise d'abord $a$ par $x$, on considère le quotient de cette division comme une valeur approchée du quotient de la division proposée et on calcule le reste $r_1$ relatif à cette approximation ; on divise ensuite $r_1$ par $x$, on considère le quotient de cette division comme une valeur approchée du quotient de la division $r_1 : (x - z)$ et on calcule le reste $r_2$ relatif à cette approximation ; on continue en divisant $r_2$ par $x$, en considérant le quotient de cette division comme une valeur approchée du quotient de la division $r_2 : (x - z)$ et en calculant le reste $r_3$ relatif à cette approximation ; on procède indéfiniment de cette manière, en identifiant la somme des valeurs approchées des quotients des divisions $(a : x)$, $(r_1 : x)$, $(r_2 : x)$, ... avec le quotient de la division proposée. En appliquant ce procédé et en indiquant, pour plus de commodité, les quotients par des fractions, on aura alors l'égalité infinitaire suivante :

$$\frac{a}{x-z} = \frac{a}{x} + \frac{az}{x^2} + \frac{az^2}{x^3} + \frac{az^3}{x^4} + \ldots = \sum_{i=0}^{\infty} \frac{az^i}{x^{i+1}} \tag{72}$$

ou bien, en divisant par $a$,

$$\frac{1}{x-z} = \frac{1}{x} + \frac{z}{x^2} + \frac{z^2}{x^3} + \frac{z^3}{x^4} + \ldots = \sum_{i=0}^{\infty} \frac{z^i}{x^{i+1}} \tag{73}$$

qui, lues en sens inverse, donnent la somme d'une série.

La méthode avec laquelle on a obtenu ce résultat est historiquement connue comme « méthode de division de Mercator », car elle fut publiquement proposée, pour la première fois, par Nicholas Mercator, dans sa *Logarithmo-technia*, en 1668, bien que Newton l'eût indépendamment employée dans plusieurs manuscrits, quelques années auparavant. Elle constitue une des premières techniques que les mathématiciens aient mises au point pour travailler avec des séries. Comme il est facile de remarquer, cette technique ne consiste que dans une extension infinitaire d'un simple algorithme algébrique. Si, au lieu de procéder indéfiniment (ou jusqu'à l'infini), on arrête en fait la procédure après $n + 1$ étapes, et qu'on évalue le reste correspondant, on a l'égalité algébrique suivante :

$$\begin{aligned} \frac{a}{x-z} &= \frac{a}{x} + \frac{az}{x^2} + \frac{az^2}{x^3} + \ldots + \frac{az^n}{x^{n+1}} + \frac{az^{n+1}}{x^{n+1}(x-z)} \\ &= \left( \sum_{i=0}^{n} \frac{az^i}{x^{i+1}} \right) + \left( \frac{z}{x} \right)^{n+1} \frac{a}{x-z} \end{aligned}$$

ou bien, en divisant encore par $a$,

$$\frac{1}{x-z} = \left( \sum_{i=0}^{n} \frac{z^i}{x^{i+1}} \right) + \left( \frac{z}{x} \right)^{n+1} \frac{1}{x-z} \tag{74}$$

qui ne concernent qu'une somme parfaitement finie.

La question qui se pose, face à la méthode de Mercator, est donc la suivante : cette extension infinitaire d'un algorithme algébrique est-elle légitime ? Pour donner à cette

question une réponse précise et la justifier d'une manière qu'on considère aujourd'hui comme irréprochable, il faut disposer de notions et techniques mathématiques qui n'étaient certes pas à la disposition ni de Newton, ni de Mercator, et qu'on présentera pour l'essentiel dans le présent paragraphe.

Pourtant Newton et Mercator, ainsi que tous les mathématiciens de leur époque, étaient certes en mesure d'observer que, si $\frac{z}{x}$ est plus petit que $-1$ ou plus grand que 1, c'est-à-dire que $z < -x$ ou $z > x$, alors autant le reste $\left(\frac{z}{x}\right)^{n+1} \frac{1}{x-z}$ qui intervient en (74) que le $(n+1)$-ième terme $\frac{z^n}{x^{n+1}} = \frac{1}{x}\left(\frac{z}{x}\right)^n$ de la série qui intervient en (73) augmentent en valeur absolue lorsque $n$ grandit, c'est-à-dire que leur valeur, qu'elle soit positive ou négative, s'éloigne de plus en plus de zéro à mesure que $n$ grandit. Comme la valeur de la fraction $\frac{1}{x-z}$ reste, quelles que soient les valeurs de $x$ et de $z$, parfaitement finie et déterminée, de cette simple observation, il suit que si $z < -x$ ou $z > x$, alors les égalités (72) et (73) ne peuvent pas être correctes, c'est-à-dire qu'en prenant de plus en plus de termes dans les séries qui entrent dans ces égalités, et en calculant leurs sommes respectives, on ne peut que s'éloigner de plus en plus de la valeur du quotient cherché. Au contraire, si $-x < z < x$, alors les valeurs du reste $\left(\frac{z}{x}\right)^{n+1} \frac{1}{x-z}$ et du terme $\frac{z^n}{x^{n+1}} = \frac{1}{x}\left(\frac{z}{x}\right)^n$ s'approchent de plus en plus de zéro, à mesure que $n$ grandit. Si on considère un $n$ très grand, le reste $\left(\frac{z}{x}\right)^{n+1} \frac{1}{x-z}$ ne modifie donc que de très peu la valeur de la somme de l'addition $\sum_{i=0}^{n} \frac{z^i}{x^{i+1}}$, dont les termes ont d'ailleurs une valeur de plus en plus proche de zéro à mesure que $i$ s'approche de $n$. Cela nous autorise à penser que dans ce cas, les égalités (72) et (73) sont correctes, c'est-à-dire qu'en prenant de plus en plus de termes dans les séries qui entrent dans ces égalités, et en calculant les sommes respectives, on s'approche de plus en plus de la valeur du quotient cherché. Ceci pourrait d'ailleurs faire l'objet d'une démonstration qu'on ne pourra pourtant pas conduire avec les seuls outils qu'on a introduit jusqu'ici. Ce raisonnement nous permet de supposer que l'extension infinitaire dont relève la méthode de Mercator est légitime si $-x < z < x$ et ne l'est pas si $z < -x$ ou $z > x$. Ceci était d'ailleurs aussi l'opinion de Newton et Mercator, ainsi que celle de tous les autres mathématiciens de l'époque, même si ces mathématiciens pensaient, à la différence de nous, que les écritures (72) et (73) pouvaient être conçues comme des écritures correctes, même dans les cas que $z < -x$ ou $z > x$, à condition de ne pas les penser, dans ces cas, comme des égalités numériques, mais seulement comme des associations formelles (pour expliquer exactement ce que cela signifie, il faudrait entrer dans un grand nombre de détails historiques et mathématiques ; le lecteur qui ne connait pas ces détails devra donc se contenter, pour le moment, d'une compréhension assez vague de cette dernière remarque, qui n'a d'ailleurs pas une importance majeure pour la suite de l'argument que j'expose ici).

Il reste à comprendre ce qui se passe si $z = -x$ ou $z = x$. Dans le deuxième cas, le dénominateur $x - z$ des fractions $\frac{a}{x-z}$ et $\frac{1}{x-z}$ s'annule et ces fractions indiquent ainsi une division impossible. Le problème ne se pose donc pas, dans ce cas. En revanche, si on opère la substitution $z = -x$ dans la (73), on obtient :

$$\frac{1}{2x} = \frac{1}{x} - \frac{1}{x} + \frac{1}{x} - \frac{1}{x} + \ldots = \frac{1}{x}\sum_{i=0}^{\infty}(-1)^i \tag{75}$$

ou bien, en multipliant par $x$,

$$1 - 1 + 1 - 1 + \ldots = \sum_{i=0}^{\infty} (-1)^i = \frac{1}{2} \tag{76}$$

qui est justement le résultat que le Père Guido Grandi (né à Cremona, le 1er octobre 1671, et mort à Pise, le 4 juillet 1742), professeur de mathématiques à l'université de Pise, énonça en 1703, dans le traité *Quadratura circuli et Hyperbole*, et confirma en 1710, dans la deuxième édition du même traité.

Or, si on groupe les termes de la série qui intervient dans la (76) deux à deux, en commençant par le premier, la (76) se transforme en l'égalité

$$(1 - 1) + (1 - 1) + \ldots = 0 + 0 + \ldots = \frac{1}{2} \tag{77}$$

tandis que, si on commence le regroupement par le deuxième terme, on a l'égalité

$$1 - (1 + 1) - (1 + 1) \ldots = 1 - 0 - 0 - \ldots = \frac{1}{2} \tag{78}$$

Le caractère paradoxal de ces égalités (qui sont d'ailleurs cohérentes entre elles) ne découragea pas le père Grandi. En vérité, Grandi ne tira pas son résultat, comme on vient de le faire, de la simple substitution $z = -x$ dans un développement obtenu par la méthode de Mercator. D'abord, il obtint ce développement d'une autre façon, en supposant explicitement que $-x < z < x$, et en suivant un argument géométrique déjà connu par Torricelli. Ensuite, en appliquant ce résultat à une certaine situation géométrique, il en tira, pour des raisons de continuité, l'égalité

$$a - a + a - a + \ldots = b \tag{79}$$

où $a$ et $b$ sont des segments déterminés tels que $b$ est par construction égal à la moitié de $a$, à partir de laquelle (76) suit comme un corollaire immédiat. En affirmant (76), Grandi ne faisait donc que faire confiance à un argument géométrique par continuité, en affirmant que cet argument l'emportait sur l'autre qui affirmait que cette égalité était arithmétiquement paradoxale. L'arithmétique ne nous dit pas, semble argumenter Grandi, ce qui se passe si on somme entre eux une infinité de zéros, dérivés du fait d'ajouter et d'enlever indéfiniment la même quantité ; un argument géométrique nous montre en revanche à quoi on devrait s'attendre si on pouvait opérer ainsi : on obtiendrait la moitié de la quantité qu'on avait ajoutée et enlevée indéfiniment.

Dans la deuxième édition de son traité, après avoir obtenu son résultat, Grandi cherche à le justifier *a posteriori* par deux arguments extra-mathématiques, qu'il me semble sympathique de résumer. Le premier argument fait intervenir en même temps la « force de l'infini » et la puissance créatrice de Dieu : si on accepte que Dieu, par sa puissance, ait pu créer toutes les choses, à partir de rien, pourquoi ne devrait-on pas accepter que la force de l'infini produise une quantité finie en additionnant entre eux des zéros à l'infini ? Le deuxième argument est encore plus surprenant : imaginons un père de famille qui, en mourant, laisse en héritage à ses deux fils un bijou fort précieux, en empêchant, par clause testamentaire, autant sa vente, que sa cession ; les fils décident alors de garder le bijou à jours alternés ; si on imagine que ces fils vivent à l'infini, ne devrait-on pas en tirer que, de cette manière, en se donnant et se soustrayant alternativement le bijou, ils finissent par le posséder chacun à moitié ?

La deuxième édition du traité de Grandi poussa Alessandro Marchetti à publier un pamphlet, où il taxa Grandi de charlatan. Grandi répondit à Marchetti et il en

naquit une vive polémique, dans laquelle, en 1713, quelques mois avant de mourir, interviendra Leibniz lui-même. Tout en rejetant les justifications *a posteriori* de Grandi, Leibniz affirme que la preuve géométrique de ce dernier est irréfutable et son résultat doit donc être considéré comme correct. Leibniz n'était certes pas un naïf, tel que Grandi. On ne peut donc que mettre sa prise de position sur le dos de sa sénilité. Ce que ni Grandi, ni Leibniz semblent en fait avoir vu est que dans cette discussion l'enjeu n'était pas la validité ou la non validité d'un argument géométrique, quel que soit cet argument, mais la possibilité même d'une extension infinitaire des règles algébriques. En effet, si on acceptait le résultat de Grandi, on devrait en tirer que le zéro cesse d'être l'élément neutre de l'addition, lorsque l'addition est réitérée à l'infini. L'algèbre de l'infini serait alors tout à fait distincte de celle du fini, et elle ne serait pas d'ailleurs univoque. Du rejet du résultat de Grandi dépend donc la possibilité d'une mathématique de l'infini, une mathématique que Leibniz avait lui-même largement promue.

La tâche de remettre les pendules à l'heure fut assumée enfin par Varignon, un exposant de premier niveau de l'Académie des Sciences. Dans un mémoire de 1715, il démontra à nouveau le résultat de Mercator, en déclarant de manière explicite que sa validité, en tant qu'égalité numérique, est limitée au cas où $-x < z < x$. Depuis 1715, les pendules de l'histoire des mathématiques n'ont plus cessé de sonner à l'heure de Varignon.

**Lectures possibles** : M. Panza, *La forma della quantità. Analisi algebrica et analisi superiore : il problema dell'unità della matematica nel secolo dell'illuminismo*, vol. 38 et 39 (1992) des *Cahiers d'histoire et de philosophie des sciences.*

Rien n'empêche pourtant de considérer les termes d'une série sous un autre point de vue, c'est-à-dire de les considérer comme tous distincts les uns des autres, indépendamment du fait que, sur l'ensemble $E$ auquel ils appartiennent, ils soient identiques, ou que sur cet ensemble soit définie une relation d'égalité qui rend certains de ces termes égaux entre eux. L'ensemble de ces termes ainsi considérés, disons $\mathfrak{U}$, sera alors nécessairement infini, et tous ses éléments seront encore, à leur tour, des éléments d'un ensemble $E$ (dont $\mathfrak{U}$ ne sera pourtant pas, nécessairement, un sous-ensemble) sur lequel une addition est définie. Il est facile de voir que $\mathfrak{U}$ sera alors un ensemble dénombrable, c'est-à-dire qu'on pourra le mettre en bijection avec l'ensemble $\mathbb{N}$ des nombres naturels (ce qui, comme on l'a déjà avancé, et comme on le confirmera plus tard par un exemple, n'est pas le cas de tous les ensembles infinis). Cette bijection pourra être employée pour définir un ordre total sur $\mathfrak{U}$, en caractérisant respectivement les éléments de cet ensemble comme le premier, le deuxième, le troisième, etc. terme de la série considérée.

Ces considérations nous permettent de fournir une définition plus précise, que celle avancée dans le chapitre 4, de l'objet mathématique qu'on appelle « série ». Avant d'énoncer cette définition, il convient pourtant de suivre pas à pas, le processus par lequel on peut parvenir à construire une série.

On pourrait partir d'un ensemble $E$. Pour commencer, il ne sera pas nécessaire de supposer que sur cet ensemble soit définie une addition, ou n'importe quelle autre opération, relation ou fonction ; on verra par la suite de quelle sorte de structure cet ensemble devra participer, selon les exigences des différentes étapes de notre construction. En partant de cet ensemble on construira en premier lieu un nouvel ensemble infini et dénombrable $\mathfrak{U}$, en assignant successivement à ce dernier ensemble des éléments de $E$, non nécessairement distincts entre eux : d'abord on choisira un élément de $E$ et on l'assignera à $\mathfrak{U}$, ensuite on choisira encore un élément de $E$ (non nécessairement distinct ou différent du premier) et on l'assignera aussi à $\mathfrak{U}$, et on continuera ainsi. Pour pouvoir procéder ainsi à l'infini, il faudra pourtant définir une loi de

détermination des éléments de $E$ qu'on assigne successivement à $\mathfrak{U}$, de sorte que ces éléments soient déterminés tous à la fois, en gardant une marque qui indique l'ordre dans lequel ils se positionnent dans $\mathfrak{U}$. Suivant la manière dont on veut définir cette loi, il faudra évidemment que sur $E$ soient définies des opérations, des relations ou des fonctions convenables. Quelle que soit la manière que l'on choisit, il est pourtant clair que cette loi devra prendre la forme d'une application, disons $u : \mathbb{N} \to E$, associant à chaque nombre naturel un et un seul élément de $E$ ; l'élément de $E$ qui sera associé par $u$ au nombre 0 sera ainsi le premier élément de $\mathfrak{U}$, celui qui sera associé par $u$ au nombre 1 sera le deuxième élément de $\mathfrak{U}$, et ainsi de suite. L'ensemble $\mathfrak{U}$ sera ainsi d'emblée non seulement dénombrable, mais aussi totalement ordonné. Si on indique, comme on l'a fait dans le chapitre 4, un nombre naturel quelconque et variable par la lettre « $i$ », on pourra alors indiquer l'ensemble $\mathfrak{U}$ ainsi construit par le symbole « $\{u_i\}_{i=0}^{\infty}$ », ce qui donne l'égalité notationnelle :

$$\mathfrak{U} = \{u_i\}_{i=0}^{\infty} = \{u_0, u_1, u_2, ..., u_{n-1}, u_n, u_{n+1}, ...\}$$

Un tel ensemble, indépendamment du fait que ses termes soient ou non, plus tard, additionnés entre eux, s'appelle « suite ». Il est facile de voir qu'une suite n'est donc rien d'autre qu'un ensemble totalement ordonnée, infini dénombrable, dont les éléments sont des éléments d'un certain ensemble préalable $E$, déterminés dans leur ordre par une loi de détermination les associant tous, l'un après l'autre, à un nombre naturel distinct. Une manière simple et compacte d'exprimer ceci est la suivante :

Définition 2.1. *On appelle « suite » l'ensemble totallement ordonné, noté « $\{u_i\}_{i=0}^{\infty}$ » des images d'une application $u$ de $\mathbb{N}$ vers un ensemble $E$ donné préalablement — dite « loi de formation des termes de la suite $\{u_i\}_{i=0}^{\infty}$ ». Si l'ensemble $E$ est fixé, on dira qu'une telle suite est une suite à termes dans $E$. Si $i$ est un nombre naturel quelconque, l'image, notée « $u_i$ », de $i$ selon $u$ sera dite « $(i+1)-$ième terme de la suite $\{u_i\}_{i=0}^{\infty}$ ».*

Pour ne prendre qu'un exemple, imaginons que $E$ soit l'ensemble $\mathbb{Q}$ des nombres rationnels. Il sera alors aisé de définir une application $u : \mathbb{N} \to \mathbb{Q}$, par exemple par le biais de l'égalité définitionnelle

$$u_i = \frac{1}{i+1}$$

$i$ étant un nombre naturel quelconque. On aura ainsi la suite

$$\left\{\frac{1}{i+1}\right\}_{i=0}^{\infty} = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...\right\}$$

que les mathématiciens appellent « suite harmonique ».

Remarque 6.5. Comme cet exemple le montre, quelle que soit la loi de formation des termes d'une suite, il est toujours possible de penser cette loi de formation comme une application de $\mathbb{N}$ vers $E$, en respectant ainsi la définition 2.1. Pour des raisons de commodité, on préfère pourtant, en quelques occasions, définir une telle loi comme une fonction de $\mathbb{N}$ vers $E$ (pour la différence entre une application et une fonction cf. ci-dessus, pp. 46-47) dont le domaine est donné par un sous-ensemble convenable de $\mathbb{N}$. Par exemple, la suite harmonique pourra être pensée comme l'ensemble $\{u_i\}_{i=1}^{\infty}$ des images de la fonction $u : \mathbb{N} \to \mathbb{Q}$, définie par l'égalité $u_i = \frac{1}{i}$ (dont le domaine de définition est l'ensemble $\mathbb{N} - \{0\}$). Il ne sera pas difficile de comprendre comment on pourra modifier la définition 2.1 si on veut tenir compte de cette possibilité.

Une fois qu'on a dit ce qu'est une suite, il sera facile de dire ce qu'est une série. Pour passer d'une série à une suite, il sera en fait suffisant de s'assurer que sur $E$ est définie une addition

associative et d'additionner les uns aux autres les termes de la suite donnée. On aura ainsi la toute simple définition suivante :

DÉFINITION 2.2. *On appelle « série » l'addition, notée « $\sum_{i=0}^{\infty} u_i$ », de tous les éléments (pris dans leur ordre) d'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$, $E$ étant un ensemble quelconque, sur lequel est définie une addition associative. La suite $\{u_i\}_{i=0}^{\infty}$ sera alors dite « suite associée à la série $\sum_{i=0}^{\infty} u_i$ » et la série $\sum_{i=0}^{\infty} u_i$ « série associée à la suite $\{u_i\}_{i=0}^{\infty}$ ». Considérée par rapport à cette série, la loi de formation des termes de la suite $\{u_i\}_{i=0}^{\infty}$ sera dite « loi de formation des termes de la série $\sum_{i=0}^{\infty} u_i$ ». Si l'ensemble $E$ est fixé, on dira qu'une telle série est une série à termes dans $E$. Considéré par rapport à cette série, le terme $u_i$ de la suite $\{u_i\}_{i=0}^{\infty}$ sera dit « $(i+1)$-ième terme de la série $\sum_{i=0}^{\infty} u_i$ ».*

Pour avoir un exemple de série, il suffira de construire la série associée à la suite harmonique, dite à son tour « série harmonique » :

$$\sum_{i=0}^{\infty} \frac{1}{i+1} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ...$$

ce qui sera évidemment une série à termes dans $\mathbb{Q}$.

REMARQUE 6.6. De même que la définition 2.1, la définition 2.2 aussi pourra être facilement adaptée si on veut définir la loi de formation des termes d'une susérie comme une fonction. Si cette possibilité est concédée, ce qui permet de travailler plus commodément avec certaines séries, la série harmonique pourra par exemple être pensée comme l'addition $\sum_{i=1}^{\infty} \frac{1}{i}$ de termes de la suite harmonique pensée à son tour comme l'ensemble $\left\{\frac{1}{i}\right\}_{i=1}^{\infty}$.

Ayant dit, avec une précision suffisante, ce que sont une suite et une série, on peut en venir à ce qu'il faut entendre par convergence d'une suite et d'une série.

Pour ce faire, commençons par considérer la suite harmonique. Il est facile de voir que lorsque la valeur de $i$ croît, la valeur de son image $\frac{1}{i+1}$ selon l'application $u$ décroît, en restant toujours un nombre rationnel strictement positif, s'approchant de plus en plus de 0, de sorte qu'en avançant dans la considération des termes de la suite harmonique, on trouvera des nombres rationnels strictement positifs de plus en plus petits, et toujours plus proches de 0. Cette constatation est possible grâce au fait que l'ensemble $\mathbb{Q}$, constituant l'ensemble d'arrivée de l'application $u : \mathbb{N} \to \mathbb{Q}$ qui définit la série harmonique, est ordonné, et en particulier totalement ordonné. La même propriété de la suite harmonique qu'on vient de remarquer peut pourtant être décrite d'une autre manière. On peut dire que la différence $\frac{1}{i+1} - 0$ entre le $(i+1)$-ième terme de cette suite et 0 s'approche de plus en plus de 0, à mesure que la valeur de $i$ croît. Cette description d'une si remarquable propriété de la suite harmonique suggère une formulation plus générale pour une propriété analogue, qu'on peut prédiquer d'une suite quelconque, à condition que l'ensemble $E$, auquel appartiennent ses termes, satisfasse à des conditions, qu'on va indiquer dans la suite.

Considérons une suite quelconque $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$, et imaginons qu'on ait défini une application $\Delta : E^2 \to D$, dite « distance », dont le domaine, est l'ensemble des couples d'éléments de $E$ et l'ensemble d'arrivée est un ensemble $D$ totalement ordonné relativement à une relation d'ordre $\preceq$, telle qu'il y ait dans $D$ un élément, disons $\alpha$, qui est le plus petit

des éléments de $D$ relativement à la relation d'ordre $\preceq$, c'est-à-dire que $\alpha$ est un élément de $D$ et pour tout $x \in D$, $\alpha \preceq x$. Si $y$ et $z$ sont deux éléments quelconques de $E$, l'image, notée « $\Delta(y,z)$ », du couple $< y,z >$ selon l'application $\Delta$ sera dite « distance entre $y$ et $z$ » (on note qu'on ne demande pas que le domaine de $\Delta$ soit l'ensemble des couples ordonnées d'éléments de $E$, mais simplement l'ensemble des couples des éléments de $E$, de sorte que dans cet ensemble on ne fera aucune différence entre $< y,z >$ et $< z,y >$, et donc, par définition, $\Delta(y,z) = \Delta(z,y)$). Si, comme dans le cas de la suite harmonique, l'ensemble $E$ coïncide avec l'ensemble $\mathbb{Q}$ des nombres rationnels, alors on pourra prendre pour la distance $\Delta$ l'application qui associe à chaque couple d'éléments $\mathfrak{p}$ et $\mathfrak{q}$ de $\mathbb{Q}$, la différence $\mathfrak{p} - \mathfrak{q}$, à condition que $\mathfrak{q} \leq \mathfrak{p}$, ou la différence $\mathfrak{q} - \mathfrak{p}$, si $\mathfrak{p} < \mathfrak{q}$, ce qu'on note généralement par le symbole « $|\ \mathfrak{p} - \mathfrak{q}|$ » et qu'on appelle « valeur absolue de la différence $\mathfrak{p} - \mathfrak{q}$ ». L'ensemble $D$ coïncidera alors avec l'ensemble $\mathbb{Q}^+$ des nombres rationnels positifs, et, si (comme il est naturel de le faire) on considère cet ensemble comme totalement ordonné par rapport à la relation d'ordre $\leq$, l'élément $\alpha$, qui est le plus petit des éléments de $D$, n'est autre que 0.

Imaginons maintenant qu'il y ait dans $E$ un élément $U$ tel que, si $i$ est un nombre naturel quelconque, éventuellement plus grand qu'un certain nombre naturel $m$, la distance entre $U$ et $u_i$ diminue de plus en plus (ou reste éventuellement égale à elle-même) à mesure que $i$ croît, c'est-à-dire que, quel que soit $i > m$, si $p$ est un nombre naturel quelconque, alors

$$\Delta(U, u_{i+p}) \preceq \Delta(U, u_i) \tag{80}$$

Si on prend pour la distance entre deux nombres rationnels la valeur absolue de leur différence, comme on l'a suggéré ci-dessus, ceci est bien le cas de la suite harmonique, pourvu qu'on pose $U = 0$, car, quel que soit le nombre naturel $i$, si $p$ est un nombre naturel quelconque, alors

$$\left|0 - \frac{1}{i+p+1}\right| = \frac{1}{i+p+1} \leq \left|0 - \frac{1}{i+1}\right| = \frac{1}{i+1}$$

Ceci n'est pas encore pourtant la propriété de la suite harmonique qu'on a observée ci-dessus. Une suite peut en effet satisfaire à la condition (80) relativement à un certain élément $U$ de $D$, sans pour autant être telle que ses éléments se comportent d'une manière qu'on serait disposé à décrire en disant qu'ils s'approchent de plus en plus de $U$, à mesure que $i$ croît, comme on l'a dit par contre de la suite harmonique pour la position $U = 0$. Il suffirait pour cela qu'il y ait dans $D$ un autre élément $\tilde{U}$, tel que la suite en question satisfasse aussi à la condition (80) relativement à $\tilde{U}$. Essayons alors, de comprendre, plus précisément, quelle est la propriété générale d'une suite, qu'on a assignée en termes informels à la suite harmonique, en disant que ses termes s'approchent de plus en plus de 0.

Pour donner une image, pour ainsi dire tangible, de cette propriété, imaginons que les termes d'une suite $\{u_i\}_{i=0}^{\infty}$ soient des points $\mathsf{B}_i$ pris sur une droite sur laquelle on a fixé un point $\mathsf{A}$ :

Figure p. 334

Il est alors possible que, au fur et à mesure que $i$ croît, les segments $\mathsf{AB}_i$, que nous pouvons prendre comme les distances entre le point $\mathsf{A}$ et les points $\mathsf{B}_i$ deviennent de plus en plus petites et toujours plus proches du segment nul comme c'est justement le cas dans, la figure précédente. Il est facile de voir ce que cela signifie : je fixe une distance $\mathsf{AC}$ quelconque non nulle (aussi petite que je veux), c'est-à-dire un segment quelconque non nul (aussi petit que je veux), pris sur la droite donnée, à partir de $\mathsf{A}$ ; et j'observe que je peux toujours prendre une valeur de $i$ assez grande pour que la distance $\mathsf{AB}_i$ soit plus petite que la distance $\mathsf{AC}$ et qu'elle reste toujours plus petite si je prends ensuite des valeurs encore plus grandes de $i$.

Il n'est pas difficile de voir que cette propriété de notre suite $\{u_i\}_{i=0}^{\infty}$ de points est justement la même qu'on a observée ci-dessus dans la suite harmonique. Et c'est exactement cette

propriété d'une suite qu'on appelle « convergence vers une (certaine) limite dans un (certain) ensemble » : la propriété qui fait que les termes de cette suite s'approchent de plus en plus (dans le sens qu'on vient de préciser) d'un certain élément de l'ensemble auquel ces termes appartiennent. En particulier notre suite $\{u_i\}_{i=0}^{\infty}$ de points converge vers le point A dans l'ensemble des points de la droite donnée. La suite harmonique converge en revanche vers 0 dans $\mathbb{Q}$. On comprendra alors que la convergence d'une suite ne dépend en rien de ce qui se passe pour des valeurs petites de $i$ ; l'important est ce qui se passe au-delà d'une certaine valeur (finie) de $i$, aussi grande que puisse être cette valeur. Ainsi une suite telle que $\left\{1, 19, 875, 24.321, ..., \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, ...\right\}$ converge vers 0 dans $\mathbb{Q}$, bien qu'elle semble commencer comme une suite divergente.

Les considérations précédentes nous suggèrent une définition apte à caractériser de manière précise cette propriété :

DÉFINITION 2.3. *On dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$ converge vers $U$ dans $E$, relativement à la distance $\Delta : E^2 \to D$, $D$ étant un ensemble totalement ordonné relativement à une relation d'ordre $\preceq$, possédant un élément minimale $\alpha$, si et seulement s'il y a un élément $U$ de $E$ tel que toutes les images $\Delta(U, u_h)$ des couples $< U, u_h >$ ($u_h$ étant un terme quelconque de la suite $\{u_i\}_{i=0}^{\infty}$) selon $\Delta$ appartiennent à $D$ et que, pour tout $\varepsilon$ appartenant à $D$, tel que $\alpha \prec \varepsilon$, il y a un nombre naturel $n$, tel que, si $i > n$, alors $\Delta(U, u_i) \prec \varepsilon$ ; en symboles :*

$$(\varepsilon \in D) \Rightarrow [\alpha \prec \varepsilon \Rightarrow (\exists n \in \mathbb{N} : \text{ tel que } : i > n \Rightarrow \Delta(U, u_i) \prec \varepsilon)]$$

*Si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$ converge vers $U$ dans $E$, alors on dit que $U$ est la limite de $\{u_i\}_{i=0}^{\infty}$ dans $E$. Si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$ est telle qu'il n'y a aucun élément $U$ de $E$ qui satisfait à la condition précédente par rapport à la distance $\Delta : E^2 \to D$, alors on dit que cette suite ne converge vers aucune limite dans $E$, relativement à cette distance, ou est divergente dans $E$, relativement à cette distance.*

Comme ci-dessous on traitera largement de suites à termes dans $\mathbb{Q}$ et qu'on supposera toujours que la distance entre deux éléments de $\mathbb{Q}$ est donnée par la valeur absolue de leur différence, il convient d'expliciter la forme qu'une telle définition prend lorsqu'elle s'applique à une suite à termes dans $\mathbb{Q}$, évaluée relativement à un distance ainsi définie :

DÉFINITION 2.4. *On dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ converge vers $U$ dans $\mathbb{Q}$, si et seulement s'il y a un élément $U$ de $\mathbb{Q}$, tel que, pour tout $\varepsilon$ appartenant à $\mathbb{Q}^+$, tel que $0 < \varepsilon$, il y a un nombre naturel $n$, tel que, si $i > n$, alors $|U - u_i| < \varepsilon$ ; en symboles :*

$$\left(\varepsilon \in \mathbb{Q}^+\right) \Rightarrow [0 < \varepsilon \Rightarrow (\exists n \in \mathbb{N} : \text{ tel que } : i > n \Rightarrow |U - u_i| < \varepsilon)]$$

*Si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ converge vers $U$ dans $\mathbb{Q}$, alors on dit que $U$ est la limite de $\{u_i\}_{i=0}^{\infty}$ dans $\mathbb{Q}$. Si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ est telle qu'il n'y a aucun élément $U$ de $\mathbb{Q}$ qui satisfait à la condition précédente, alors on dit que cette suite ne converge vers aucune limite dans $\mathbb{Q}$ ou est divergente dans $\mathbb{Q}$.*

Pour montrer le bien fondé de cette définition et éclairer comment elle fonctionne, démontrons que la suite harmonique converge vers 0 dans $\mathbb{Q}$ (ou, si on préfère, dans $\mathbb{Q}^+$) :

THÉORÈME 2.1. *La suite harmonique $\left\{\frac{1}{i+1}\right\}_{i=0}^{\infty}$ converge vers 0 dans $\mathbb{Q}$.*

**Preuve.** Il est clair d'abord que aussi bien 0 que toutes les valeurs de $\frac{1}{i+1}$ et de la distance $\left|0 - \frac{1}{i+1}\right|$ appartiennent à à $\mathbb{Q}$ (et même à $BbbQ^+$). Considérons un élément quelconque $\varepsilon$ de $\mathbb{Q}^+$ plus grand que zéro, c'est-à-dire un nombre rationnel strictement positifs $\frac{\nu}{\mu}$ (où $\nu$ et $\mu$ sont deux nombres naturels quelconques différents de 0). Il s'agit alors de démontrer qu'il y a un nombre naturel $n$ tel que $i > n \Rightarrow \left|0 - \frac{1}{i}\right| = \frac{1}{i} < \frac{\nu}{\mu}$. Il est clair que ce nombre est toujours

constructible par une simple opération algébrique. En fait, si $i$ est plus grand ou égal à $\mu$, par exemple s'il est égal à $\mu + p$ ($p$ étant un nombre naturel quelconque), alors $\frac{1}{i} < \frac{\nu}{\mu}$, car dans ce cas on aurait $\frac{1}{i} = \frac{1}{\mu+p}$ et $\frac{1}{\mu+p}$ est sans doute plus petit que $\frac{\nu}{\mu}$ (en fait $\frac{1}{\mu+p} < \frac{\nu}{\mu} \Leftrightarrow \mu < \nu\mu + \nu p$ et, $\nu$ et $\mu$ étant des nombres naturels différents de 0, $\mu$ est sans doute plus petit que $\nu\mu + \nu p$). □

REMARQUE 6.7. Par un raisonnement analogue, mais inversé, on pourrait aussi démontrer, par exemple, que la suite $\left\{i^2\right\}_{i=0}^{\infty}$ à termes dans $\mathbb{N}$ ne converge vers aucun nombre naturel, ou bien qu'elle est divergente dans $\mathbb{N}$, relativement à la distance $\Delta : \mathbb{N}^2 \to \mathbb{N}$, définie par l'égalité $\Delta(p, q) = |p - q|$, $p$ et $q$ étant deux nombres naturels quelconques et $|p - q|$ étant égale à $p - q$ si $q \leq p$ et à $q - p$ si $p < q$, comme on l'a dit ci-dessus pour des nombres rationnels. C'est d'ailleurs le cas de toutes les suites à termes dans $\mathbb{N}$, sauf si ces termes deviennent, au-delà d'une certaine valeur de $i$, tous égaux entre eux, car la distance $|p - q|$ ne peut être plus petite que 1 que si elle est égale à zéro, ce qui a lieu seulement si $p = q$. Donc toutes les suites à termes dans $\mathbb{N}$, à partir des quelles on peut construire les séries dont on a considéré les réduites partielles dans le chapitre 4, sont divergentes dans $\mathbb{N}$.

REMARQUE 6.8. La preuve du théorème 2.1 montre bien que le cœur des définitions 2.3 et 2.4 réside dans la dépendance qu'elles instaurent entre les valeurs de $\varepsilon$ et de $n$. Pour caractériser précisément la propriété d'une suite qu'on peut informellement indiquer en disant que ses termes se rapprochent de plus en plus d'une certaine limite, ces définitions établissent en fait que, quelle que soit la distance non nulle à laquelle on veut se positionner par rapport à cette limite, il y a toujours un terme de la suite qui se trouve à une distance de cette limite inférieure à celle-ci, tous les termes successifs de la suite se trouvant aussi à une distance de cette limite inférieure à celle-ci. Ainsi, le point est le suivant : une suite à termes dans $E$ converge vers une limite $U$ dans $E$, si et seulement si, quelque soit le $\varepsilon$ choisit, pourvu qu'il soit plus grand que la valeur minimale que peut prendre la distance considérée (généralement zéro), on peut lui associer (construire à partir du choix de ce $\varepsilon$) un nombre naturel $n$ qui satisfait à la condition demandée : $n$ dépend donc de $\varepsilon$, et toute preuve de la convergence d'une suite consiste à exhiber une manière de construir un $n$ convenable lorsque un $\varepsilon$ quelconque est donné.

Il est maintenant facile de voir comment on peut définir informellement une propriété, dont une série peut éventuellement jouir, qui apparaisse comme analogue à la convergence d'une suite vers une certaine limite dans un certain ensemble : on pourra dire en effet, tout simplement, qu'une série converge vers une certaine limite dans un certain ensemble lorsque les résultats des additions successives de ses termes s'approchent de plus en plus d'un certain élément de l'ensemble considéré. Une série convergente vers une certaine limite dans un certain ensemble sera alors telle qu'on pourra lui associer, de manière univoque, un certain élément de cet ensemble, justement la limite vers laquelle elle y converge, qu'on pourrait traiter comme le résultat de l'addition infinie qui la constitue. En d'autres termes, dire d'une série qu'elle converge vers une certaine limite dans un certain ensemble reviendra à dire que cette série possède une somme dans cet ensemble, et peut donc y être traitée, en ce qui concerne son aptitude à produire (et à exprimer) un résultat, comme une addition ordinaire. On comprendra alors l'importance que, dans la considération d'une suite, revêt l'évaluation de sa convergence.

Une fois qu'on a ainsi éclairci ce que signifie précisement pour une suite de converger vers une certaine limite dans un certain ensemble, il ne sera pas difficile de faire de même pour une série. Si une série quelconque $\sum_{i=0}^{\infty} u_i$ est en fait donnée, il est facile de comprendre comment il est

possible de construire, à partir de cette série, une suite dont la convergence éventuelle vers une certaine limite dans un certain ensemble nous assure que la série donnée converge, elle-aussi, vers la même limite dans le même ensemble. Il suffit pour cela de former la suite $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$ des sommes auxquelles on parvient en additionnant successivement les termes de la série donnée, dite « suite des réduites partielles de la série suite !des réduites partielles d'une série $\sum_{i=0}^{\infty} u_i$ » : si elle est convergente vers $U$ dans $E$, alors la série $\sum_{i=0}^{\infty} u_i$ est, elle aussi, convergente vers $U$ dans $E$. On aura alors la définition suivante :

DÉFINITION 2.5. *On dit qu'une série $\sum_{i=0}^{\infty} u_i$ à termes dans $E$ converge vers $U$ dans $E$, relativement à la distance $\Delta : E^2 \to D$, $E$ étant un ensemble sur lequel est définie une addition par rapport à laquelle cet ensemble est fermé, et $D$ un ensemble totalement ordonné relativement à une relation d'ordre $\preceq$, possédant un élément minimal $\alpha$, si et seulement si la suite $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$ de ses réduites partielles (qui sera alors une suite à termes dans $E$) converge vers $U$ dans $E$, relativement à la même distance $\Delta : E^2 \to D$, c'est-à-dire qu'il y a un élément $U$ de $E$ tel que toutes les images $\Delta\left(U, \sum_{i=0}^{h} u_i\right)$ des couples $< U, \sum_{i=0}^{h} u_i >$ ($\sum_{i=0}^{h} u_i$ étant un terme quelconque de la suite $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$) selon $\Delta$ appartiennent à $D$ et que, pour tout $\varepsilon$ appartenant à $D$, tel que $\alpha \prec \varepsilon$, il y a un nombre naturel $n$, tel que, si $j > n$, alors $\Delta\left(U, \sum_{i=0}^{j} u_i\right) \prec \varepsilon$ ; en symboles :*

$$(\varepsilon \in D) \Rightarrow \left[\alpha \prec \varepsilon \Rightarrow \left(\exists n \in \mathbb{N} \text{ tel que } j > n \Rightarrow \Delta\left(U, \sum_{i=0}^{j} u_i\right) \prec \varepsilon\right)\right]$$

*Si une série $\sum_{i=0}^{\infty} u_i$ à termes dans $E$ converge vers $U$ dans $E$, alors on dit que $U$ est la limite de $\sum_{i=0}^{\infty} u_i$ dans $E$. La relation qui s'instaure entre une série et sa limite est indiquée par le symbole d'égalité ; écrire l'égalité*

$$\sum_{i=0}^{\infty} u_i = U$$

*$U$ étant un élément de $E$, équivaut ainsi à affirmer que la série $\sum_{i=0}^{\infty} u_i$ converge vers $U$ dans $E$. Si une série $\sum_{i=0}^{\infty} u_i$ à termes dans $E$ est telle qu'il n'y a aucun élément $U$ de $E$ qui satisfait à la condition précédente par rapport à la distance $\Delta : E^2 \to D$, alors on dit que cette série ne converge vers aucune limite dans $E$, relativement à cette distance, ou est divergente dans $E$, relativement à cette distance.*

De même que pour les suites, on traitera largement ci-dessous de séries à termes dans $\mathbb{Q}$ et on supposera toujours que la distance entre deux éléments de $\mathbb{Q}$ est donnée par la valeur absolue de leur différence. Il convient donc d'expliciter, aussi dans ce cas, la forme qu'une telle définition prend lorsqu'elle s'applique à une suite à termes dans $\mathbb{Q}$, évaluée relativement à une distance définie ainsi :

DÉFINITION 2.6. *On dit qu'une série* $\sum_{i=0}^{\infty} u_i$ *à termes dans* $\mathbb{Q}$ *converge vers* $U$ *dans* $\mathbb{Q}$, *si et seulement si la suite* $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$ *de ses réduites partielles (qui sera alors une suite à termes dans* $\mathbb{Q}$*) converge vers* $U$ *dans* $\mathbb{Q}$, *c'est-à-dire qu'il y a un élément* $U$ *de* $\mathbb{Q}$, *tel que, pour tout* $\varepsilon$ *appartenant à* $\mathbb{Q}^+$, *tel que* $0 < \varepsilon$, *il y a un nombre naturel* $n$, *tel que, si* $j > n$, *alors* $\left|U - \sum_{i=0}^{j} u_i\right| < \varepsilon$ *; en symboles :*

$$\left(\varepsilon \in \mathbb{Q}^+\right) \Rightarrow \left[0 < \varepsilon \Rightarrow \left(\exists n \in \mathbb{N} \text{ tel que } i > n \Rightarrow \left|U - \sum_{i=0}^{j} u_i\right| < \varepsilon\right)\right]$$

*Si une série* $\sum_{i=0}^{\infty} u_i$ *à termes dans* $\mathbb{Q}$ *converge vers* $U$ *dans* $\mathbb{Q}$, *alors on dit que* $U$ *est la limite de* $\sum_{i=0}^{\infty} u_i$ *dans* $\mathbb{Q}$. *Si une série* $\sum_{i=0}^{\infty} u_i$ *à termes dans* $\mathbb{Q}$ *est telle qu'il n'y a aucun élément* $U$ *de* $\mathbb{Q}$ *qui satisfait à la condition précédente, alors on dit que cette série ne converge vers aucune limite dans* $\mathbb{Q}$ *ou est divergente dans* $\mathbb{Q}$.

NOTE HISTORIQUE 6.7. La construction de l'ensemble *BbbR* des nombres réels, que je vais présenter dans la suite du présent chapitre, se réclame, comme il est désormais facile d'imaginer, de la notion de convergence d'une suite à termes dans $\mathbb{Q}$ vers une certaine limite dans $\mathbb{Q}$. Pour des raisons évidentes d'ordre logique, je dois donc présenter la notion de convergence d'une suite à termes dans $\mathbb{Q}$ vers une certaine limite dans $\mathbb{Q}$, avant de définir l'ensemble *BbbR*. Comme j'ai essayé de le montrer, la définition (2.4) qui accomplit cette tache n'est pourtant qu'un cas particulier d'une définition plus générale qui, comme on le verra dans la suite, pourrait très bien se référer à l'ensemble des nombres réels.

Historiquement, la clarification de la notion de convergence d'une suite, et celle de la notion de limite d'une fonction, strictement connectée à celle-ci, a en revanche concerné d'abord des suites à termes dans *BbbR*. Ce fut seulement lorsqu'ils disposaient déjà d'une définition suffisamment précise pour la limite d'une fonction de *BbbR* sur *BbbR*, et qu'ils avaient pu tirer de cette définition une définition également précise pour la convergence d'une suite à termes dans *BbbR* vers une limite dans *BbbR*, que les mathématiciens comprirent que cette définition pouvait être restreinte au cas des suites à termes dans $\mathbb{Q}$ et utilisée pour fournir une construction rigoureuse de l'ensemble *BbbR* des nombres réels, qu'ils avaient précédemment pris comme une donnée, en se fiant à une image géométrique qui identifiait cet ensemble avec l'ensemble des points sur une droite, ou, pour être plus précis, des valeurs de segments qu'on peut prendre sur une droite (cf. la note historique 6.5).

Il est impossible de déterminer avec précision le moment où les mathématiciens ont commencé à parler de limite. Il est pourtant certain que le premier à faire un usage très large d'une notion proche de celle de limite, et à essayer de construire sur cette notion une véritable théorie mathématique, fut Isaac Newton, qui utilisa l'idée de limite pour justifier des résultats qu'il posa à la base de sa théorie des fluxions, la théorie qui deviendra plus tard ce que nous connaissons aujourd'hui comme le calcul infinitésimal. Lorsque Newton employait cette notion, il avait surtout derrière la tête l'idée d'une valeur fixe vers laquelle une variable s'approche de plus en plus, comme dans un mouvement continu qui tend vers un certain but. Certes, Newton savait très

bien que les valeurs assumées par beaucoup de ses variables dépendaient des valeurs assumées par d'autres variables, c'est-à-dire, comme on le dirait aujourd'hui, que ces variables étaient en réalité des fonctions d'autres variables. Pourtant, il n'élabora jamais sa proto-théorie des limites à un degré suffisant pour éclairer généralement la relation qui s'instaure entre la limite d'une fonction d'une certaine variable et la limite de cette variable. *De facto*, il continua à travailler avec des limites de variables qui, pour ainsi dire, variaient continûment de façon naturelle. Il ne pensait à la limite d'une suite que comme à la limite de la variable, à variation discrète, qui prend successivement toutes les valeurs indiquées par les termes de cette suite. Dans ce contexte, une suite convergente n'était pensée que comme une suite dont les termes ont des valeurs qui tendent de plus en plus à se rapprocher d'une valeur fixe, sans que cette idée ne fût jamais éclairée davantage. En réalité, Newton ne traitait de suites que comme moyens pour travailler sur les séries, étant donné que la limite d'une série peut, tout naturellement, être pensée et définie (comme l'on vient de voir) comme la limite de la suite de ses réduites partielles.

On a souvent soutenu qu'entre Newton et Cauchy (c'est-à-dire *grosso modo* entre les années '60 du XVII$^{\text{ème}}$ siècle et les années '20 du XIX$^{\text{ème}}$) les mathématiciens n'eurent aucun égard à la convergence des séries avec lesquelles ils travaillaient. Ceci est tout simplement faux. Ce qui est vrai est qu'avant Cauchy, les mathématiciens pensaient que des séries de fonctions — c'est-à-dire les séries telles que leurs termes $u_i$ sont des fonctions non seulement de $i$, mais aussi d'une autre variable $x$, qui généralement était conçue comme une variable à valeurs réelles — pouvaient être déclarées égales à d'autres fonctions de $x$, même si $x$ prenait des valeurs qui rendaient ces séries divergentes, tout en sachant fort bien que, dans ce cas, ces égalités n'étaient pas des égalités numériques, mais indiquaient de simples relations formelles (on a déjà évoqué cette situation dans la note historique 6.6, où on a donné un exemple d'une série de fonctions qui ne converge que pour certaines valeurs de la variable). La distinction entre séries convergentes et séries divergentes ne concernait donc pas la légitimité de l'affirmation de certaines égalités générales, mais la possibilité de l'application de ces égalités à des calculs numériques. Pourtant, bien que, entre Newton et Cauchy, la capacité de distinguer entre séries convergentes et séries divergentes, et de calculer les limites des premières, progressa de manière notable, les mathématiciens continuèrent essentiellement à penser la convergence d'une série *via* la notion newtonienne de limite, c'est-à-dire de manière fort informelle et imprécise. Si ceci ne porta pas, *in concreto*, à des erreurs majeures, ce n'était certes pas sur ces bases qu'on pouvait développer une théorie convenable et claire de la convergence.

Les choses commencèrent à changer assez radicalement avec Cauchy et son *Cours d'analyse* de 1821. D'abord, ce dernier convainquit les mathématiciens de son époque que la question de la convergence d'une série de fonctions ne concernait pas les applications numériques de la théorie des séries, mais la possibilité même d'affirmer certaines égalités en général. Ensuite, il donna une définition générale de la limite d'une variable qui fait présager la conception moderne de limite. Enfin, il organisa autour du concept de limite (et de quelques autres concepts élémentaires) toute la scène de l'analyse. Quant au deuxième point, voici ce qu'il écrivit dans les « Préliminaires » à son traité : « Lorsque les valeurs successivement attribuées à une même variable s'approchent indéfiniment d'une valeur fixe, de manière à finir par en différer aussi peu que l'on voudra, cette dernière est appelée la *limite* de toutes les autres ». Ce qui compte ici, et marque la nouveauté, est naturellement la deuxième partie de la définition : « de

manière à finir par en différer aussi peu que l'on voudra ». C'est cet éclaircissement de la définition classique qui va gouverner les démonstrations successives. Si Cauchy veut prouver que la valeur $X$ est la limite de la variable $x$ (ou, si on préfère, de ses valeurs), il n'a qu'à montrer que, pour toute quantité positive $h$, il y a une valeur $\overline{x}$ de $x$, telle que, pour toutes les valeurs $\overline{\overline{x}}$ successives à $\overline{x}$, la différence entre $X$ et $\overline{\overline{x}}$ est plus petite que $h$. Il n'y a plus besoin de se réclamer de l'infini et de l'infiniment petit. C'est en revanche l'infiniment petit qui se laisse définir en termes de limite : « Lorsque les valeurs numériques successives d'une même variable décroissent indéfiniment, de manière à s'abaisser au- dessous de tout nombre donné, cette variable devient ce qu'on nomme un *infiniment petit* ou une quantité *infiniment petite*. Une variable de cette espèce a zéro pour limite ». Autrement dit : le terme « infiniment petit » ne sert qu'à désigner une variable dont la limite est zéro, c'est-à-dire une variable $x$, telle que, quel que soit $h$ positif, il y a une valeur $\overline{x}$ de $x$, telle que, pour toutes les valeurs $\overline{\overline{x}}$ successives à $\overline{x}$, $|\overline{\overline{x}} - 0| < h$. Enfin, bien que de manière encore assez confuse, autant dans la définition que dans ses applications, Cauchy se réclame de la notion de limite pour caractériser les séries convergentes. Une suite $\{u_i\}_{i=0}^{\infty}$ étant donnée, Cauchy pose

$$s_n = u_0 + u_1 + u_2 + \ldots + u_{n-1}$$

et postule : « Si, pour des valeurs de $n$ toujours croissantes, la somme $s_n$ s'approche indéfiniment d'une certaine limite $s$, la série sera dite convergente, et la limite en question s'appellera la somme de la série ». L'usage du terme « limite », en renvoyant, du moins implicitement, à la définition des « préliminaires », permet d'interpréter ainsi : la série $\sum_{i=0}^{\infty} u_i$ associée à la suite $\{u_i\}_{i=0}^{\infty}$ converge vers $s$, si, quel que soit $h$ positif, il y a une valeur $s_N$ de la variable $s_n$ (c'est-à-dire, une valeur $N$ de $n$) telle que pour toutes les valeurs $s_m$ successives à $s_N$ (c'est-à-dire, pour tout $m$ plus grand que $N$) la différence $|s - s_m|$ est plus petite que $h$.

On peut penser qu'une telle interprétation est trop charitable et cache des incertitudes et parfois de véritables confusions qui restent présentes chez Cauchy. La question mériterait d'être discutée sur le plan historique, mais, même si on suppose qu'il en est ainsi, il reste que les définitions de Cauchy ouvrirent la voie à la systématisation que nous considérons aujourd'hui comme définitive, de la théorie des limites et de la convergence. Cette systématisation arriva avec l'œuvre de Karl Weierstrass et de ses leçons d'analyse à l'université de Berlin. D'abord, celui-ci comprit que la véritable question n'était pas celle de la limite d'une variable, mais celle de la limite d'une fonction. Ensuite, il comprit que la notion de limite d'une fonction tient à une relation, exprimée à son tour par une fonction, entre deux variations. Ainsi, il posa qu'une fonction $f(x)$ d'une variable $x$ tend vers la limite $F$, lorsque la variable $x$ tend vers $X$, si et seulement si pour toute valeur positive $\varepsilon$, il y a une valeur positive $\delta$, telle que : si $|x - X| < \delta$, alors $|f(x) - F| < \varepsilon$. Ce n'est donc plus la limite d'une variable qui est définie, mais la limite d'une fonction d'une certaine variable, lorsque cette variable tend vers une certaine limite. La condition « lorsque cette variable tend vers une certaine limite » ne doit pas d'ailleurs être éclairée indépendamment par une nouvelle définition. L'expression « limite d'une fonction d'une certaine variable, lorsque cette variable tend vers une certaine limite » doit être prise comme un tout défini *via* l'implication : $|x - X| < \delta \Rightarrow |f(x) - F| < \varepsilon$. C'est la définition qui est devenue ensuite célèbre comme la définition $\varepsilon$-$\delta$ de la limite d'une fonction, une définition

qui se réclame, comme on le voit assez aisément, d'une relation entre $\delta$ et $\varepsilon$, c'est-à-dire, pour s'exprimer dans les termes de la note historique 5.1, de l'existence d'un $\delta$ conditionnée par le choix préalable de $\varepsilon$.

D'ici, pour passer à la convergence d'une suite, il suffit d'observer qu'une suite $\{u_i\}_{i=0}^{\infty}$ peut être prise comme une fonction $u(i)$ de l'indice $i$ et de postuler qu'une suite $\{u_i\}_{i=0}^{\infty}$ converge vers la limite $U$ si et seulement si $U$ est la limite de $u(i)$, lorsque $i$ tend vers l'infini. Comme « tendre vers l'infini » ne signifie rien d'autre que devenir de plus en plus grand, il s'ensuit qu'une suite $\{u_i\}_{i=0}^{\infty}$ converge vers la limite $U$ si et seulement si pour toute valeur positive $\varepsilon$, il y a un nombre naturel $n$ tel que : si $i > n$, alors $|u_i - U| < \varepsilon$. Ce n'est, comme on le voit, rien d'autre qu'une généralisation de la définition 2.6.

**Lectures possibles** : J. Dhombres, *Nombre, mesure et continu. Épistémologie et histoire*, Cedic et F. Nathan, Paris, 1978.

* * *

Quand Augustin-Louis Cauchy naquit à Paris, le 21 août 1789, la France vivait, dans l'enthousiasme pour les uns et l'angoisse pour les autres, les premières semaines de la Révolution. Louis-François Cauchy, son père, comptait parmi les seconds. Ancien haut fonctionnaire de police, il voyait non seulement sa carrière, mais aussi sa vie fort en danger. Il sut pourtant s'adapter aux circonstances et, après avoir obtenu d'autres positions dans l'administration de l'État, il se retrouva, en 1800, après le 18 Brumaire, parmi les fonctionnaires du Sénat, avec un rang de première importance qui lui valut un logement de fonction au Palais du Luxembourg. Ce fut là qu'Augustin-Louis grandit, côtoyant de grandes personnalités de l'empire, et entra surtout en contact avec Laplace, chancelier du Sénat et supérieur direct de son père.

En 1805, il réussit son concours d'entrée à l'École Polytechnique et en 1807 il fut admis à l'École des Ponts et Chaussées. Nommé d'abord aspirant-ingénieur et puis ingénieur ordinaire de deuxième classe, il fut destiné au chantier de Cherbourg, où il resta presque trois ans, du début de 1810 à la fin de 1812. À Cherbourg, il poursuivit seul ses études de mathématiques, qui lui permirent d'envoyer à l'Institut deux mémoires fort appréciés à propos de polyèdres (dont un, fort célèbre, marque les origines de la topologie algébrique). En 1812, il fut nommé correspondant de la Société Philomatique, dont il devint membre en 1814. Cependant, d'abord en 1813, et plus tard en 1814 et en 1815, sa candidature pour un poste à la section de géométrie de l'Institut fut sèchement refusée.

Bien qu'ils sussent s'adapter aux institutions impériales, Louis-François et Augustin-Louis Cauchy étaient restés des catholiques royalistes et il saluèrent avec enthousiasme et esprit de vengeance le retour de la monarchie. Membre de la Congrégation de la Sainte-Vierge dès 1808, Augustin-Louis pouvait d'ailleurs compter sur l'appui de cette institution dont le pouvoir grandissait : en décembre 1815, il fut nommé professeur à l'École Polytechnique et le 21 mars 1816, il fut nommé d'office à l'Académie des Sciences, par une ordonnance qui, en rétablissant la vieille institution et en effaçant l'Institut, imposait de nouveaux membres pour combler les nombreuses épurations. Ce n'était pas la façon la plus heureuse d'intégrer l'institution qui l'avait repoussé par trois fois, mais elle s'adaptait bien à la personnalité de Cauchy, qui d'ailleurs s'imposa bientôt comme un des savants les plus influents (mais aussi les moins aimés et les plus intrigants) de l'Académie.

Nommé professeur remplaçant, d'abord à la faculté des sciences, en 1821, et ensuite au Collège de France, en 1824, Cauchy partagea les années de la Restauration entre l'enseignement, la recherche et l'activité d'académicien. Pour soutenir son enseignement à l'École Polytechnique, il publia en 1821 le *Cours d'Analyse de l'École Royale Polytechnique* et en 1823 le *Résumé des leçons données à l'École Royale Polytechnique sur le calcul infinitésimal*. En même temps que, par ses recherches de pointe, il ouvrait de nouvelles frontières à la physique mathématique et il fondait l'analyse complexe, il bouleversa par ces deux œuvres didactiques les fondements de l'analyse réelle et du calcul différentiel et intégral.

Sa carrière fut pourtant brusquement interrompue par la Révolution de Juillet. Sa position avait été trop liée à la politique de la Restauration et il dut quitter la France. Il alla d'abord en Suisse, puis en Italie, où il s'installa à Turin, avec la charge de professeur de physique. En 1833, il se rendit à Prague, comme précepteur du Duc de Bordeaux et en 1836 à Gorizia, à la suite de la cour de ce dernier. En 1838 il rentra à Paris, il réintégra l'Académie, où il avait conservé sa place, et il commença à communiquer les résultats des recherches accomplies pendant l'exil. Nommé en 1839 au bureau des Longitudes, d'où il sera rejeté en 1843, il continua ses recherches en analyse complexe et en algèbre, et en 1849 il fut nommé professeur d'astronomie mathématique à la Faculté des Sciences de Paris. Après le Coup d'État de 1851, fidèle à ses convictions légitimistes, il refusa de prêter serment de fidélité à l'Empereur. Il mourut à Sceaux, le 23 mai 1857.

**Lectures possibles** : B. Belhoste, *Cauchy, un mathématicien légitimiste au* XIX$^{\text{ème}}$ *siècle*, Belin, Paris, 1985.

* * *

Karl Weierstrass naquit à Ostenfelde, près de M ?nster, le 31 octobre 1815. Entré à quatorze ans au Gymnase catholique de Padeborn, il s'inscrit en 1834 à l'université de Bonn, pour y étudier le droit. Il échoua pourtant dans ses études et après quatre ans, il rentra chez sa famille, sans avoir obtenu aucun titre. En 1839 il commença de nouvelles études à Münster pour préparer le certificat d'aptitude à l'enseignement dans les écoles secondaires. Parmi ses nouveaux professeurs, il y avait le mathématicien Christof Gudermann, dont il suivit, comme unique élève, un cours consacré aux fonctions elliptiques. Ce fut le début de la fascination de Weierstrass pour les mathématiques et en particulier pour l'analyse. En 1841, Weierstrass obtint son certificat et il commença à enseigner les mathématiques dans les écoles secondaires. Il se consacra en même temps à des recherches sur des sujets d'analyse, et en 1854 un de ses articles, à propos de fonctions abéliennes, fut publié dans le *Journal* de Crelle, et lui valut, en 1856, sa nomination d'abord à l'université et ensuite à l'Académie de Berlin. Il s'imposa rapidement, malgré son âge relativement avancé, comme un enseignant extraordinaire et un mathématicien fort prolifique. Ses contributions originales à l'analyse réelle et complexe furent fort nombreuses, et grâce à son enseignement, il parvint graduellement à donner un visage nouveau aux fondements de l'analyse réelle. Il abandonna l'enseignement en 1890 et mourut à Berlin le 19 février 1897.

**Lectures possibles** : R. Bölling, « Karl Weierstrass : Stationen eines Lebens », *Jahresberichte der Deutschen mathematike Vereinigung*, 96, 1994, pp. 56-75 ; K.-R. Biermann und G. Schubring, « Einige Nachträge zur Bigraphie von Karl Weierstrass »,

in J. W. Dauben (ed. by), *History of Mathematics : State of the Art*, Academic Press, San Diego, 1996, pp. 65-91.

En partant de la définition 2.5, il est possible de démontrer qu'une série $\sum_{i=0}^{\infty} u_i$ ne converge vers une certaine limite dans un ensemble $E$, auquel on suppose que ses termes appartiennent, relativement à la distance donnée par la valeur absolue de la différence de deux éléments de $E$, qu'à condition que l'addition soit définie sur $E$ de manière à admettre dans $E$ un élément neutre, disons $e$, et que la suite $\{u_i\}_{i=0}^{\infty}$ de termes de cette série converge vers $e$ dans $E$. Cette démonstration est laissée au lecteur en guise d'éxercice. Si $E$ coïncide avec $\mathbb{Q}$, alors $e = 0$. Une série $\sum_{i=0}^{\infty} u_i$ à termes dans $\mathbb{Q}$ ne converge donc vers une certaine limite dans $\mathbb{Q}$ qu'à condition que la suite $\{u_i\}_{i=0}^{\infty}$ de ses termes converge vers 0 dans $\mathbb{Q}$. Ainsi si la suite $\{u_i\}_{i=0}^{\infty}$ est divergente dans $E$, la série $\sum_{i=0}^{\infty} u_i$ l'est aussi.

REMARQUE 6.9. De là il suit que toute série à termes dans $\mathbb{N}$ est divergente dans $\mathbb{N}$, relativement à la distance donnée par la valeur absolue de la différence de deux termes de $\mathbb{N}$, sauf dans le cas fort particulier où ses termes s'annulent tous au-delà d'une certaine valeur de $i$, ce qui réduit une telle série à une addition ordinaire. Cela est en particulier le cas de toutes les séries à termes dans $\mathbb{N}$, à partir des quelles on peut construire les séries dont on a considéré les réduites partielles dans le chapitre 4.

La convergence de la suite $\{u_i\}_{i=0}^{\infty}$, vers $e$ dans $E$ n'est pourtant qu'une condition nécessaire pour la convergence de la série associée $\sum_{i=0}^{\infty} u_i$ vers une certaine limite dans $E$. Il est en fait possible de construire des suites convergentes vers $e$ dans $E$, telles que les séries associées sont divergentes dans $E$. Un exemple bien connu est justement fourni par la suite harmonique. On peut en effet démontrer le théorème suivant :

THÉORÈME 2.2. *La série* $\sum_{i=0}^{\infty} \frac{1}{i+1}$ *, dite « série harmonique », associée à la suite harmonique, diverge dans* $\mathbb{Q}$.

**Preuve**. Il n'est pas facile de prouver ce théorème en se réclamant directement de la définition de convergence d'une série dans $\mathbb{Q}$ vers une certaine limite dans $\mathbb{Q}$. Généralement les mathématiciens le prouvent en ayant recours à l'un des nombreux critères ou conditions suffisantes de convergence qu'on peut déterminer à partir de cette définition.

Une manière très simple de le faire est de se réclamer de la condition suffisante suivante : si $\sum_{i=0}^{\infty} v_i$ et $\sum_{i=0}^{\infty} u_i$ sont deux séries à termes dans $\mathbb{Q}^+ - \{0\}$ (c'est-à-dire que leurs termes sont tous des nombres fractionnaires strictement positifs) tels que, quel que soit $i$,

$$v_i \leq u_i$$

et la série $\sum_{i=0}^{\infty} v_i$ est telle que les termes $\sum_{i=0}^{h} v_i$ $(h = 0, 1, 2, ...)$ de la suite de ses réduites partielles croissent dans $\mathbb{Q}$ au-delà de toute limite, c'est-à-dire que, pour tout nombre rationnel (strictement positif) $\Lambda$, il y a un nombre naturel $n$, tel que

$$h > n \Rightarrow \sum_{i=0}^{h} v_i > \Lambda$$

alors les termes $\sum_{i=0}^{h} u_i$ $(h = 0, 1, 2, ...)$ de la suite des réduites partielles de la série $\sum_{i=0}^{\infty} u_i$ croissent dans $\mathbb{Q}$ au-delà de toute limite, et donc la série $\sum_{i=0}^{\infty} u_i$ est divergente dans $\mathbb{Q}$. La preuve de cette implication peut être laissée au lecteur comme exercice.

On considère alors la série à termes dans $\mathbb{Q}^+ - \{0\}$

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \underbrace{\frac{1}{8} + \ldots + \frac{1}{8}}_{4 \text{ fois}} + \underbrace{\frac{1}{16} + \ldots + \frac{1}{16}}_{8 \text{ fois}} + \ldots = \sum_{i=1}^{\infty} \underbrace{\frac{1}{2^1} + \ldots + \frac{1}{2^i}}_{2^{i-1} \text{ fois}}$$

Si on considère cette série comme l'addition infinie $\sum_{i=0}^{\infty} v_i$ des termes $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{4}, \frac{1}{8}, \ldots$, on aura successivement

$$v_0 = 1 \; ; v_1 = \frac{1}{2} \; ; v_2 = \frac{1}{4} \; ; v_3 = \frac{1}{4} \; ; v_4 = \frac{1}{8} \; ; \ldots$$

Donc, si on pose $\sum_{i=0}^{\infty} u_i = \sum_{i=0}^{\infty} \frac{1}{i+1}$, on aura, pour tout $i$ naturel, $v_i \leq u_i$. Mais, quel que soit $i$, on aura aussi

$$\underbrace{\frac{1}{2^i} + \cdots + \frac{1}{2^i}}_{2^{i-1} \text{ fois}} = \frac{1}{2}$$

et donc

$$1 + \sum_{i=1}^{\infty} \underbrace{\frac{1}{2^i} + \cdots + \frac{1}{2^i}}_{2^{i-1} \text{ fois}} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots$$

Le lecteur pourra s'exercer à montrer que cette série est telle que les termes $1, \frac{3}{2}, \frac{4}{2}, \frac{5}{2}, \ldots$ de la suite de ses réduites partielles croissent dans $\mathbb{Q}$ au-delà de toute limite ; il ne rencontrera pour cela aucune difficulté. Or, comme la série $1 + \sum_{i=1}^{\infty} \underbrace{\frac{1}{2^i} + \cdots + \frac{1}{2^i}}_{2^{i-1} \text{ fois}}$ résulte de la série $\sum_{i=0}^{\infty} v_i$ en regroupant des termes successifs, il s'ensuit que la série $\sum_{i=0}^{\infty} v_i$ est aussi telle que les termes $\sum_{i=0}^{h} v_i$ $(h = 0, 1, 2, \ldots)$ de la suite de ses réduites partielles croissent dans $\mathbb{Q}$ au-delà de toute limite. Il suffira alors de se réclamer de la condition suffisante précédente pour conclure que la série harmonique est divergente dans $\mathbb{Q}$. □

REMARQUE 6.10. Le lecteur est invité à réfléchir sur la manière dont cette preuve emploie la possibilité de mettre un ensemble infini (dénombrable) en correspondance biunivoque avec une de ses parties propres ; une propriété des ensembles infinis qu'on a discutée abondamment dans le chapitre 4.

Un exemple d'une série à termes dans $\mathbb{Q}$, y convergeant vers une certaine limite est en revanche celui de la série des inverses des carrés :

THÉORÈME 2.3. *La série* $\sum_{i=0}^{\infty} \frac{1}{2^i}$ *converge vers* 2 *dans* $\mathbb{Q}^+$ *(et donc dans* $\mathbb{Q}$*).*

**Preuve.** À la différence du précédent, ce théorème peut être prouvé fort facilement en se réclamant directement de la définition 2.6. Quel que soit le nombre naturel $j$, on aura en effet,

d'après le théorème 2.1,

$$\sum_{i=0}^{j} \frac{1}{2^i} = \frac{2^j + 2^{j-1} + 2^{j-2} + ... + 2 + 1}{2^j} = \frac{\sum_{i=0}^{j} 2^i}{2^j} = \frac{1 - 2^{j+1}}{(1-2)2^j} = \frac{2^{j+1} - 1}{2^j}$$

De là, il s'ensuit sur-le-champ que

$$\left| 2 - \sum_{i=0}^{j} \frac{1}{2^i} \right| = 2 - \frac{2^{j+1} - 1}{2^j} = \frac{1}{2^j}$$

et il est aisé de vérifier que, quel que soit le nombre rationnel strictement positif $\varepsilon$ il est toujours possible de prendre la valeur de $j$ assez grande pour que $\left| 2 - \sum_{i=0}^{j} \frac{1}{2^i} \right| < \varepsilon$. □

NOTE HISTORIQUE 6.8. La série des inverses des carrés, ou du moins la série qui dérive de celle-ci lorsqu'on lui enlève le premier terme, a été souvent associée au premier des quatre paradoxes de Zénon à propos du mouvement, qui sont exposés et discutés par Aristote dans le VI$^{\text{ème}}$ livre de la *Physique*, le paradoxe de la dichotomie.

De ces quatre paradoxes, celui de la dichotomie est celui qui est exposé le moins clairement par Aristote, qui, on peut dire, se limite à le réfuter bien avant de l'avoir précisément présenté. « Dans le premier [ argument de Zénon] — écrit Aristote [239b 11-13] — l'impossibilité du mouvement est tirée de ce que le mobile transporté doit parvenir d'abord à la moitié avant d'accéder au terme ». Après cette entrée en matière, Aristote renvoie à un passage précédent, où il avait dénoncé une erreur dans l'argument de Zénon, consistant à affirmer « que les infinis ne peuvent être parcourus ou touchés chacun successivement en un temps fini » [233a 22-23]. La comparaison entre ces deux passages ne peut que laisser perplexe.

Du second, il semblerait que l'argument de Zénon consiste en ceci : si un mobile doit parcourir un espace, disons $S$, il doit d'abord en parcourir la moitié, $\frac{1}{2}S$, ensuite la moitié de la partie restante, $\frac{1}{4}S$, et encore ensuite la moitié de la partie qui reste encore à parcourir, $\frac{1}{8}S$, et ainsi de suite, de sorte qu'avant de parvenir à son but, il devra parcourir une infinité de traits, et il n'est pas possible, dans un temps fini, de parcourir une infinité de traits. Si l'argument de Zénon était celui-ci, la connexion avec la série des inverses des carrés viendrait du fait que Zénon ne ferait, en dernière instance, qu'obtenir une unité d'espace comme la somme des portions de cette unité qui correspondent aux termes successifs au premier dans cette série. Pourtant, on comprend mal pourquoi la convergence de cette série vers 2 , ou bien la convergence vers 1 de la série qui en résulte en éliminant le premier terme, devrait être un argument à opposer aux conclusions de Zénon, comme il a été dit trop souvent et beaucoup trop rapidement.

Au contraire, ceci semblerait être plutôt une prémisse de l'argument. Le bon contre-argument à opposer à Zénon serait plutôt celui d'Aristote : le temps peut, lui-aussi, être divisé comme l'on divise l'espace (car la division de l'espace dont relève l'argument de Zénon n'est qu'une division en puissance, et non pas en acte).

Si on fait confiance, en revanche, au premier passage d'Aristote, l'argument de Zénon semble être tout autre. Loin de concéder que le mobile puisse, de toute manière, parcourir la première moitié de $S$, puis la moitié de la deuxième moitié de $S$, et ainsi de suite, ce qui paraît une prémisse assez bizarre pour un argument qui devrait nier la possibilité du mouvement, Zénon semblerait nier la possibilité qu'un corps parvienne

à se mouvoir, en affirmant qu'avant de parcourir n'importe quel espace, il devrait parcourir la moitié de cet espace, et, avant d'en parcourir la moitié, la moitié de la moitié, et la moitié de la moitié de la moitié, et ainsi de suite. Ainsi conçu l'argument de Zénon paraît bien plus conséquent, et il se fonderait non pas sur la possibilité d'obtenir une unité d'espace en additionnant sa moitié, avec la moitié de sa moitié, la moitié de la moitié de sa moitié, et ainsi de suite, mais plutôt sur la possibilité d'enlever de cette unité d'espace, quelle qu'elle soit, d'abord sa moitié, ensuite la moitié de sa moitié, la moitié de la moitié de sa moitié et ainsi de suite. Comme de la convergence vers 2 de la série des inverses des carrés, il résulte l'égalité

$$1-\frac{1}{2}-\frac{1}{2^2}-\frac{1}{2^3}-\ldots=1-\left[\left(\sum_{i=0}^{\infty}\frac{1}{2^i}\right)-1\right]=1-(2-1)=0$$

il semblerait cependant que ce résultat, loin de réfuter l'argument de Zénon, en fournisse une confirmation. Pour réfuter cet argument, on devrait alors utiliser encore une fois des arguments similaires à celui d'Aristote, qui pourtant, pris en tant que tel, ne semblerait pas faire l'affaire dans ce cas.

Naturellement, il n'est pas dans mon intention de discuter ici plus en détails (autant logiques que philologiques) l'argument de Zénon, ni de dire comment il peut, s'il le peut, être résolu. Mon ambition est bien plus modeste. Je voudrais m'appuyer sur cet exemple pour faire une observation plus générale : dans la plupart des cas (et je crois même dans la totalité) la prétention de pouvoir utiliser, comme tel, un résultat mathématique comme argument en faveur ou contre une certaine thèse philosophique (qui ne concerne pas, s'il y en a une, la philosophie mathématique intimement connectée avec ce résultat) est illusoire ; un résultat mathématique n'est jamais qu'un résultat mathématique, si on veut l'employer pour affirmer une thèse métaphysique, on doit l'interpréter d'une manière ou de l'autre et le connecter d'une manière ou d'une autre avec d'autres arguments, ces interprétations et connexions, n'étant pas, quant à elles, du ressort des mathématiques. Donc, affirmer que le résultat mathématique $X$ apporte un soutient à la thèse philosophique $T$ ne peut que revenir à avancer qu'une certaine interprétation du résultat $X$, apte à établir des connexions (logiques ou métaphoriques) entre ce résultat et des thèses ou des arguments philosophiques, apporte un soutient à la thèse $T$.

**Lectures possibles** : M. Cavaing, *Zénon d'Élée. Prolégomènes aux doctrines du continu*, Vrin, Paris, 1982.

Remarque 6.11. Les considérations précedentes nous permettent d'énoncer une généralisation remarquable du théorème 4.2. On suppose que $a$ et $b$ sont tels qu'il soit possible de diviser $b$ par $a$ (ceci est par exemple le cas si $a$ et $b$ sont deux nombres rationnels et $a$ est différent de 0). On peut alors écrire le binôme $(a+b)$ sous la forme du produit $a(1+\frac{b}{a})$. En appliquant ce théorème, on aura alors

$$\left[a\Big(1+\frac{b}{a}\Big)\right]^n=a^n\left(1+\frac{b}{a}\right)^n=\sum_{i=0}^{n}\frac{\prod_{k=0}^{i-1}(n-k)}{i!}a^{n-i}b^i$$

et, en posant $\frac{b}{a}=x$ :

$$(1+x)^n=\frac{a^n\,(1+x)^n}{a^n}=\sum_{i=0}^{n}\frac{\prod_{k=0}^{i-1}(n-k)}{i!}x^i$$

(car, comme on le montrera tout à l'heure, pour tout nombre rationnel $\mathfrak{q}$ et tout nombre naturel $h$, $\mathfrak{q}^{-h} = \frac{1}{\mathfrak{q}^h}$), qui est finalement la plus simple des expressions possibles du développement binomial pour un exposant naturel quelconque.

Imaginons maintenant que dans le produit

$$\frac{\prod_{k=0}^{i-1}(n-k)}{i!}$$

où $i$ est un nombre naturel quelconque strictement positif, on substitue le nombre naturel $n$ avec un nombre rationnel quelconque « $\frac{p}{q}$ ». On obtiendra le produit

$$\frac{\prod_{k=0}^{i-1}(\frac{p}{q}-k)}{i!} = \frac{\left(\frac{p}{q}\right)\left(\frac{p}{q}-1\right)\left(\frac{p}{q}-2\right)...\left(\frac{p}{q}-(i-1)\right)}{i!}$$

Comme $i$ est un nombre naturel strictement positif, $i-1$ est un nombre naturel, et, si $\frac{p}{q}$ n'est pas à son tour un nombre naturel, il n'y a pas de valeurs de $i$ qui rendent la différence $\frac{p}{q}-(i-1)$ égale à 0, et annulent du même coup le produit

$$\frac{\prod_{k=0}^{i-1}(\frac{p}{q}-k)}{i!}$$

Cela signifie que l'addition

$$1 + \frac{\prod_{k=0}^{0}(\frac{p}{q}-k)}{1!}x + \frac{\prod_{k=0}^{1}(\frac{p}{q}-k)}{2!}x^2 + \frac{\prod_{k=0}^{2}(\frac{p}{q}-k)}{3!}x^3 + ...$$

peut être réitérée à l'infini sans qu'aucun de ses termes ne s'annule. On a ainsi une série que, en généralisant le symbolisme adopté pour les coefficients binomiaux référés à des exposants naturels, on écrit ainsi :

$$\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$$

Comme on a obtenu cette série en substituant $\frac{p}{q}$ à $n$ dans le développement de $(1+x)^n$, il est naturel de se demander si une telle série converge vers $(1+x)^{\frac{p}{q}}$ dans quelques ensembles auxquels appartiennent la puissance $(1+x)^{\frac{p}{q}}$ et les termes $\binom{p/q}{i}x^i$. Si on suppose que $x$ est un nombre rationnel, alors les termes $\binom{p/q}{i}x^i$ sont des nombres rationnels, et il est donc naturel de se demander si la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$ converge vers $(1+x)^{\frac{p}{q}}$ dans $\mathbb{Q}$.

Pour donner un sens à cette question, il faut d'abord comprendre ce que peut signifier qu'un nombre rationnel est élevé à une puissance fractionnaire. Comme par définition on a, quels que soient les nombres naturels $m$ et $n$ et le nombre rationnel $\mathfrak{q}$,

$$(\mathfrak{q}^m)^n = \underbrace{\mathfrak{q}^m \cdot \mathfrak{q}^m \cdot \ldots \mathfrak{q}^m}_{nfois}$$

$$= \underbrace{\left(\underbrace{\mathfrak{q}\cdot\mathfrak{q}\cdot\ldots\mathfrak{q}}_{mfois}\right)\cdot\left(\underbrace{\mathfrak{q}\cdot\mathfrak{q}\cdot\ldots\mathfrak{q}}_{mfois}\right)\cdot\ldots\cdot\left(\underbrace{\mathfrak{q}\cdot\mathfrak{q}\cdot\ldots\mathfrak{q}}_{mfois}\right)}_{nfois} = \mathfrak{q}^{mn}$$

si on pose $t = mn$, on aura

$$\mathfrak{q}^t = (\mathfrak{q}^m)^n$$

Ainsi, si on note par « $\sqrt[s]{z}$ », $s$ étant un nombre naturel quelconque et $z$ l'élément d'un ensemble sur lequel est définie une multiplication, l'opération inverse à la puissance $z^s$ — de sorte que $\sqrt[s]{z} = y$ si et seulement si $y^s = z$ — on aura

$$\mathfrak{q}^m = \mathfrak{q}^{\frac{t}{n}} = \sqrt[n]{\mathfrak{q}^t}$$

et, en généralisant, quels que soient les nombres naturels $h$ et $k$ ($k \neq 0$),

$$\mathfrak{q}^{\frac{h}{k}} = \sqrt[k]{\mathfrak{q}^h} \tag{81}$$

D'autre part, comme, quels que soient les nombres naturels $n$ et $m$,

$$\mathfrak{q}^{n+m} = \mathfrak{q}^n \cdot \mathfrak{q}^m$$

si on pose $s = n + m$, on aura

$$\mathfrak{q}^s = \mathfrak{q}^n \cdot \mathfrak{q}^m$$

et donc

$$\mathfrak{q}^n = \mathfrak{q}^{s-m} = \frac{\mathfrak{q}^s}{\mathfrak{q}^m}$$

et, en généralisant, quels que soit le nombre naturel $h$,

$$\mathfrak{q}^{-h} = \frac{1}{\mathfrak{q}^h} \tag{82}$$

En combinant 81 et 82, on aura alors, quel que soient le nombre rationnel $\mathfrak{q}$ et les nombres relatifs $p$ et $q$ ($q \neq 0$)

$$\mathfrak{q}^{-\frac{h}{k}} = \frac{1}{\sqrt[k]{\mathfrak{q}^h}} \tag{83}$$

Cela résout notre problème préliminaire en donnant un sens à l'écriture $(1+x)^{\frac{p}{q}}$, où $x$ et $\frac{p}{q}$ sont deux nombres rationnels quelconques. Il reste à savoir, pour répondre à notre question précédente, si la série $\sum_{i=0}^{\infty} \binom{p/q}{i} x^i$ converge vers $(1+x)^{\frac{p}{q}}$ dans $\mathbb{Q}$. Pourtant, (83) nous fait comprendre sur le champ qu'il ne suffit pas de supposer que $x$ soit un nombre rationnel pour que $(1+x)^{\frac{p}{q}}$ le soit aussi. Il suffit, par exemple, que $x$ soit égal à 1 et $\frac{p}{q}$ soit égale à $\frac{1}{2}$ pour que $(1+x)^{\frac{p}{q}}$ soit égale à $2^{\frac{1}{2}} = \sqrt{2}$, qui comme on l'a vu ci-dessus, n'est guère un nombre rationnel. Même si on suppose que $x$ est un nombre rationnel, il est ainsi plus raisonnable de se demander si la série $\sum_{i=0}^{\infty} \binom{p/q}{i} x^i$ converge vers $(1+x)^{\frac{p}{q}}$, non pas dans l'ensemble des nombres rationnels, mais dans une extension de cet ensemble qui comprend la valeur de $(1+x)^{\frac{p}{q}}$, quels que soient $x$ et $\frac{p}{q}$. Le lecteur comprendra plus tard que l'ensemble $\mathbb{R}$ des nombres réels est justement une extension de $\mathbb{Q}$ qui respecte cette condition, même dans le cas où $x$ est à son tour un nombre réel. On pourra donc supposer que $x$ varie sur $\mathbb{R}$, est se demander si la série $\sum_{i=0}^{\infty} \binom{p/q}{i} x^i$ converge vers $(1+x)^{\frac{p}{q}}$ dans $\mathbb{R}$. La réponse à cette question est bien connue. Il n'est pourtant pas possible de prouver qu'elle est correcte en n'exploitant que les moyens limités qui nous sont fournis par l'exposé précédent. On s'en tiendra donc ici à l'énoncer, en la justifiant de manière absolument informelle.

Si l'on note par « $|x|$ » la valeur absolue de $x$ (c'est-à-dire $x$ si $x \geq 0$ et $-x$ si $x < 0$), alors trois cas peuvent être distingués : $|x| < 1$, $|x| = 1$ et $|x| > 1$. Si $|x| > 1$, alors la succession

$\left\{\binom{p/q}{i}x^i\right\}_{i=0}^{\infty}$ ne peut converger vers aucune limite dans $\mathbb{R}$, car la valeur absolue du facteur $x^i$ croît beaucoup plus rapidement que la valeur absolue du terme $\binom{p/q}{i}$ ne pourra décroître, la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$ sera alors divergente dans $\mathbb{Q}$. Si $|x| = 1$, alors la réponse à notre question dépend de la valeur de $\frac{p}{q}$. Enfin, si $|x| < 1$, alors la valeur absolue du facteur $x^i$ décroît beaucoup plus rapidement que la valeur absolue du terme $\binom{p/q}{i}$ ne pourra croître et la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$ est sans doute convergente vers $(1+x)^{\frac{p}{q}}$ dans $\mathbb{Q}$, ce qu'on pourra exprimer par l'implication

$$(x \in \mathbb{R} \wedge |x| < 1) \Rightarrow \left[(1+x)^{\frac{p}{q}} = \sum_{i=0}^{\infty}\binom{p/q}{i}x^i\right] \tag{84}$$

qui constitue la généralisation annoncée du théorème 4.2.

On terminera en observant que le résultat précédent nous fournit un des résultats les plus fondamentaux de l'analyse : le théorème du développement binomial pour un exposant rationnel quelconque.

NOTE HISTORIQUE 6.9. Selon le point de vue moderne, le théorème du développement binomial pour un exposant rationnel consiste justement dans la détermination des conditions sous lesquelles la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$, où $x$ est supposé varier sur l'ensemble des nombres réels, converge vers $(1+x)^{\frac{p}{q}}$ dans $\mathbb{R}$, quel que soit le nombre rationnel $\frac{p}{q}$. Ce théorème établit donc un intervalle de variation de $x$ — qui, comme l'on vient de voir, va de $-1$ à 1, en excluant ces limites — tel que pour toute valeur déterminée $x_0$ que $x$ assume à l'intérieur de cet intervalle et pour tout nombre rationnel $\frac{p}{q}$, la série (de constantes) $\sum_{i=0}^{\infty}\binom{p/q}{i}x_0^i$ converge vers la valeur constante $(i+x_0)^{\frac{p}{q}}$ dans $\mathbb{R}$. Une fois qu'on a démontré le théorème 4.2 et qu'on connaît par conséquent la forme des coefficients, dits « binomiaux », qui entrent dans le développement de $(1+x)^n$, lorsque $n$ est un nombre naturel quelconque, ceci est la seule question qui semble se poser pour nous, étant donné que la détermination des coefficients $\binom{p/q}{i}$ qui entrent dans la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$ ne suit que par simple substitution de $\frac{p}{q}$ à $n$ dans la forme qui fournit les coefficients du développement de $(1+x)^n$.

Ce qu'on a dit jusqu'ici, spécialement dans les notes historiques 3.5 et 6.7, devrait pourtant nous faire comprendre que les choses n'en allèrent pas toujours ainsi. En particulier, les choses n'allaient pas ainsi au XVII$^{\text{ème}}$ siècle, lorsque Newton parvint pour la première fois, en 1665, à un résultat qui constitue un ancêtre direct de notre théorème du développement binomial pour un exposant rationnel : un ancêtre si direct que les historiens utilisent d'habitude le même nom de « théorème du développement binomial pour un exposant rationnel » pour le désigner, en précisant, parfois, de manière tout à fait anachronique, que Newton ne démontra pas ce théorème, et se contenta de l'énoncer (sans, pour autant, préciser jamais ce que Newton aurait, au juste, dû démontrer).

Newton ne possédait ni une définition précise de convergence, ni, surtout, des critères sûrs de convergence, et il n'était donc pas à même d'établir avec certitude les conditions de convergence de la série $\sum_{i=0}^{\infty}\binom{p/q}{i}x^i$, n'opérant que sur cette série, prise

en tant que telle. Son problème était plus celui d'obtenir cette série que d'en éévaluer la convergence. Et la manière dans laquelle cette série était obtenue était pour lui la garantie d'un lien entre cette même série et la puissance $(1+x)^{\frac{p}{q}}$, un lien qu'il aurait ensuite pu confirmer *a posteriori*, par des vérifications numériques.

Mais, on pourrait se demander : pourquoi Newton était-il intéressé à associer une série telle que $\sum_{i=0}^{\infty} \binom{p/q}{i} x^i$, à la puissance $(1+x)^{\frac{p}{q}}$, indépendamment, ou du moins préalablement, à l'évaluation de la convergence de cette série ? La réponse est fort simple, mais elle fait intervenir une problématique mathématique qui est totalement étrangère au parcours qui nous a conduit à énoncer la (2.2). Cela montre, encore une fois, que les directions d'évolution de l'histoire ne coïncident pas nécessairement (et même ne coïncident presque jamais) avec l'ordre logique que nous assignons aujourd'hui à l'exposition des résultats mathématiques.

Entre 1664 et 1665, à l'époque à laquelle il parvint à ses premières et plus extraordinaires acquisitions mathématiques, Newton chercheait à comprendre comment on pouvait évaluer, ou tout simplement exprimer, l'aire de la région du plan comprise entre une courbe quelconque, deux coordonnées rectilignes et un axe (cf. la note historique 4.1). En particulier, il était intéressé à évaluer, ou tout simplement à exprimer, l'aire d'une telle région du plan, lorsque la courbe qui délimite cette région est une hyperbole, une courbe d'équation $y = \frac{1}{x}$. Il était d'ailleurs au courant d'une découverte, assez récente à l'époque, due essentiellement à Grégoire de Saint-Vincent, un mathématicien jésuite belge qui avait travaillé à Rome et qui avait publié en 1647 un lourd traité, l'*Opus geometricum*, riche en résultats importants (mais vicié aussi par une erreur, la prétention d'avoir atteint la quadrature du cercle, que l'histoire ne lui pardonna jamais). Grégoire avait compris, et il l'avait dit, de manière plus ou moins claire dans l' *Opus geometricum*, que l'aire de l'hyperbole se comporte comme des logarithmes naturels. Évaluer cette aire, pour toute valeur de $x$, était donc une manière d'évaluer ces logarithmes, et l'exprimer par le biais d'une forme algébrique était une manière d'exprimer par une forme algébrique des logarithmes. Newton possédait d'ailleurs un algorithme, qu'il avait hérité pour l'essentiel de Wallis, mais qu'il avait su interpréter à sa manière, qui permettait de passer de toute équation telle que $y = \sum_{i=0}^{n} A_i x^{q_i}$ (où les $q_i$ sont des exposants rationnels quelconques, mais différents de $-1$, et les $A_i$ des coefficients constants quelconques) à une écriture de la forme $\sum_{i=0}^{n} B_i x^{p_i}$ (où les $p_i$ et les $B_i$ sont encore respectivement des exposants rationnels et des coefficients constants quelconques) exprimant l'aire délimitée par la courbe exprimée par une telle équation. Il pouvait donc espérer pouvoir étendre cet algorithme à des séries et l'appliquer au problème de l'expression de l'aire de l'hyperbole. Mais pour le faire, il devait d'abord transformer l'équation $y = \frac{1}{x}$ en une équation de la forme « $y = \sum_{i=0}^{n} A_i x^{q_i}$ ». Or, en posant $x = 1 + z$, cette équation devient : $y = \frac{1}{1+z} = (1+z)^{-1}$. S'il avait été possible de développer la puissance $(1+z)^{-1}$ dans une série ne contenant que des puissances de $z$, le problème aurait été résolu. Pour des raisons analogues, qu'il serait ici trop difficile de détailler, le développement en série de toute puissance telle que $(1+x)^{\frac{p}{q}}$ aurait aussi permis à Newton d'appliquer son algorithme à la recherche de l'expression de l'aire d'autres courbes qu'il était pour lui important d'exprimer. Ainsi, le problème de l'association

d'une série, ne contenant que des puissances de $x$, à une puissance telle que $(1+x)^{\frac{p}{q}}$ se présentait à Newton comme un problème fondamental.

La manière dont Newton résolut ce problème, en parvenant à déterminer la forme générale des coefficients binomiaux pour des exposants rationnels quelconques (et donc, du même coup, celle des coefficients binomiaux pour des exposants naturels), ne peut pas être reconstruite ici avec précision. Je dirais seulement qu'il raisonna sur le triangle de Pascal, en cherchant en même temps à étendre à gauche la matrice qui correspond à ce triangle et à l'interpoler en introduisant, entre deux colonnes successives, un nombre arbitraire de colonnes intermédiaires. Il parvint finalement à son but vers la fin de l'été 1665 et il énonça son résultat fondamental, donnant la formule d'interpolation du triangle de Pascal, et donc la forme de tout coefficient binomial pour un exposant rationnel quelconque, dans la quatrième proposition d'un traité consacré à la quadrature des courbes, qu'il laissa pourtant à l'état d'esquisse. À partir de cette date, Newton n'oublia jamais plus ce résultat, qui au contraire l'accompagna constamment dans son effort d'édification d'une mathématique nouvelle.

**Lectures possibles** : D. T. Whiteside (ed. by) *The Mathematical Papers of Isaac Newton*, Cambridge Univ. Press, Cambridge, 1967-1981 (8 vols.), vol. I ; M. Panza, Newton el les origines de l'analyse˜ :1664-1666, Blancherd, Paris, 2004.

### 3. Conditions de mesure des segments

Après avoir introduit les notions de suite et de série et avoir spécifié ce que signifie qu'une suite ou une série convergent vers une (certaine) limite dans un (certain) ensemble, revenons à nos segments $\mathsf{MN}$ et $\mathsf{PQ}$ et supposons qu'ils soient incommensurables entre eux. Il n'y aura donc pas de nombre naturel $\nu$ qui vérifie (59) et (60). Malgré cela, il est facile de montrer que la différence

$$\mathsf{MN} - \sum_{i=0}^{\nu} n_i(\mathsf{PQ}_i) = \mathsf{MN} - \left[ n_\nu + \sum_{i=0}^{\nu-1} n_i \left( \prod_{j=i+1}^{\nu} m_j \right) \right] (\mathsf{PQ}_\nu)$$

qu'on pourra noter « $R_\nu$ », diminue à mesure que le nombre $\nu$ croît en s'approchant de plus en plus au segment nul. Pour prouver ceci, on peut raisonner comme il suit.

Au bout de $\mu+1$ étapes dans notre procédure, on sera parvenu à l'inégalité suivante :

$$n_\mu(\mathsf{PQ}_\mu) < \mathsf{MN} - \sum_{i=0}^{\mu-1} n_i(\mathsf{PQ}_i) < (n_\mu+1)(\mathsf{PQ}_\mu)$$

ou bien

$$n_\mu(\mathsf{PQ}_\mu) < \mathsf{MN} - \left[ \sum_{i=0}^{\mu-1} n_i \left( \prod_{j=i+1}^{\mu} m_j \right) \right] (\mathsf{PQ}_\mu) < (n_\mu+1)(\mathsf{PQ}_\mu)$$

et on aura ainsi

$$R_\mu = \mathsf{MN} - \sum_{i=0}^{\mu-1} n_i(\mathsf{PQ}_i) - n_\mu(\mathsf{PQ}_\mu) = \mathsf{MN} - \sum_{i=0}^{\mu} n_i(\mathsf{PQ}_i) \tag{85}$$

$$= \mathsf{MN} - \left[ n_\mu + \sum_{i=0}^{\mu-1} n_i \left( \prod_{j=i+1}^{\mu} m_j \right) \right] (\mathsf{PQ}_\mu) \neq \overline{0} \tag{86}$$

où le symbole « $\overline{0}$ » indique le segment nul. Pour continuer dans la procédure de mesure, on devra alors choisir un nombre naturel $m_{\mu+1}$ plus grand que 1 et une partie $\mathsf{PQ}_{\mu+1}$ de $\mathsf{PQ}_{\mu}$ (et donc de $\mathsf{PQ}$) telle que $\mathsf{PQ}_{\mu} = m_{\mu+1}(\mathsf{PQ}_{\mu+1})$, et déterminer, en fonction de ce choix, un nombre naturel $n_{\mu+1}$ tel que

$$n_{\mu+1}(\mathsf{PQ}_{\mu+1}) < R_{\mu} < (n_{\mu+1}+1)(\mathsf{PQ}_{\mu+1})$$

Ce nombre $m_{\mu+1}$ ayant été fixé, il est clair que

$$\overline{0} < R_{\mu} - n_{\mu+1}(\mathsf{PQ}_{\mu+1}) < \mathsf{PQ}_{\mu+1}$$

ou bien

$$\overline{0} < R_{\mu} - n_{\mu+1}\frac{\mathsf{PQ}}{\prod_{j=1}^{\mu+1} m_j} < \frac{\mathsf{PQ}}{\prod_{j=1}^{\mu+1} m_j} \tag{87}$$

Or, comme, quel que soit le nombre naturel $\mu$, les termes $m_j$ ($j = 1, 2, \ldots, \mu + 1$) sont tous des nombres naturels plus grands que 1, il s'ensuit que

$$\left\{ \frac{1}{\prod_{j=1}^{\nu+1} m_j} \right\}_{\nu=0}^{\infty}$$

est une suite à termes dans $\mathbb{Q}^+$ qui converge vers 0 dans $\mathbb{Q}^+$, c'est-à-dire que :

*i*) tous les termes

$$\frac{1}{\prod_{j=1}^{\nu+1} m_j}$$

et donc toutes les valeurs de la distance

$$\left| 0 - \frac{1}{\prod_{j=1}^{\nu+1} m_j} \right|$$

($\nu = 0, 1, 2, ...$), appartiennent à $\mathbb{Q}^+$ (c'est-à-dire qu'ils sont des nombres rationnels positifs) ;

*ii*) pour tout $\varepsilon > 0$ appartenant à $\mathbb{Q}^+$, il y a un nombre naturel $N$, tel que si $\nu > N$, alors

$$\left| 0 - \frac{1}{\prod_{j=1}^{\nu+1} m_j} \right| < \varepsilon$$

La preuve de $(i)$ résulte d'une induction complète fort simple, car si $\nu = 0$, alors

$$\frac{1}{\prod_{j=1}^{\nu+1} m_j} = \frac{1}{m_1} \in \mathbb{Q}^+$$

et si $s$ est un nombre naturel quelconque plus grand que 0, et

$$\frac{1}{\prod_{j=1}^{s+1} m_j} \in \mathbb{Q}^+$$

alors

$$\frac{1}{\prod\limits_{j=1}^{s'+1} m_j} = \frac{1}{\prod\limits_{j=1}^{s+1} m_j} \cdot \frac{1}{m_{s+2}} \in \mathbb{Q}^+$$

($\mathbb{Q}^+$ étant, comme on l'a vu, fermé par rapport à la multiplication).

La preuve de $(ii)$ n'est pas plus difficile. D'abord on observe que, pour tout $\nu$ naturel

$$\left| 0 - \frac{1}{\prod\limits_{j=1}^{\nu+1} m_j} \right| = \frac{1}{\prod\limits_{j=1}^{\nu+1} m_j}$$

et que, $\varepsilon$ étant un nombre rationnel strictement positif, il y a deux nombres naturels $\lambda$ et $\eta$, différents de 0, tels que $\varepsilon = \frac{\lambda}{\eta}$. Ensuite, on considère le produit $\prod\limits_{j=1}^{\nu+1} m_j$ et on remarque que, les termes $m_j$ $(j = 1, 2, ..., \nu)$ étant des nombres naturels plus grands que 1, ce produit satisfait sûrement à la condition $\prod\limits_{j=1}^{\nu+1} m_j \geq 2^{\nu+1} \geq 2\nu$. De là on peut enfin conclure qu'il suffit de poser $\nu = \lambda \cdot \eta$, pour avoir

$$\left| 0 - \frac{1}{\prod\limits_{j=1}^{\nu+1} m_j} \right| = \frac{1}{\prod\limits_{j=1}^{\nu+1} m_j} \leq \frac{1}{2\lambda\eta} < \frac{\lambda}{\eta} = \varepsilon$$

ce qui conclut la preuve.

Comme, quel que soit le segment $\mathsf{PQ}$, $0 \cdot (\mathsf{PQ}) = \overline{0}$, de là il suit que le segment

$$\mathsf{PQ}_{\nu+1} = \frac{\mathsf{PQ}}{\prod\limits_{j=1}^{\nu+1} m_j}$$

s'approche de plus en plus du segment nul à mesure que $\nu + 1$ (et donc $\nu$) croît et (87) nous fait comprendre que ceci est aussi le cas du segment $R_\nu$, c'est-à-dire que la suite des segments $\{R_\nu\}_{v=0}^{\infty}$ converge vers le segment nul dans l'ensemble $E$ de tous les segments, nuls ou non nuls.

Or, de (85), il suit que

$$\begin{aligned} R_\nu &= \mathsf{MN} - \sum_{i=0}^{\nu} n_i(\mathsf{PQ}_i) \\ &= \mathsf{MN} - \sum_{i=0}^{\nu} n_i \frac{\mathsf{PQ}}{\prod\limits_{j=1}^{i} m_j} \\ &= \mathsf{MN} - \left[ \sum_{i=0}^{\nu} \frac{n_i}{\prod\limits_{j=1}^{i} m_j} \right] \mathsf{PQ} \end{aligned}$$

(où on aura posé, comme tout à l'heure, $m_0 = 1$), et de là il est facile de conclure que, pour tout $\nu$,

$$\mathsf{MN} = \left[ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right] \mathsf{PQ} + R_\nu \tag{88}$$

Donc, si $\mathsf{MN}$ et $\mathsf{PQ}$ sont des segments incommensurables, alors il n'y a aucun nombre naturel $\nu$, tel que $R_\nu = \overline{0}$, bien que la somme des segments

$$\sum_{i=0}^{\nu} n_i \left(\mathsf{PQ}_i\right) = \left[ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right] \mathsf{PQ}$$

(avec $m_0 = 1$) s'approche de plus en plus de $\mathsf{MN}$, et donc le nombre rationnel positif

$$\left[ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right]$$

(avec $m_0 = 1$), s'approche de plus en plus de la mesure de $\mathsf{MN}$, relativement à l'unité de mesure $\mathsf{PQ}$, lorsque $\nu$ croît.

Comment comprendre cette affirmation ? Choisissons un nombre naturel $\nu$ quelconque. De (88), il suit que

$$\mathsf{MN} - R_\nu = \left[ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right] \mathsf{PQ}$$

(avec $m_0 = 1$). Donc, si on décide de s'arrêter après $\nu + 1$ étapes et d'assigner au segment $\mathsf{MN}$ la mesure donnée par la somme

$$\sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

alors on devra assigner la même mesure à tous les segments $\mathsf{MN}_\nu$, tels que

$$\mathsf{MN} - R_\nu \leq \mathsf{MN}_\nu \leq \mathsf{MN} + \mathsf{PQ}_\nu$$

Il est alors clair que notre conclusion revient à affirmer qu'au fur et à mesure que $\nu$ croît, la classe des segments auxquels on doit assigner la même mesure, si on s'arrête dans notre procédure au bout de $\nu + 1$ étapes, ne contient que des segments qui sont de plus en plus proches de $\mathsf{MN}$. L'erreur qu'on peut commettre en prenant pour $\mathsf{MN}$ un segment quelconque de cette classe est donc de plus en plus négligeable.

Imaginons maintenant que la série

$$\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

($m_0 = 1$) converge vers une certaine limite dans $\mathbb{Q}^+$. Cela signifierait (conformément à la définition 2.3) qu'il y aurait un nombre rationnel strictement positif $U = \frac{h}{k}$ ($h$ et $k$ étant des nombres naturels différents de 0), tel que la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

(avec $m_0 = 1$) converge vers $U$ dans $\mathbb{Q}^+$. Alors, quels que soient les nombres naturels différents de zéro $\lambda$ et $\eta$, le nombre rationnel strictement positif $\frac{\lambda}{\eta}$ devrait être tel qu'on pourrait toujours trouver un nombre naturel positif $N$, tel que si $\nu = N + 1$, alors

$$\left| \frac{h}{k} - \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right| = \left| \frac{h}{k} - \sum_{i=0}^{N+1} \frac{n_i}{\prod_{j=1}^{i} m_j} \right| < \frac{\lambda}{\eta} \tag{89}$$

Or, comme les nombres $n_i$ et $m_j$ ($i = 0, 1, ..., \nu\,; j = 0, 1, 2, ..., i$) sont tous naturels, les termes de la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

croissent avec $\nu$, et en particulier sont tels que pour tout $\nu$,

$$\sum_{i=0}^{\nu+1} \frac{n_i}{\prod_{j=1}^{i} m_j} - \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \geq 0$$

Donc, pour tout $\nu$, $\frac{h}{k}$ ne peut être plus petit que

$$\sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

et par conséquent

$$\left| \frac{h}{k} - \sum_{i=0}^{N+1} \frac{n_i}{\prod_{j=1}^{i} m_j} \right| = \frac{h}{k} - \sum_{i=0}^{N+1} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

L'inégalité (89) est donc équivalente à la suivante :

$$\frac{h}{k} - \sum_{i=0}^{N+1} \frac{n_i}{\prod_{j=1}^{i} m_j} < \frac{\lambda}{\eta}$$

On devrait en conclure, conformément à (88), que, aussi petit que l'on prenne le nombre rationnel positif $\frac{\lambda}{\eta}$, on pourrait trouver une valeur $N+1$ de $\nu$ telle que

$$\mathsf{MN} - R_{N+1} > \left(\frac{h}{k} - \frac{\lambda}{\eta}\right)(\mathsf{PQ})$$

Mais on a déjà vu que la suite de segments $\{R_\nu\}_{\nu=0}^{\infty}$ converge vers le segment nul dans l'ensemble $E$ de tous les segments et donc cela ne pourrait être le cas qu'à condition que

$$\mathsf{MN} = \frac{h}{k}(\mathsf{PQ})$$

ce qu'on sait être impossible, car $\mathsf{MN}$ et $\mathsf{PQ}$ sont deux segments qu'on a supposé être incommensurables.

On a donc démontré par l'absurde (sans utiliser le tiers exclu) que, si $\mathsf{MN}$ et $\mathsf{PQ}$ sont deux segments incommensurables, la série

$$\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

ne peut pas être convergente vers une certaine limite dans $\mathbb{Q}^+$. D'autre part, quelle que soit la valeur de $\nu$, le segment résultant de l'addition

$$\sum_{i=0}^{\nu} n_i\,(\mathsf{PQ}_i) = \left[\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}\right](\mathsf{PQ})$$

ne peut jamais être plus grand que $\mathsf{MN}$, car de (88) il suivrait alors, en posant

$$\left[\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}\right](\mathsf{PQ}) = \mathsf{MN} + K$$

($K$ étant un segment non nul),

$$\mathsf{MN} - R_\nu = \mathsf{MN} + K$$

ce qui est impossible, car $R_\nu$ ne peut pas prendre des valeurs négatives.

Il s'ensuit que la suite

$$\left\{\sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j}\right\}_{\nu=0}^{\infty}$$

et donc la série

$$\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

(avec $m_0 = 1$) ne convergent pas vers une limite dans $\mathbb{Q}^+$, c'est-à-dire qu'il n'y a aucun nombre rationnel positif qui puisse être traité comme la limite de cette suite et de cette série, bien que

les termes de la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

ne puissent pas prendre dans $\mathbb{Q}^+$ des valeurs aussi grandes qu'on veut, et en particulier qu'ils ne puissent prendre aucune valeur rationnelle $V$, telle que

$$\mathsf{MN} \leq V\,(\mathsf{PQ})$$

La suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

ne converge donc pas vers une limite dans $\mathbb{Q}^+$, bien qu'elle soit croissante et supérieurement bornée dans $\mathbb{Q}^+$ (on dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ est « croissante », s'il y a un nombre naturel $n$, tel que $i > n \Rightarrow u_{i+1} > u_i$ et on dit qu'elle est « supérieurement bornée dans $E$ » dans un ensemble si tous les termes $u_i$ $(i = 0, 1, 2, ...)$ de cette suite appartiennent à $E$ et s'il y a un élément $\Lambda$ de $E$, tel que, quel que soit $i$, $u_i \leq \Lambda$ ; on reviendra plus loin sur cette dernière définition avec plus de précision).

Tout se passe donc comme si les termes successifs de cette suite, qui appartiennent tous à $\mathbb{Q}^+$, allaient s'accumuler autour de quelque chose comme un trou dans $\mathbb{Q}^+$, une valeur qui n'est pas dans $\mathbb{Q}^+$, mais peut être approchée autant qu'on veut par des éléments de $\mathbb{Q}^+$.

Remarque 6.12. Lorsqu'on dit d'une suite à termes dans un certain ensemble $E$ qu'elle est divergente dans $E$, on pense immédiatement que ses termes se distribuent sur $E$ d'une manière telle que leur distance ne tend pas à s'amenuiser, c'est-à-dire qu'ils ne tendent pas à s'accumuler l'un sur l'autre, ou, pour le dire d'une troisième manière encore, qu'ils ne sont pas attirés vers un centre. Lorsque les termes d'une suite à termes dans $E$ se comportent ainsi, alors cette suite est sans doute divergente dans $E$. Le long argument précédent nous montre pourtant qu'il est possible qu'une suite à termes dans $E$ diverge dans $E$, même si ses termes se distribuent sur $E$ d'une manière telle que leur distance tend à s'amenuiser, c'est-à-dire qu'ils tendent à s'accumuler l'un sur l'autre, ou, si on préfère, sont attirés vers un centre. Cela se passe, tout simplement, lorsque ce centre est, dans un sens, de plus en plus approché par des éléments de $E$, sans pour autant appartenir à $E$. En parlant fort informellement, on pourra donc dire qu'il y a deux sortes de raisons pour lesquelles une suite à termes dans $E$ est divergente dans $E$ : la première raison tient, pour ainsi dire, à la suite elle-même, et dépend du fait que cette suite n'obéit à aucune loi d'accumulation ; la deuxième raison tient par contre à l'ensemble $E$ et dépend du fait que cet ensemble n'est pas, pour ainsi dire, assez plein, présente des lacunes, ne contient pas le point d'accumulation de toutes les séries qui obéissent à une loi d'accumulation, dont les termes lui appartiennent, en un seul mot, qu'il n'est pas continu. Dans le prochain paragraphe, on reviendra plus en détails sur cette deuxième possibilité, en ne considérant pourtant que des suites à termes dans $\mathbb{Q}$.

La situation qu'on vient de décrire suggère d'ajouter à $\mathbb{Q}^+$ un nouvel élément $\alpha_{\mathsf{MN}}$ et une infinité d'autres éléments

$$\beta_{\nu,\mathsf{MN}} = \left| \alpha_{\mathsf{MN}} - \sum_{i=0}^{\nu} \frac{n_i}{\prod\limits_{j=1}^{i} m_j} \right| = \alpha_{\mathsf{MN}} - \sum_{i=0}^{\nu} \frac{n_i}{\prod\limits_{j=1}^{i} m_j}$$

($\nu = 0, 1, 2, ...$), de façon à construire un nouvel ensemble $\mathbb{Q}^+ \cup \Omega_{\mathsf{MN}}$ tel que la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod\limits_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

et donc la série

$$\sum_{i=0}^{\infty} \frac{n_i}{\prod\limits_{j=1}^{i} m_j}$$

(avec $m_0 = 1$) soient convergentes vers $\alpha_{\mathsf{MN}}$ dans $\mathbb{Q}^+ \cup \Omega_{\mathsf{MN}}$ . Ceci fait, on pourra affirmer, tout naturellement, que le segment $\mathsf{MN}$ a une mesure dans $\mathbb{Q}^+ \cup \Omega_{\mathsf{MN}}$ relativement à l'unité de mesure $\mathsf{PQ}$ et écrire l'égalité :

$$\mathsf{MN} = \left( \sum_{i=0}^{\infty} \frac{n_i}{\prod\limits_{j=1}^{i} m_j} \right) (\mathsf{PQ}) = \alpha_{\mathsf{MN}} (\mathsf{PQ})$$

ou, si on prend $\mathsf{PQ}$ comme une unité de mesure universelle :

$$\mathsf{MN} = \sum_{i=0}^{\infty} \frac{n_i}{\prod\limits_{j=1}^{i} m_j} = \alpha_{\mathsf{MN}}$$

## 4. L'ensemble des nombres réels

Dans le paragraphe 1, on a montré que, quelle que soit l'unité de mesure choisie, il n'est pas possible d'assigner à tout segment un nombre rationnel positif, exprimant la mesure de ce segment en termes de cette unité de mesure, de manière que le même nombre rationnel positif soit assigné à deux segments $H$ et $K$ si et seulement si $H = K$. Dans le paragraphe 3, on a ensuite montré que si $H$ est un segment incommensurable avec l'unité de mesure choisie, on peut du moins construire une suite de nombres rationnels positifs, telle que ses termes expriment, en termes de cette unité de mesure, la mesure de segments de plus en plus proches de $H$. On a donc terminé en proposant d'élargir l'ensemble $\mathbb{Q}^+$ de manière à construire un nouvel ensemble contenant un élément qui exprime (exactement) la mesure de $H$ en termes de l'unité de mesure choisie. Si l'on répéte la même opération pour tout segment incommensurable avec cette unité de mesure, on obtient ainsi un nouvel ensemble tel que, quel que soit le segment $K$, il est possible de lui associer un élément de cet ensemble qui exprime (exactement) la mesure de ce segment en termes d'une telle unité de mesure. Il y aura donc dans cet ensemble au moins autant d'éléments distincts qu'il y a de segments différents. Cela signifie que si on considère une droite quelconque, et l'on fixe un point sur cette droite, alors le nouvel ensemble qu'on construit de

cette manière contiendra au moins autant d'éléments distincts qu'on peut tracer de segments différents sur la droite donnée, à partir du point fixé et dans une direction choisie. Comme chacun de ces segments est caractérisé de manière univoque par ses extrémités, et qu'une de ces extrémités est fixée, cela signifie que dans le nouvel ensemble il y aura au moins autant d'éléments que sur une demi-droite il y a de points (qu'on peut traiter comme des extrémités d'un segment gisant sur cette demi-droite). Si on assigne, de surcroît, à chaque élément de cet ensemble, un élément inverse par rapport à l'addition, on obtient un autre ensemble qui contient au moins autant d'éléments qu'on peut tracer de segments sur la droite donnée, à partir du point fixé et dans n'importe quelle direction. Ce nouvel ensemble contiendra donc au moins autant d'éléments que sur une droite il y a de points (qu'on peut traiter comme des extrémités d'un segment gisant sur cette droite).

Jusqu'ici, l'opération d'extension de $\mathbb{Q}^+$ qui permet de parvenir à la construction d'un tel ensemble n'a été pourtant qu'évoquée de manière très vague et informelle. Il s'agit donc de montrer, avec plus de précision, comment une telle extension de $\mathbb{Q}^+$ peut être obtenue. Et en particulier, il faut montrer que, si on opère convenablement, il est possible d'obtenir une extension de $\mathbb{Q}^+$ qui contienne exactement autant d'éléments que sur une droite il y a de points (qu'on puisse traiter comme des extrémités d'un segment gisant sur cette droite), et qui est telle que ces éléments se comportent les uns par rapport aux autres comme ces points semblent se comporter les uns par rapport aux autres (cette construction étant parfaitement indépendante de l'unité de mesure choisie au départ, qui peut, tout simplement, être identifiée avec le segment unitaire, auquel est associé d'emblée le nombre rationnel positif 1). Comme une droite est l'archétype reconnu de la continuité, l'ensemble qu'on construira de cette manière pourra être pensé comme un ensemble continu, ou même comme une objectivation mathématique de la notion de continuité, c'est-à-dire comme « le continue ». Cet ensemble, qu'on note par le symbole « $\mathbb{R}$ » est appelé « ensemble des nombres réels » et ses éléments sont donc dits « nombres réels ».

Si on veut identifier cet ensemble, il n'est pourtant pas nécessaire de le construire explicitement à partir de $\mathbb{Q}^+$. On peut aussi le caractériser comme un ensemble qui satisfait à certains axiomes. On aura alors une caractérisation de $\mathbb{R}$ analogue à celle que les axiomes de Peano fournissent pour $\mathbb{N}$, et à celle qu'il est possible d'obtenir, comme on l'a montré à la fin du chapitre 4, pour $\mathbb{Q}$. Dans la suite du présent paragraphe, on montera comment $\mathbb{R}$ peut être identifié autant d'une manière que de l'autre : on commencera par construire $\mathbb{R}$ explicitement à partir de $\mathbb{Q}^+$, et on le reconnaîtra ensuite comme un ensemble qui satisfait à un certain système d'axiomes.

Remarque 6.13. De ce qu'on vient de dire, il devrait résulter clairement que, quelle que soit la définition qu'on choisit pour l'ensemble des nombres réel, cette définition n'est pas arbitraire, mais résulte de l'effort de fournir une structure qui satisfasse à deux exigences : d'abord, cette structure doit être telle qu'il est possible de se réclamer des éléments de l'ensemble qui la compose pour mesurer de manière exacte chaque segment, en termes de n'importe quelle unité de mesure, c'est-à-dire que cet ensemble doit pouvoir être mis en bijection avec l'ensemble de segments qu'on peut tracer sur une droite, à partir d'une extrémité fixée ; ensuite, elle doit satisfaire à des conditions qui la rendent apte à exprimer la forme ou la propriété que nous assignons à une droite, lorsque nous disons qu'elle est continue (on peut imaginer, à première vue, que ces deux exigences coïncident ; on montrera pourtant, vers la fin du présent chapitre, qu'il est possible de satisfaire à la première, sans pour autant satisfaire à la deuxième). Encore une fois, l'effort de formalisation accompli par les mathématiciens est guidé par un but, et ce but est celui de représenter (et donc de comprendre) un phénomène préalable.

Le but de comprendre, décrire et représenter la nature profonde de la continuité, que ce soit celle d'une droite, d'un mouvement ou d'une pensée, date des origines mêmes de notre culture. Il constitue déjà une des visées fondamentales de la *Physique* d'Aristote. Dans ce texte, Aristote donne deux définitions distinctes de la continuité qu'il semble prendre comme équivalentes. La deuxième de ces définitions identifie la continuité avec la divisibilité à l'infini : un segment serait continu car on peut indéfiniment le diviser. Cette définition sera, beaucoup plus tard, reprise par Kant dans la première *Critique*. Aujourd'hui, on pense pourtant qu'elle est inacceptable, car la divisibilité à l'infini s'identifie à la densité par rapport à $\leq$, et cette dernière est déjà, comme on l'a vu, une propriété de l'ensemble $\mathbb{Q}$ des nombres rationnels, qui, manifestement, ne peut pas être pensé, à cause de l'argument avancé dans le paragraphe 1, comme une expression convenable de la continuité d'une droite. La première des définitions d'Aristote (d'après laquelle un continu est ce dont les parties sont telles que leurs extrémités s'identifient) semble en revanche, pour beaucoup de raisons qu'on ne peut pas développer ici, plus proche de la caractérisation moderne, d'après laquelle l'ensemble $\mathbb{R}$ des nombres réels s'identifie avec le continu.

Il y a pourtant des philosophes, et aussi des mathématiciens, qui pensent que la définition d'Aristote révèle un trait profond de la propriété de la continuité qui n'est pas saisi par cette caractérisation. En suivant Pierce, ces philosophes nient que l'ensemble des nombres réels peut être mis en bijection avec les composants ultimes d'une droite, où même qu'une droite puisse être pensée comme un objet composé (tel qu'est en revanche un ensemble). Si on identifie les composants ultimes d'une droite avec des points, affirmer que l'ensemble des nombres réels ne peut être mis en bijection avec ces composants ultimes, semble équivaloir à affirmer que les définitions habituelles de l'ensemble des nombres réels (et donc, entre autres, celles qu'on présentera par la suite) ne réalisent pas le premier but auquel elles tendent, celui de caractériser un ensemble qui puisse être mis en bijection avec l'ensemble des segments qu'on peut tracer sur une droite, à partir d'un point donné. Aucun philosophe sérieux, et encore moins aucun mathématicien, ne peut pourtant nier que l'ensemble des nombres réels peut être mis en bijection avec l'ensemble des segments qu'on peut tracer sur une droite à partir d'un point donné. Ceci est en effet l'objet d'une preuve qui apparaît comme irrécusable. D'où vient alors qu'on puisse nier (sans contredire un théorème mathématique bien établi, et en se comportant donc en philosophes et mathématiciens sérieux) que l'ensemble des nombres réels puisse être mis en bijection avec les composants ultimes d'une droite. La réponse est simple : on peut nier que la droite géométrique est composée par les extrémités non géométriquement superposées de tous les segments géométriquement différents qu'on peut prendre sur elle. Ceci semble avoir été l'opinion de Pierce, et semble être aujourd'hui l'opinion des mathématiciens qui pensent que l'ensemble des nombres réels, tel qu'il est habituellement défini, n'est pas une bonne objectivation de la propriété de continuité d'une droite. C'est pourquoi j'ai ci-dessus précisé que l'ensemble des points d'une droite qui peuvent être mis en bijection avec l'ensemble des nombres réels est l'ensemble des points de cette droite qu'on peut traiter comme des extrémités d'un segment gisant sur celle-ci.

Note Historique 6.10. Dans la troisième de ses *Cambridge Conferences* (cf. la note historique 2.3), Peirce qualifie de continue une « collection » qui a la même « multitude » que la collection de toutes les collections possibles de ses éléments. Pour donner un sens à l'argument par lequel Peirce parvient à cette définition, il ne semble guère nécessaire de définir positivement les notions de collection et multitude. Il suffit de savoir ce que signifie que la multitude d'une collection d'individus distincts — disons, par simplicité, bien que le terme ne soit pas de Peirce, « la multitude d'un ensemble » — est la même que celle d'un autre ensemble, ou, le cas échéant, ce que

signifie qu'elle est plus grande ou plus petite que celle-ci. C'est ce que le lecteur peut aisément déduire du déroulement de l'argumentation : deux ensembles ont la même multitude si et seulement si les individus qui les composent sont entre eux en correspondance biunivoque ; un de ces ensembles a en revanche une multitude plus grande que l'autre si les individus de ce dernier sont en correspondance biunivoque avec les individus d'une partie propre du premier.

On comprendra alors que, pour l'essentiel, la notion de multitude d'un ensemble utilisée par Peirce correspond à notre notion de cardinalité d'un ensemble et celle d'individus d'un ensemble à notre notion d'éléments d'un ensemble. On continuera donc à exposer l'argument de Peirce en se ralliant à l'usage courant et en parlant de cardinalité, plutôt que de multitude, et d'éléments plutôt que d'individus.

Parmi les ensembles, nous dit Peirce, certains sont finis (cf. encore la note historique 2.3). L'ensemble composé par toutes les classes d'équivalences possibles composées par des ensembles finis de même cardinalité (qui a évidemment, dans les termes de Peirce, la même multitude dque l'ensemble des nombres naturels) a ensuite une cardinalité plus grande que n'importe quel ensemble fini. Notons, comme d'habitude, la cardinalité de cet ensemble par le symbole « $\aleph_0$ » (où « $\aleph$ » est la première lettre de l'alphabet hébreu, et se lit « aleph » ). Comme tout ensemble fini a une cardinalité plus petite que cet ensemble, et comme aucun ensemble infini ne peut avoir, à son tour, une cardinalité plus petite, il s'ensuit que la cardinalité de cet ensemble est la plus petite parmi toutes les cardinalité d'ensembles infinis. En acceptant celle que nous reconnaissons aujourd'hui comme l'hypothèse du contin (qui affirme qu'il n'y a pas d'ensembles dont la cardinalité est plus grande que $\aleph_0$ et plus petite que la cardinalité, généralement notée « $2^{\aleph_0}$ », de l'ensemble de tous les sous- ensembles possibles d'un ensemble de cardinalité $\aleph_0$), Peirce suppose ensuite que la cardinalité immédiatement supérieure est celle de l'ensemble de tous les sous-ensembles possibles d'un ensemble de cardinalité $\aleph_0$. On pourra indiquer un ensemble comme celui-ci par le symbole « $\mathbf{P}(\mathbb{N})$ ». En continuant de la même manière, et en acceptant implicitement l'hypothèse généralisée du continu (cf. la fin du paragraphe 4), on aura une progression d'ensembles qu'on pourra noter par $\mathbf{P}^2(\mathbb{N})$, $\mathbf{P}^3(\mathbb{N})$, $\mathbf{P}^4(\mathbb{N})$, ... Il suffit alors à Peirce de démontrer qu'aucun ensemble ne peut avoir la même cardinalité que l'ensemble de tous ses sous-ensembles possibles, pour transformer cette progression d'ensembles en une progression de cardinalités. Ceci étant dit, laissons la parole à Peirce lui-même :

« Considérons [...] une collection contenant un individu pour tout individu d'une collection de collections comprenant une collection de toute multitude non dénombrable. C'est-à-dire que cette collection se composera de toutes les multitudes finies ainsi que de toutes les collections possibles de ces multitudes, ainsi que de toutes les collections possibles de collections de ces multitudes et de toutes les collections possibles de collections de collections de ces multitudes, et ainsi de suite *à l'infini*. Cette collection est évidemment de multitude aussi grande que celle de toutes les collections possibles de ces éléments. Mais nous venons de voir que ceci ne peut être vrai de toute collection dont les individus sont distincts des autres [Peirce énonce ce résultat un peu en amont dans sa conférence]. En conséquence nous constatons que nous avons maintenant atteint une multitude tellement grande que les individus d'une telle collection se fondent les uns dans les autres et perdent leurs identités distinctes. Une telle collection est *continue* ».

Considérons d'abord la deuxième des deux caractérisations de ce que Peirce appelle une « collection continue », celle qui intervient dans le passage cité après l'adverbe « c'est-à-dire ». La manière la plus naturelle pour nous de représenter l'objet qui correspond à cette description est de le représenter comme l'union infinie $\bigcup_{i=0}^{\infty}\mathbf{P}^i(\mathbb{N})$, où l'indice $i$ varie sur l'ensemble $\mathbb{N}$ des naturels. Pourtant, si on adopte cette représentation, la deuxième caractérisation de ce que Peirce appelle une « collection continue » n'est équivalente à la première (celle qui précède l'adverbe « c'est-à-dire » ) qu'à la condition de n'accepter comme cardinaux que les cardinaux des ensembles $\mathbf{P}^i(\mathbb{N})$, où $i$ est justement un nombre naturel quelconque, c'est-à-dire de ne considérer parmi les cardinalités (ou multitudes) possibles que celles des ensembles $\mathbf{P}^i(\mathbb{N})$, où l'indice $i$ varie justement sur l'ensemble $\mathbb{N}$ des naturels. Mais si, pour ainsi dire, au-delà des naturels, on imagine des nombres cardinaux infinis (ou, comme on dit généralement « transfinis » ) tels que ceux qui indiquent les cardinalités successives des ensembles infinis, à commencer par $\aleph_0$, et qu'on donne à l'indice $i$, dans le symbole « $\mathbf{P}^i\ (\mathbb{N})$ », des valeurs correspondant à ces nombres, alors les deux caractérisations d'une « collection continue » proposées par Peirce ne sont évidemment plus équivalentes.

Or, si on imagine que dans la théorie des ensembles de Peirce, il n'y a pas de cardinaux au-delà des $\omega_i$ = card. $(\mathbf{P}^i(\mathbb{N}))$, alors l'union $\bigcup_{i=0}^{\infty}\mathbf{P}^i(\mathbb{N})$ est effectivement, comme Peirce le veut, une « classe propre » dans cette théorie (c'est-à-dire une classe « trop grande » pour être un ensemble). La raison est qu'on ne dispose pas de cardinaux suffisants pour compter parmi les sous-ensembles de $\bigcup_{i=0}^{\infty}\mathbf{P}^i(\mathbb{N})$ ceux qui sont composés par l'union de n'importe quels sous- ensembles de n'importe quel ensemble $\mathbf{P}^i(\mathbb{N})$. Alors $\bigcup_{i=0}^{\infty}\mathbf{P}^i(\mathbb{N}\ )$ correspond bien, comme Peirce le prétend, à la collection de tous ses sous-ensembles possibles et elle n'est pas un ensemble. Cependant une telle théorie des ensembles n'est pas seulement très difficilement formalisable, mais elle est aussi fort peu plausible, car il paraît étrange de ne pas imaginer que la succession des cardinaux aille au-delà des cardinaux des ensembles $\mathbf{P}^i(\mathbb{N})$ ($i$ étant un nombre naturel), une fois qu'on a accepté d'aller au-delà du dénombrable dans la hiérarchie des ensembles. Or, si on accepte des cardinaux de toutes sortes d'infinités, la situation change, et il n'est plus possible d'affirmer que l'union $\bigcup_{i=0}^{\infty}\mathbf{P}^i(\mathbb{N})$ n'est pas un ensemble, car sa cardinalité est alors strictement inférieure à celle de l'ensemble de tous ses sous-ensembles. Pour construire une classe propre nous devons continuer l'itération de Peirce au-delà de l'infini dénombrable, en réalisant une *induction transfinie*.

Il est difficile de dire laquelle parmi ces deux possibilités est celle envisagée par Peirce (à une époque où la formalisation moderne de la théorie des ensembles était loin d'être disponible) et même d'exclure que Peirce ait ici simplement commis une erreur. Une chose est pourtant claire, et c'est ce qui nous intéresse ici le plus : pour Peirce un continu, est une collection qui n'est pas une collection d'individus distincts, une classe qui ne peut pas être pensée comme un ensemble ; en termes modernes, une classe propre ; ce qu'il appelle « collection continue » n'est donc pas un ensemble.

Peirce n'a aucune hésitation à propos de la légitimité d'un tel objet. Il prétend même qu'une circonférence est un exemple de collection continue, car elle est décrite par le mouvement d'une particule et se compose donc « des points que cette particule a occupés » pendant le temps de son mouvement, bien qu' « aucun point de cette ligne ne se différencie absolument, quant à son identité, de tout autre ».

Voici un argument qui contredit l'isomorphisme couramment établi entre les points qui composent une ligne géométrique et l'ensemble des nombres réels (dont la cardinalité n'est autre, comme on le verra, que celle de $\mathbf{P}(\mathbb{N})$). Or, Peirce avait lui-même affirmé cet isomorphisme en 1892 (dans l'article « The Law of Mind », déjà cité dans la note historique 2.3) et il ne pouvait pas en méconnaître ou rejeter la preuve qui est aujourd'hui habituelle (cf. la suite du présent chapitre). La question est alors la suivante : cette preuve est-elle vraiment une preuve de l'isomorphisme énoncé ? La réponse de Peirce est implicitement négative et cela me semble largement justifié. Car il ne s'agit jamais que d'une preuve de l'isomorphisme entre la classe des classes d'équivalence des segments géométriquement superposables (ou plus simplement la classe de tous les segments géométriquement différents possibles) et l'ensemble des nombres réels. Pour passer de cet isomorphisme à l'autre, il faut supposer que la droite géométrique est composée par les extrémités non géométriquement superposées de tous les segments géométriquement différents qu'on peut prendre sur elle. En d'autres termes, il faut interpréter un segment comme un demi-ouvert dans $\mathbb{R}$. Et la manière la plus simple de le faire est justement d'affirmer *a priori* l'isomorphisme qu'on voudrait prouver.

On comprend alors la raison qui a poussé Peirce à qualifier plus tard (respectivement en 1906 et 1911) son article de 1892 de « *blundering* » et « *crude* » : il semble confondre (comme une grande partie des mathématiciens du XX$^{\text{ème}}$ siècle) la question de la nature du continu avec celle de la mesure d'un continu, tel que la droite géométrique. Pourtant, une confusion a été rarement aussi féconde que celle-ci, car elle est à coup sûr à l'origine de l'introduction du continu en tant qu'objet mathématique. La question mathématique qui semble alors se poser à Peirce (et à tous ceux qui rejettent cette confusion) est la suivante : peut-on construire un objet mathématique, essentiellement différent de $\mathbb{R}$, qui répond non seulement aux exigences de la mesure, mais aussi à celles de l'expression objective de l'être un, en tant que un ? Cette deuxième exigence est aussi ancienne que la première, car on la retrouve affirmée en toutes lettres dans la *Physique* d'Aristote.

On peut interpréter les nombreuses prises de position de Peirce — autant dans les conférences de Cambridge qu'ailleurs — en faveur d'une interprétation infinitésimaliste de la droite géométrique, comme l'indice d'une conception du continu en quelque sorte similaire à celle proposée par l'analyse non-standard (cf. la note historique 6.11). Cette interprétation s'accorde parfaitement avec un texte de 1893, « The Logic of Quantity ». Dans ce texte, Peirce ne semble pas avoir encore complètement abandonné l'espoir de retrouver une définition du continu, convenable à ses yeux, par une correction de la définition de Dedekind (cf. le paragraphe 4.2). Il interprète cependant le continu ainsi défini en termes infinitésimaux, en affirmant que la partition d'un segment en $2^{\aleph_0}$ parties produit non pas des points, mais des parties structurellement similaires au segment de départ.

En 1898, à l'époque des *Cambridge Conferences*, Peirce semble désormais avoir abandonné l'idée de comprendre la nature du continu grâce à une lecture infinitésimaliste de la définition de Dedekind. S'il continue ici et là à parler d'infinitésimaux, il me semble qu'il n'a d'autre intention que de dénoncer l'insuffisance du point de vue de la mesure, quant à la question de la nature de l'un. Cette nature — cela me semble être le point essentiel de la conception avancée par Peirce dans les conférences de Cambridge — n'est pas celle d'un ensemble. Une expression objective de l'être un ne peut être cherchée que dans un objet mathématique autre qu'un ensemble. C'est

pour éclairer ce point que dans la huitième de ses conférences, Peirce présente la notion d'agrégat potentiel. L'idée qui semble apparaître est celle d'une caractérisation purement corrélative (cf. la note historique 1.4) du continu. On retrouve une idée similaire dans une lettre de 1900 à l'éditeur de *Science*. Ici Peirce emploie le terme « ligne » pour indiquer un objet, disons $\Sigma$, qui satisfait aux postulats suivants : i) « les points peuvent être déterminés dans une certaine relation » à lui, qu'on pourrait qualifier de la relation de « être sur » ; ii) quatre points différents qui sont sur $\Sigma$ étant déterminés, chacun d'eux « est séparé d'un des autres par les deux restants » ; iii) pour n'importe quels trois points $\mathsf{A}$, $\mathsf{B}$ et $\mathsf{C}$ qui sont sur $\Sigma$, « toute multitude de points peut être déterminée » sur $\Sigma$ de telle manière que chacun d'entre eux est séparé de $\mathsf{A}$ par $\mathsf{B}$ et $\mathsf{C}$. Il est difficile d'interpréter précisément cette définition. Ce qui est important est que, d'après Peirce, $\Sigma$ ne peut pas être un ensemble et ne peut donc être conçu autrement que comme une collection continue, au sens de la troisième conférence de Cambridge. S'il en est ainsi, tout ensemble de points (c'est-à-dire d'objets qui gisent sur $\Sigma$), quel que soit sa cardinalité, peut être déterminé sur $\Sigma$. Pourtant, précise Peirce, cette possibilité ne relève pas de nous, mais de la nature elle-même. En d'autres termes, et si je comprends bien la remarque de Peirce : si la première cardinalité transfinie nous apparaît comme la cardinalité du continu (par rapport à la mesure), ceci tient aux limites de nos capacités cognitives et non pas à la structure intrinsèque de la nature.

**Lectures possibles** : M. Panza, « De la continuité comme concept au continu comme objet mathématique », *in* J.-M. Salanskis et H. Sinaceur (éds.) *Le Labyrinthe du continu*, Springer-France, Paris 1992, pp. 16-30.

Remarque 6.14. Les opinions de Peirce ne sont qu'un symptôme, parmi beaucoup d'autres, d'un fait indubitable : bien que la définition moderne de l'ensemble des nombres réels apporte une contribution essentielle à la compréhension du phénomène de la continuité, elle ne permet pas de clore le débat sur la nature du continu. Ce débat est encore aujourd'hui très vivant et très riche. Il a été, entre autres, revitalisé au début des années soixante, par A. Robinson, qui a montré qu'il y a une manière logiquement cohérente d'étendre $\mathbb{R}$, en y introduisant des éléments qui fonctionnent comme des infinitésimaux, en donnant origine, de cette manière, à ce qu'il a lui-même appelée « analyse non standard ».

Note Historique 6.11. En 1920, en reprenant des résultats précèdents de L. Löwenheim, le mathématicien norvégien A. T. Skolem (1887-1963) démontra que si une théorie exprimée dans un langage dénombrable du premier ordre (c'est-à-dire un langage dans lequelle on ne peut que quantifier sur des individus, mais non pas sur des propriétés d'individus : on peut dire « pour chaque $x$, $P(x)$ » ou « il y a un $x$, tel que $P(x)$ », mais non pas « pour chaque $P$, $P(x)$ » ou « il y a un $P$, tel que $P(x)$ » ) admet un modèle infini (c'est-à-dire, pour être rapides, que les axiomes de cette théorie et, donc, ses théorèmes sont satisfaits par un ensemble infini), alors elle admet sans doute un modèle dénombrable. C'est le résultat que les logiciens appellent généralement « théorème de Löwenheim-Skolem descendant ». De ce théorème, il suit que de tout ensemble infini non dénombrable qui satisfait à certaines conditions, exprimées par des axiomes écrits dans un langage dénombrable du premier ordre, il est possible d'extraire un sous-ensemble dénombrable qui satisfait à ces mêmes conditions ; dit en d'autres termes : la théorie élémentaire (c'est-à-dire du premier ordre) de chaque structure infinie admet un modèle dénombrable. Quelques années plus tard, Tarski démontra une conséquence du théorème de Löwenheim-Skolem descendant qui depuis est connu sous le nom de « théorème de Löwenheim-Skolem ascendant », car, en un

certain sens, il renverse la direction du théorème précèdent. Ce théorème affirme que la théorie élémentaire de chaque structure infinie de cardinalité $\alpha$ admet un modèle de cardinalité $\beta$, quel que soit $\beta$ plus grand que $\alpha$.

Comme il est possible de substituer au cinquième axiome de Peano une infinité d'axiomes, dont chacun porte sur une propriété exprimée dans un langage dénombrable, c'est-à-dire qu'il est possible d'écrire dans un langage du premier ordre un ensemble (infini) d'axiomes équivalents aux axiomes de Peano, de ce dernier théorème il suit que ces axiomes (écrits au premier ordre) admettent un modèle infini non dénombrable, et ce modèle peut être obtenu comme une extension de $\mathbb{N}$. Il doit donc être possible d'élargir $\mathbb{N}$ de telle sorte que l'ensemble élargi qu'on obtient par cet élargissement n'est pas dénombrable et satisfait néanmoins aux axiomes de Peano écrits au premier ordre. Ce fut Skolem lui-même qui construisit (en 1934) un élargissement de $\mathbb{N}$ de cette sorte et qui montra que les nouveaux individus qui étaient ainsi ajoutés à $\mathbb{N}$ se comportaient comme des nombres naturels infinis.

En 1960 Robinson (né en 1918 à Waldemburg, en Allemagne, aujourd'hui la ville polonaise de Walbrzych, et mort en 1974 à Yale) fit la même chose en partant de $\mathbb{R}$ : il construisit une extension de $\mathbb{R}$ de cardinalité supérieure à $\mathbb{R}$ qui satisfait à tous les théorèmes satisfaits par $\mathbb{R}$ (et pour laquelle tous les résultats de l'analyse ordinaire sont donc valables) dont la cardinalité est supérieure à la cardinalité de $\mathbb{R}$, et montra que les nouveaux individus qui étaient ainsi ajoutés à $\mathbb{R}$ se comportent comme des nombres réels infiniment petits, infiniment grands et infiniment proches de chaque nombre réel ordinaire. Il baptisa cet ensemble « ${}^*\mathbb{R}$ » (« er *star* » et il appela sa théorie « analyse non standard ».

Quelques années plus tard, en 1977, le mathématicien américain E. Nelson montra qu'il est possible d'ajouter, au langage habituel de la théorie des ensembles, un nouveau prédicat, le prédicat unaire 'être standard', et d'employer la nouvelle théorie ainsi construite pour obtenir une version axiomatique de l'analyse non standard qui ne nécessite pas, de ce fait, la complexe construction de Robinson, ce qui, dans l'intention de Nelson lui-même, aurait dû servir (et *de facto* servit) à rendre les méthodes de l'analyse non standard « directement utilisables par le mathématicien dans son activité ».

**Lectures possibles** : A. Robinson, *Non-Standard Analysis*, North-Holland, Amsterdam, 1960 ; H. Barreau et J. Harthong, *La mathématique non standard*, Éditions du CNRS, Paris, 1989 ; R. Lutz et L. G. Albuquerque, « Reasonning with infinitesimals. Modern infinitesimals as a tool to match intuitive and formal reasonning in analysis », C. Alvarez et M. Panza, eds., *Logic and Mathematical Reasoning*, numero spciale de *Synthese*, **134**, 1-2, 2003, pp. ? ? ?.

**4.1. Définition explicite des réels : la construction de Cantor.** On commencera notre construction de $\mathbb{R}$ à partir de $\mathbb{Q}^+$, en essayant de comprendre, plus généralement, la situation dans laquelle se trouvent la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

et la série

$$\sum_{i=0}^{\infty} \frac{n_i}{\prod_{j=1}^{i} m_j}$$

en $\mathbb{Q}^+$. Pour ce faire, revenons à la définition 2.3. Cette définition établit les conditions sous lesquelles on peut dire d'une suite $\{u_i\}_{i=0}^{\infty}$ qu'elle est convergente vers $U$ dans $E$. On a pourtant vu qu'elle n'est pas apte à caratériser les suites à termes dans $E$ dont les termes obéissent à une loi d'accumulation : être convergente vers une certaine limite $U$ dans $E$ ne signifie pas, pour une suite à termes dans $E$, satisfaire à une loi d'accumulation ; il est donc possible de trouver des suites à termes dans $E$ qui obéissent à une loi d'accumulation, mais sont néanmoins divergentes dans $E$. On peut pourtant penser qu'entre une suite à termes dans $E$ qui converge vers une certaine limite dans $E$ et une autre suite à termes dans $E$ qui diverge dans $E$, tout en obéissant à une loi d'accumulation, il y a une analogie bien plus profonde qu'entre la deuxième de ces suites et une troisième suite à termes dans $E$ qui n'obéit à aucune loi d'accumulation. Si on pense ainsi, on pourrait trouver gênant que, d'après la définition 2.3, les deux dernières suites soient qualifiées de divergentes et la première soit en revanche qualifiée de convergente. Il ne suffira pas d'observer que la définition 2.3 capture une autre analogie, également importante, qui subsiste entre la deuxième suite et la troisième, et non pas entre la deuxième et la première : la série dont les termes de ces suites sont des sommes partielles a, en une sens, une somme dans $E$, tandis que cela n'est le cas ni de la deuxième, ni de la troisième suite. Il ne s'agit pas, en effet, de contester la légitimité de la définition 2.3, mais de se demander si cette définition fournit à elle seule les outils mathématiques nécessaires pour distinguer entre les différentes sortes de suites qu'il semble convenable de distinguer. Or, la réponse à cette question est sans doute négative : l'exemple donné dans le paragraphe précédent fait surgir la nécessité d'une autre définition apte à capturer, et donc à préciser formellement, la notion informelle d'obéissance à une loi d'accumulation. La manière la plus naturelle de faire débuter la recherche d'une telle définition est de se demander s'il n'y aurait pas une propriété, dont jouit toute suite à termes dans $E$ convergente vers une limite dans $E$, qu'il serait possible de formuler sans se réclamer de la limite dans $E$ de cette suite. La réponse est positive et repose pour l'essentiel sur une idée qui a été présentée pour la première fois par le mathématicien français Augustin-Louis Cauchy dans son *Cours d'analyse*, publié à Paris en 1821.

Imaginons qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ converge vers $U$ dans $\mathbb{Q}$, alors, d'après la définition 2.4, elle est telle qu'il y a un élément $U$ de $\mathbb{Q}$, tel que, pour tout élément $\varepsilon$ de $\mathbb{Q}^+$, différent de 0, il y a un nombre naturel $n$, tel que, si $i > n$, alors $|U - u_i| < \varepsilon$. Qu'on pose $\varepsilon = 2\xi$. Il devra y avoir aussi un nombre naturel $n$, tel que si $j$ est un nombre naturel quelconque et $i > n$, alors

$$|U - u_i| < \xi \qquad \text{et} \qquad |U - u_{i+j}| < \xi \tag{90}$$

Or, si $x \in \mathbb{Q}$ (mais la même chose est vraie pour tout ensemble $E$, totalement ordonné et fermé par rapport à la soustraction), on aura, d'après la définition de la valeur absolue,

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases} \tag{91}$$

et donc, si $x$ et $y$ appartiennent à $\mathbb{Q}$,

$$|x + y| = \begin{cases} x + y & \text{si } x + y \geq 0 \\ -x - y & \text{si } x + y < 0 \end{cases} \tag{92}$$

et ainsi, pour tout couple de rationnels $x$ et $y$ :

$$|x+y| \leq |x| + |y| \tag{93}$$

Pour le prouver, il suffit de vérifier que c'est ainsi dans les quatre cas : $x, y \geq 0$ ; $x, y < 0$ ; $x \geq 0$, $y < 0$, $x+y \geq 0$ ; $x \geq 0$, $y < 0$, $x+y < 0$ qui (à cause de la commutativité de l'addition) épuisent les cas possibles.

REMARQUE 6.15. Ceux, parmi les lecteurs, qui sont déjà familiers avec la notion de vecteur comprendront que la (93) nous dit, au fond, que la somme des modules de deux vecteurs est toujours plus grande ou égale au module du vecteur résultant de la composition de ces mêmes vecteurs. Pour « voir » cette propriété fondamentale de la composition vectorielle appliquée dans un cas exemplaire, le lecteur n'a qu'à considérer un triangle et observer que la somme de deux de ses trois côtés est toujours plus grande (ou, à la limite, égale) au troisième côté. C'est pourquoi (93) est souvent appellée « inégalité du triangle ». Cette propriété du triangle correspond d'ailleurs à une propriété bien connue de la droite : une droite est le chemin le plus court qui joint deux points quelconques sur un plan.

Il est alors facile de comprendre que

$$|x-y| = |x+(-y)| \leq |x| + |-y| = |x| + |y|$$

et donc, en revenant à la (90) :

$$|u_{i+j} - u_i| = |(U-u_i) - (U-u_{i+j})| \leq |U-u_i| + |U-u_{i+j}| < 2\xi = \varepsilon$$

Donc, si une suite $\{u_i\}_{i=0}^{\infty}$ converge vers une certaine limite $U$ dans $\mathbb{Q}$, alors, quelle que soit $U$, elle est telle que pour tout $\varepsilon$ appartenant à $\mathbb{Q}$ strictement positif, il y a un nombre naturel $n$, tel que si $i > n$ et $p \in \mathbb{N}$, alors

$$|u_{i+p} - u_i| < \varepsilon \tag{94}$$

Or, non seulement il est possible d'assigner cette propriété à une suite à termes dans $\mathbb{Q}$ qui converge vers une certaine limite dans $\mathbb{Q}$, sans se référer explicitement à la limite de cette suite, mais il semble aussi que cette propriété d'une telle suite soit exactement celle dont on veut parler quand on dit que cette suite obéit à une loi d'accumulation. Il est en effet facile de montrer que cette propriété est satisfaite par la suite

$$\left\{ \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right\}_{\nu=0}^{\infty}$$

à termes dans $\mathbb{Q}$ et divergente dans $\mathbb{Q}$, c'est-à-dire que, quel que soit $\varepsilon$ appartenant à $\mathbb{Q}^+$ et différent de 0, il y a un nombre naturel $n$, tel que si $\nu > n$ et $p \in \mathbb{N}$, alors

$$\left| \sum_{i=0}^{\nu+p} \frac{n_i}{\prod_{j=1}^{i} m_j} - \sum_{i=0}^{\nu} \frac{n_i}{\prod_{j=1}^{i} m_j} \right| = \left| \sum_{i=\nu+1}^{\nu+p} \frac{n_i}{\prod_{j=1}^{i} m_j} \right| = \sum_{i=\nu+1}^{\nu+p} \frac{n_i}{\prod_{j=1}^{i} m_j} < \varepsilon \tag{95}$$

Cela est facile à vérifier, car par construction on a, pour tout $\mu$ naturel,

$$\left[\sum_{i=0}^{\mu}\frac{n_i}{\prod_{j=1}^{i} m_j}\right](\mathsf{PQ}) = \mathsf{MN} - R_\mu$$

et donc

$$\left[\sum_{i=v+1}^{\nu+p}\frac{n_i}{\prod_{j=1}^{i} m_j}\right](\mathsf{PQ}) = (\mathsf{MN} - R_{\nu+p}) - (\mathsf{MN} - R_\nu) = R_\nu - R_{\nu+p}$$

Mais, comme la suite $\{R_\nu\}_{\nu=0}^{\infty}$ converge vers le segment nul dans l'ensemble de tous les segments (nuls ou non nuls), la différence $R_\nu - R_{\nu+p}$ ne peut, quel que soit $p$, que s'approcher de plus en plus de ce même segment, lorsque $\nu$ croît ; de là, il est facile de tirer (95).

NOTE HISTORIQUE 6.12. Dans le paragraphe 1 du *Cours d'analyse*, tout de suite après avoir défini la convergence d'une série comme on l'a vu dans la note historique 6.7, Cauchy ajoute : « D'après les principes ci-dessus établis, pour que la série $u_0, u_1, u_2, \ldots, u_n, u_{n+1}, \ldots$ [comme il est clair d'après le passage qu'on a cité dans la note historique 6.7, Cauchy se réfère ici, en termes modernes, à la série $\sum_{i=0}^{\infty} u_i$ associée à la suite $\{u_i\}_{i=0}^{\infty}$ ] soit convergente [...], il est nécessaire et il suffit que, pour des valeurs infiniment grandes du nombre $n$, les sommes $s_n, s_{n+1}, s_{n+2}, \ldots$ diffèrent de la limite $s$, et par conséquent entre elles, de quantités infiniment petites ». Ce qui nous intéresse dans cette citation, et qui a marqué fort profondément les mathématiques successives, est évidemment l'incidente « et par conséquent entre elles ». Même si, apparement, Cauchy ne semble pas donner une grande importance à cette incidente, qu'il semble introduire presque en passant, la différence entre les deux critères de convergence énoncées par Cauchy est évidemment essentielle.

Pour s'assurer de la convergence de la série $\sum_{i=0}^{\infty} u_i$ d'après le premier de ces critères, il faut en effet connaître *a priori* la limite $s$ de cette série. En effet, pour peu qu'on donne un sens précis aux conditions qui assignent à $n$ « des valeurs infiniment grandes » et aux différences entre $s_n, s_{n+1}, s_{n+2}, \ldots$ et $s$ des valeurs infiniment petites, il semble que ce critère ne diffère pas essentiellement de la condition à laquelle Cauchy se réfère lors de sa définition de la convergence d'une série. En effet si le terme « infiniment petit » désigne une variable dont la limite est zéro, dire d'un nombre naturel $n$ qu'il prend des valeurs infiniment grandes ne peut que signifier que la variable à valeurs rationnelles $\frac{1}{n}$ a zéro comme limite, c'est-à-dire que pour tout $h$ positif, il y a une valeur $\overline{n}$ de $n$, telle que, pour toutes les valeurs $\overline{\overline{n}}$ plus grandes que $\overline{n}$, $\frac{1}{\overline{\overline{n}}} < h$, ce qui est toujours vrai si $n$ croît sans bornes. Si Cauchy prétend ainsi distinguer entre sa définition et le premier des critères précédents, c'est qu'il pense possible, en dépit de sa définition de l'infiniment petit, de traiter des valeurs infiniment grandes et infiniment petites respectivement de $n$ et des différences entre $s_n, s_{n+1}, s_{n+2}, \ldots$ et $s$, d'une manière qui n'est pas en revanche consentie par sa définition.

Ceci mis à part, considérons le deuxième critère. Comme on l'a dit dans la note historique 6.7, Cauchy se pose d'emblée dans l'ensemble des nombres réels, même s'il ne possède aucune définition satisfaisante de cet ensemble. Pour lui, il n'y a donc pas de doute qu'une série, dont les réduites partielles satisfont à une loi d'accumulation, a

une limite, c'est-à-dire qu'il existe une limite pour cette série. Le problème pour lui est plutôt celui de caractériser de manière assez précise la condition qui demande qu'une série satisfasse à une loi d'accumulation. C'est exactement ce qu'il fait en demandant que « pour des valeurs infiniment grandes du nombre $n$, les sommes $s_n, s_{n+1}, s_{n+2}, \ldots$ diffèrent [...] entre elles, de quantités infiniment petites ». En effet, dans la remarque qui suit l'énoncé de ses critères, Cauchy donne pour acquis ce qui est en revanche pour nous l'objet de la preuve la plus difficile, c'est-à-dire que pour chaque série (à termes dans $\mathbb{R}$) qui satisfait à cette condition, il existe dans $\mathbb{R}$ une limite $s$ qui satisfait à la condition énoncée par Cauchy dans sa définition de convergence. Cette définition n'est d'ailleurs, justement, qu'une définition de convergence tout court, et non pas, comme c'est en revanche le cas de nos définitions, une définition de convergence vers une certaine limite dans $\mathbb{R}$. Cauchy ne se préoccupe pas non plus de démontrer que si une série $\sum_{i=0}^{\infty} u_i$ converge, alors « pour des valeurs infiniment grandes du nombre $n$, les sommes $s_n, s_{n+1}, s_{n+2}, \ldots$ diffèrent [...] entre elles, de quantités infiniment petites ». Cette preuve est pourtant immédiate et Cauchy semble vouloir la laisser à ses lecteurs en guise d'exercice.

Il ne reste qu'à rendre explicite ce qui devrait déjà apparaître clairement après les citations précédentes : Cauchy n'énonce son critère que pour des séries et non pas pour des suites, même si, pour traiter de séries, il passe, exactement comme nous, par la considération des suites de leurs réduites partielles. C'est que l'objet suite, pris en tant que tel, n'attire pas l'attention de Cauchy, comme il n'avait pas attiré celle des mathématiciens précédents. C'est seulement plus tard, et justement en connexion avec l'effort d'une définition précise des notions de limite et de convergence, que cet objet s'imposa comme l'un des objets fondamentaux de l'analyse.

**Lectures possibles** : A. L. Cauchy, *Cours d'analyse de l'École Royale Polytechnique. Première partie : analyse algébrique* (éd. et introdution par U. Bottazzini) Clueb, Bologne, 1992 (réimp. de l'édition originale de 1821).

Il semble alors que la condition (94) exprime une propriété d'une suite à termes dans $\mathbb{Q}$ qui est satisfaite, en même temps, par une suite à termes dans $\mathbb{Q}$ qui converge vers une certainne limite dans $\mathbb{Q}$ et par une suite à termes dans $\mathbb{Q}$ qui, tout en étant divergente dans $\mathbb{Q}$, obéit à une loi d'accumulation. Il est alors naturel de généraliser cette condition et de la fixer par une définition :

DÉFINITION 4.1. *On dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $E$ est une suite de Cauchy, relativement à la distance $\Delta : E^2 \to D$, $D$ étant un ensemble totalement ordonné relativement à une relation d'ordre $\preceq$, possédant un élément minimal $\alpha$, si et seulement si toutes les images $\Delta(u_h, u_k)$ d'un couple quelconque $< u_h, u_k >$ de termes de la suite $\{u_i\}_{i=0}^{\infty}$ selon $\Delta$ appartiennent à $D$, et pour tout $\varepsilon$ appartenant à $D$, tel que $\alpha \prec \varepsilon$, il y a un nombre naturel $n$, tel que, si $i > n$ et $j \in \mathbb{N}$, alors $\Delta(u_{i+j}, u_i) \prec \varepsilon$ ; en symboles :*

$$(\varepsilon \in D) \Rightarrow [\alpha \prec \varepsilon \Rightarrow (\exists n \in \mathbb{N} \text{ tel que } [(i > n) \wedge (j \in \mathbb{N})] \Rightarrow \Delta(u_{i+j}, u_i) \prec \varepsilon)]$$

*On dit ensuite qu'une série $\sum_{i=0}^{\infty} u_i$ à termes dans $E$, $E$ étant un ensemble sur lequel est définie une addition par rapport à laquelle cet ensemble est fermé, est une série de Cauchy, relativement à la distance $\Delta : E^2 \to D$, si et seulement si la suite $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$ à termes dans $E$ est une suite de Cauchy relativement à cette même distance.*

Aussi dans ce cas, il convient d'expliciter la forme qu'une telle définition prend lorsqu'elle s'applique à une suite ou à une série à termes dans $\mathbb{Q}$, évaluées relativement à la distance entre deux éléments de $\mathbb{Q}$ donnée par la valeur absolue de leur différence :

DÉFINITION 4.2. *On dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ est une suite de Cauchy si et seulement si pour tout $\varepsilon$ appartenant à $\mathbb{Q}^+$, différent de 0, il y a un nombre naturel $n$, tel que, si $i > n$ et $j \in \mathbb{N}$, alors $|u_{i+j} - u_i| < \varepsilon$ ; en symboles :*

$$(\varepsilon \in \mathbb{Q}^+) \Rightarrow [0 < \varepsilon \Rightarrow (\exists n \in \mathbb{N} \text{ tel que } [(i > n) \wedge (j \in \mathbb{N})] \Rightarrow |u_{i+j} - u_i| < \varepsilon)]$$

*On dit ensuite qu'une série $\sum_{i=0}^{\infty} u_i$ à termes dans $\mathbb{Q}$ est une série de Cauchy si et seulement si la suite $\left\{\sum_{i=0}^{j} u_i\right\}_{j=0}^{\infty}$ à termes dans $\mathbb{Q}$ est une suite de Cauchy.*

On a déjà démontré que si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ est convergente vers $U$ dans $\mathbb{Q}$, alors c'est une suite de Cauchy. Il est pourtant évident, depuis la longue discussion précédente, que la réciproque ne vaut pas : une suite de Cauchy à termes dans $\mathbb{Q}$ peut être divergente dans $\mathbb{Q}$. Il est pourtant possible de considérer des ensembles $E$, et des distances $\Delta$ définies sur ces ensembles, tels qu'une suite à termes dans $E$ est convergente vers une limite dans $E$, relativement à la distance $\Delta$, si et seulement si c'est une suite de Cauchy, relativement à cette même distance. D'après le but qu'on a fixé ci-dessus, on construira justement l'ensemble des nombres réels comme l'extension minimale $\mathbb{R}$ de $\mathbb{Q}$, telle qu'une suite à termes dans $\mathbb{Q}$ soit convergente vers une limite dans $\mathbb{R}$ (toujours relativement à la distance entre deux termes de $\mathbb{R}$ donnée par la valeur absolue de leur différence) si et seulement si c'est une suite de Cauchy (relativement à cette même distance) ; et on montrera ensuite que cette extension $\mathbb{R}$ de $\mathbb{Q}$ sera aussi telle qu'une suite à termes dans $\mathbb{R}$ est convergente vers une limite dans $\mathbb{R}$ (relativement à la distance entre deux termes de $\mathbb{R}$ donnée par la valeur absolue de leur différence) si et seulement si c'est une suite de Cauchy (relativement à cette même distance). Dit en d'autres termes : on construira l'ensemble des nombres réels comme l'extension minimale $\mathbb{R}$ de $\mathbb{Q}$ qui soit fermée par rapport à l'opération du passage à la limite des suites de Cauchy à termes dans $\mathbb{Q}$, et on montrera que l'ensemble ainsi obtenu est aussi fermé par rapport à l'opération du passage à la limite des suites de Cauchy à termes dans $\mathbb{R}$. Il en résultera, évidemment, que toute série de Cauchy à termes dans $\mathbb{R}$ possède une limite dans $\mathbb{R}$ même, et donc que $\mathbb{R}$ est fermé non seulement par rapport à l'addition finie, mais aussi par rapport à l'addition infinie, lorsque cette dernière consiste en une série de Cauchy.

REMARQUE 6.16. Il résulte alors clairement que $\mathbb{R}$ sera construit d'emblée comme un ensemble intervenant dans une structure donnée, au moins, par : un ensemble ; une addition inversible et associative fonctionnant comme une loi de composition interne définie sur cet ensemble ; une application de $\mathbb{R}$ sur $\mathbb{R}$, donnant la valeur absolue de tout terme de $\mathbb{R}$ , et donc de la différence entre deux termes quelconques de $\mathbb{R}$ ; une relation d'ordre par rapport à laquelle cet ensemble résulte totalement ordonné. En réalité, il n'est pas nécessaire, pour qu'on puisse définir des suites de Cauchy sur un certain ensemble, que cet ensemble soit totalement ordonné par rapport à une quelconque relation d'ordre. Si on définit convenablement une distance, c'est-à-dire si on fournit cet ensemble d'une métrique convenable, cette condition est superflue (la définition des suites de Cauchy à termes dans l'ensemble $\mathbb{C}$ des nombres complexes, fournit un exemple de cette possibilité, qu'il nous sera pourtant impossible ici d'exhiber). Dans la suite, on caractérisera pourtant $\mathbb{R}$ comme un ensemble totalement ordonné par rapport à $\leq$ et on se réclamera de cette relation d'ordre pour définir les suites de Cauchy à termes dans $\mathbb{R}$.

La manière la plus simple d'accomplir cette construction est de définir une relation d'égalité sur l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$ et de définir $\mathbb{R}$ comme l'ensemble des classes d'équivalence de ces suites sous cette relation d'égalité. On commence par la définition suivante :

DÉFINITION 4.3. *Une suite de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$, est dite « nulle » (en symboles : $\{u_i\}_{i=0}^{\infty} = 0$) si elle converge vers 0 dans $\mathbb{Q}$ ; elle est dite « positive » si, pour tout nombre rationnel $\varepsilon$ strictement positif, il y a un nombre naturel $n$, tel que $(i > n) \Rightarrow u_i > -\varepsilon$ ($-\varepsilon$ étant évidemment l'inverse de $\varepsilon$ par rapport à l'addition définie sur $\mathbb{Q}$) ; elle est dite « négative » si elle n'est pas positive ; elle est dite enfin « strictement positive » si elle est positive, sans être nulle.*

REMARQUE 6.17. Le lecteur est invité à démontrer comme exercice que, d'après ces définitions, une suite de Cauchy à termes dans $\mathbb{Q}$ positive peut être nulle et que toute suite de Cauchy à termes dans $\mathbb{Q}$ nulle est positive. Cela lui permettra de comprendre que la définition précédente est parfaitement légitime et naturelle.

À partir de là, on peut ensuite définir la relation d'égalité sur les suites de Cauchy comme il suit :

DÉFINITION 4.4. *On dit que deux suites de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$, sont « égales » (en symboles : $\{u_i\}_{i=0}^{\infty} = \{v_i\}_{i=0}^{\infty}$) si et seulement si la suite $\{u_i - v_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ est nulle.*

REMARQUE 6.18. Le lecteur est invité à démontrer comme exercice que deux suites de Cauchy à termes dans $\mathbb{Q}$ nulles sont nécessairement égales.

Une définition de l'ensemble des nombres réels pourra alors être la suivante :

DÉFINITION 4.5. *On appelle « ensemble des nombres réels » l'ensemble, noté « $\mathbb{R}$ », des classes d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$, relativement à la relation d'égalité qu'on vient de définir. Si $\{u_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{Q}$, on note la classe d'équivalenece à laquelle elle appartient par le symbole « $Cl\,(\{u_i\}_{i=0}^{\infty})$ » de sorte que, si $\{u_i\}_{i=0}^{\infty}$et $\{v_i\}_{i=0}^{\infty}$ sont deux suites de Cauchy à termes dans $\mathbb{Q}$, telles que $\{u_i\}_{i=0}^{\infty} = \{v_i\}_{i=0}^{\infty}$, alors les symboles « $Cl\,(\{u_i\}_{i=0}^{\infty})$ » et « $Cl\,(\{v_i\}_{i=0}^{\infty})$ » désigneront la même classe d'équivalence et donc le même nombre réel.*

Cette définition, qui est originairement due à G. Cantor, nous assure que l'ensemble $\mathbb{R}$ des nombres réels peut être mis en bijection avec l'ensemble des segments distincts (nuls ou non nuls) qu'on peut tracer sur une droite donnée, à partir d'une origine fixée, et donc qu'il peut être mis en bijection avec l'ensemble des points de cette droite qu'on peut traiter comme les extrémités des segments gisant sur celle-ci. En effet, en utilisant la procédure décrite dans le paragraphe 1 du présent chapitre, et en la réitérant éventuellement à l'infini, il est possible d'associer à chacun de ces segments, et donc à chacun de ces points, une suite de Cauchy de rationnels, et il n'est pas difficile de démontrer que, quelle que soit l'unité de mesure choisie, deux suites de Cauchy à termes dans $\mathbb{Q}$ sont égales si et seulement si elles sont associées, selon cette procedure, au même segment pris sur la droite en question. Le lecteur pourra conduire seul cette démonstration.

D'autre part, lorsqu'une suite de Cauchy à termes dans $\mathbb{Q}$ est donnée il est également possible de lui associer un segment de sorte que, le même segment est associé à deux suites de Cauchy distinctes si et seulement si ces suites sont égales. Bien qu'elle réponde donc à une de nos exigences, cette définition peut néanmoins paraître paradoxale. Les deux questions suivantes viennent en fait spontanément à l'esprit : en quel sens peut-on dire que l'ensemble des

classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ (dont les éléments sont finalement des ensembles de sous-ensembles de $\mathbb{Q}$) est une extension de $\mathbb{Q}$, c'est-à-dire qu'il contient $\mathbb{Q}$ ? En quel sens peut-on traiter de nombres des classes d'équivalence de suites de rationnels ?

Pour répondre à ces questions, on commencera par adopter la définition suivante :

DÉFINITION 4.6. *Si $Cl(\{u_i\}_{i=0}^{\infty})$ est un nombre réel ($\{u_i\}_{i=0}^{\infty}$ étant une suite de Cauchy à termes dans $\mathbb{Q}$), alors on dit : qu'il est nul si et seulement si et seulement si la suite $\{u_i\}_{i=0}^{\infty}$ est nulle ; qu'il est positif si et seulement si la suite $\{u_i\}_{i=0}^{\infty}$ est positive ; qu'il est strictement positif si et seulement si la suite $\{u_i\}_{i=0}^{\infty}$ est strictement positive ; et qu'il est négatif si et seulement si la suite $\{u_i\}_{i=0}^{\infty}$ est négative. Il n'y aura alors qu'un seul nombre réel nul, qu'on pourra indiquer avec le symbole « 0 ».*

On passera ensuite à la définition d'une addition et d'une multiplication sur $\mathbb{R}$. Pour ce faire, il sera d'abord nécessaire de définir ces opérations sur l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$. Voici comment cela est possible :

DÉFINITION 4.7. *On appelle « addition » de deux suites de Cauchy à termes dans $\mathbb{Q}$ l'opération, notée « + », qui conduit des suites de Cauchy à termes dans $\mathbb{Q}$ $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ à la suite de Cauchy à termes dans $\mathbb{Q}$ $\{u_i + v_i\}_{i=0}^{\infty}$ ; en symboles :*

$$\{u_i\}_{i=0}^{\infty} + \{v_i\}_{i=0}^{\infty} = \{u_i + v_i\}_{i=0}^{\infty}$$

DÉFINITION 4.8. *On appelle « multiplication » de deux suites de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ l'opération, notée « $\cdot$ » qui conduit des suites de Cauchy à termes dans $\mathbb{Q}$ $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ à la suite de Cauchy à termes dans $\mathbb{Q}$ $\{u_i \cdot v_i\}_{i=0}^{\infty}$ ; en symboles :*

$$\{u_i\}_{i=0}^{\infty} \cdot \{v_i\}_{i=0}^{\infty} = \{u_i \cdot v_i\}_{i=0}^{\infty}$$

Il est facile de voir que ces définitions sont cohérentes avec les précédentes et que les opérations d'addition et de multiplication ainsi définies restent univoques. Par exemple, on peut montrer que si $\{u_i\}_{i=0}^{\infty} = \{v_i\}_{i=0}^{\infty}$ et $\{u'_i\}_{i=0}^{\infty} = \{v'_i\}_{i=0}^{\infty}$,

alors $\{u_i\}_{i=0}^{\infty} + \{v_i\}_{i=0}^{\infty} = \{u'_i\}_{i=0}^{\infty} + \{v'_i\}_{i=0}^{\infty}$ et $\{u_i\}_{i=0}^{\infty} \cdot \{v_i\}_{i=0}^{\infty} = \{u'_i\}_{i=0}^{\infty} \cdot \{v'_i\}_{i=0}^{\infty}$. Le lecteur pourra le faire seul, en guise d'exercice ; il ne rencontrera aucune difficulté. Les théorèmes qu'il aura ainsi établis, rendent légitime la définition suivante, qui définit l'addition et la multiplication sur $\mathbb{R}$ :

DÉFINITION 4.9. *Si $Cl(\{u_i\}_{i=0}^{\infty})$ et $Cl(\{v_i\}_{i=0}^{\infty})$ sont deux nombres réels ($\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ étant deux suites de Cauchy à termes dans $\mathbb{Q}$), alors*

$$Cl\left(\{u_i\}_{i=0}^{\infty}\right) + Cl\left(\{v_i\}_{i=0}^{\infty}\right) = Cl\left(\{u_i + v_i\}_{i=0}^{\infty}\right)$$

*et*

$$Cl\left(\{u_i\}_{i=0}^{\infty}\right) \cdot Cl\left(\{v_i\}_{i=0}^{\infty}\right) = Cl\left(\{u_i \cdot v_i\}_{i=0}^{\infty}\right)$$

D'après cette définition, il sera facile de montrer que l'ensemble $\mathbb{R}$ des classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$, de même que l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$, est fermé relativement à l'addition, à la soustraction (définie comme l'opération inverse de l'addition) et à la multiplication, et que si on enlève de cet ensemble l'élément 0, l'ensemble qui en résulte est aussi fermé par rapport à la division (définie comme l'opération inverse de la multiplication).

La fermeture par rapport à la soustraction de l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$ autorise la définition suivante :

DÉFINITION 4.10. *Une suite de Cauchy à termes dans $\mathbb{Q}$ $\{u_i\}_{i=0}^{\infty}$ est dite « plus petite » qu'une suite de Cauchy à termes dans $\mathbb{Q}$ $\{v_i\}_{i=0}^{\infty}$ (en symboles : $\{u_i\}_{i=0}^{\infty} < \{v_i\}_{i=0}^{\infty}$), lorsque la série*

*de Cauchy à termes dans* $\mathbb{Q}$ $\{u_i - v_i\}_{i=0}^{\infty} = \{u_i\}_{i=0}^{\infty} - \{v_i\}_{i=0}^{\infty}$ *est négative. Si* $Cl\left(\{u_i\}_{i=0}^{\infty}\right)$ *et* $Cl\left(\{v_i\}_{i=0}^{\infty}\right)$ *sont deux nombres réelles (*$\{u_i\}_{i=0}^{\infty}$ *et* $\{v_i\}_{i=0}^{\infty}$ *étant deux suites de Cauchy à termes dans* $\mathbb{Q}$*), alors*

$$Cl\left(\{u_i\}_{i=0}^{\infty}\right) < Cl\left(\{v_i\}_{i=0}^{\infty}\right) \text{ si et seulement si } \{u_i\}_{i=0}^{\infty} < \{v_i\}_{i=0}^{\infty}$$

Le lecteur pourra démontrer tout seul, comme exercice, que cette définition est cohérente avec la définition 4.6. Cette définition étant donnée, il est facile de montrer que la relation $\leq$ ($<$ ou $=$) est une relation d'ordre autant sur $\mathbb{R}$ que sur l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$. La preuve en est facile et peut être laissée au lecteur comme exercice.

À partir des définitions précédentes, il est ensuite possible de démontrer que toute série de Cauchy à termes dans $\mathbb{Q}$, qui converge dans $\mathbb{Q}$ vers une certaine limite, se comporte, relativement à toutes les autres séries de la même sorte, comme la limite rationnelle de cette série se comporte dans $\mathbb{Q}$, relativement aux limites de ces autres séries. Et de là on en tirera, toujours à partir des définitions précédentes, que cela est aussi le cas des classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une certaine limite dans $\mathbb{Q}$. Dit d'une autre manière : les classes d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une certaine limite dans $\mathbb{Q}$, se comportent, relativement l'une à l'autre, comme les nombres rationnels se comportent relativement l'un à l'autre. La base de cette affirmation est donnée par le théorème suivant :

THÉORÈME 4.1. *Si les suites de Cauchy à termes dans* $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$ *et* $\{v_i\}_{i=0}^{\infty}$ *convergent dans* $\mathbb{Q}$*, respectivement vers les limites* $U$ *et* $V$*, alors :*

*(i) la suite* $\{u_i + v_i\}_{i=0}^{\infty} = \{u_i\}_{i=0}^{\infty} + \{v_i\}_{i=0}^{\infty}$ *converge dans* $\mathbb{Q}$ *vers la limite* $U + V$ *;*

*(ii) la suite* $\{K \cdot u_i\}_{i=0}^{\infty}$*,* $K$ *étant une constante rationnelle quelconque, converge dans* $\mathbb{Q}$ *vers la limite* $K \cdot U$ *;*

*(iii) la suite* $\{u_i \cdot v_i\}_{i=0}^{\infty} = \{u_i\}_{i=0}^{\infty} \cdot \{v_i\}_{i=0}^{\infty}$ *converge dans* $\mathbb{Q}$ *vers la limite* $U \cdot V$ *;*

*(iv) la suite* $\{u_i\}_{i=0}^{\infty}$ *est égale à la suite* $\{v_i\}_{i=0}^{\infty}$ *si et seulement si* $U = V$ *;*

*(v) la suite* $\{u_i\}_{i=0}^{\infty}$ *est plus petite que la suite* $\{v_i\}_{i=0}^{\infty}$ *si et seulement si* $U < V$*.*

**Preuve.** La preuve de ce théorème se compose évidemment de cinq preuves distinctes. Les voici :

(*i*) Comme $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent dans $\mathbb{Q}$ respectivement vers les limites $U$ et $V$, alors, quel que soit le nombre rationnel strictement positif $\varepsilon$, qu'on pourra supposer égal à $2\xi$, $\xi$ étant à son tour un nombre rationnel strictement positif quelconque, il y aura deux nombres naturels $n$ et $n'$, tels que

$$i > Max\{n, n'\} \Rightarrow \begin{cases} |U - u_i| < \xi \\ |V - v_i| < \xi \end{cases} \tag{96}$$

où, quels que soient les éléments $x$ et $y$ d'un ensemble totalement ordonné, le symbole « $Max\{x, y\}$ » indique le plus grand parmi $x$ et $y$ (la preuve de ce lemme est banale et peut être laissée aux lecteurs comme exercice). De là, il s'ensuit que

$$i > Max\{n, n'\} \Rightarrow |U - u_i| + |V - v_i| < 2\xi = \varepsilon$$

et donc, selon (93),

$$i > Max\{n, n'\} \Rightarrow |(U + V) - (u_i + v_i)| < 2\xi = \varepsilon$$

ce qui démontre (*i*).

(*ii*) Comme $\{u_i\}_{i=0}^{\infty}$ converge dans $\mathbb{Q}$ vers $U$, alors, quel que soit le nombre rationnel strictement positif $\varepsilon$, qu'on pourra supposer égal à $|K|\,\xi$, $\xi$ étant à son tour un nombre rationnel strictement positif quelconque, il y aura un nombre naturel $n$, tel que

$$i > n \Rightarrow |U - u_i| < \xi \tag{97}$$

Ceci étant posé, qu'on observe que pour tout couple de nombres rationnels $x$ et $y$

$$|x \cdot y| = \begin{cases} xy & \text{si } x \text{ et } y \text{ sont positifs ou négatifs à la fois} \\ & \text{ou si } x = 0 \text{ ou } y = 0 \\ -xy & \text{si } x \text{ et } y \text{ sont l'un strictement positif et l'autre négatif} \end{cases}$$

de sorte que, d'après (91), on aura :

$$|x \cdot y| = |x| \cdot |y| \tag{98}$$

d'où il suit que

$$|KU - Ku_i| = |K(U - u_i)| = |K| \cdot |U - u_i|$$

et donc, conformément à (97),

$$i > n \Rightarrow |K(U - u_i)| = |K| \cdot |U - u_i| < |K| \cdot \xi = \varepsilon$$

ce qui prouve (*ii*).

(*iii*) On observe d'abord que

$$\begin{aligned} |UV - u_i v_i| &= |u_i v_i - UV| \\ &= |(U - u_i) \cdot (V - v_i) + U(v_i - V) + V(u_i - U)| \end{aligned}$$

et donc, selon (93) et (98) :

$$|UV - u_i v_i| \leq |U - u_i| \cdot |V - v_i| + |U| \cdot |v_i - V| + |V| \cdot |u_i - U| \tag{99}$$

Or, comme $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent dans $\mathbb{Q}$, respectivement vers $U$ et $V$, alors, quels que soient les nombres rationnels strictement positif $\xi$ et $\eta$ et donc le nombre rationnel strictement positif $\varepsilon = \xi^2 + (|U| + |V|)\eta$, il y aura quatre nombres naturels $n$, $n'$, $m$ et $m'$, tels que

$$i > Max\{n, n', m, m'\} \Rightarrow \begin{cases} |U - u_i| < \xi \\ |V - v_i| < \xi \\ |U - u_i| = |u_i - U| < \eta \\ |V - v_i| = |v_i - V| < \eta \end{cases}$$

donc, d'après (99) :

$$i > Max\{n, n', m, m'\} \Rightarrow |UV - u_i v_i| < \xi^2 + (|U| + |V|)\eta = \varepsilon$$

ce qui prouve (*iii*).

(*iv.a*) Comme $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent dans $\mathbb{Q}$, respectivement vers $U$ et $V$, alors, quel que soit le nombre rationnel strictement positif $\varepsilon$, qu'on pourra supposer égal à $2\xi$, $\xi$ étant à son tour un nombre rationnel strictement positif quelconque, il y aura deux nombres naturels $n$ et $n'$, tels que

$$i > Max\{n, n'\} \Rightarrow \begin{cases} |U - u_i| < \xi \\ |V - v_i| = |v_i - V| < \xi \end{cases}$$

donc, d'après (93) :

$$i > Max\{n, n'\} \Rightarrow |(U - V) + (v_i - u_i)| < 2\xi = \varepsilon$$

et, si $U = V$,

$$i > Max\{n, n'\} \Rightarrow |0 - (u_i - v_i)| < 2\xi = \varepsilon$$

de sorte que la suite $\{u_i - v_i\}_{i=0}^{\infty}$ converge vers 0 dans $\mathbb{Q}$, c'est-à-dire qu'elle est nulle, et les suites $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ sont donc égales, conformément à la définition 4.4.

(*iv.b*) Commençons en prouvant que si une suite $\{w_i\}_{i=0}^{\infty}$ converge vers une limite $W$ dans $\mathbb{Q}$, alors la suite $\{W - w_i\}_{i=0}^{\infty}$ est nulle, c'est-à-dire qu'elle converge vers 0 dans $\mathbb{Q}$ : si $\{w_i\}_{i=0}^{\infty}$ converge vers $W$ dans $\mathbb{Q}$, alors, quel que soit le nombre rationnel strictement positif $\varepsilon$, il y a un nombre naturel $n$, tel que

$$i > n \Rightarrow |W - w_i| < \varepsilon$$

et donc

$$i > n \Rightarrow |0 - (W - w_i)| = |w_i - W| = |W - w_i| < \varepsilon$$

et donc la suite $\{W - w_i\}_{i=0}^{\infty}$ converge vers 0 dans $\mathbb{Q}$. De là, il suit que, comme les suites $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent dans $\mathbb{Q}$, respectivement vers $U$ et $V$, alors les suites $\{U - u_i\}_{i=0}^{\infty}$ et $\{V - v_i\}_{i=0}^{\infty}$ convergent toutes les deux vers 0 dans $\mathbb{Q}$. Donc, quel que soit le nombre rationnel strictement positif $\varepsilon$, qu'on pourra poser égal à $2\xi$, $\xi$ étant à son tour un nombre rationnel strictement positif quelconque, il y aura deux nombres naturels $n$ et $n'$, tels que

$$i > Max\{n, n'\} \Rightarrow \begin{cases} |U - u_i| < \xi \\ |V - v_i| = |v_i - V| < \xi \end{cases}$$

et donc, d'après (93) :

$$i > Max\{n, n'\} \Rightarrow |(U - u_i) - (V - v_i)| = |(U - V) + (v_i - u_i)| < \varepsilon$$

Mais, si $\{u_i\}_{i=0}^{\infty} = \{v_i\}_{i=0}^{\infty}$ ceci n'est possible que si $U - V = 0$ et donc $U = V$.

(*v.a)* On suppose d'abord que $U < V$. On aura alors un nombre rationnel strictement positif $W$, tel que $V - U = W$. Or, comme les suites $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent respectivement vers $U$ et $V$ dans $\mathbb{Q}$, il y aura alors deux nombres naturels $n$ et $n'$, tels que

$$i > Max\{n, n'\} \Rightarrow \begin{cases} |U - u_i| = |u_i - U| < \frac{W}{2} \\ |V - v_i| < \frac{W}{2} \end{cases}$$

et donc, d'après (93) :

$$i > Max\{n, n'\} \Rightarrow |(V - U) + (u_i - v_i)| = |W + (u_i - v_i)| < W$$

ce qui est possible seulement si

$$i > Max\{n, n'\} \Rightarrow (u_i - v_i) < 0$$

donc la suite $\{u_i - v_i\}_{i=0}^{\infty}$ est négative et ainsi, selon la définition 4.10,

$$\{u_i\}_{i=0}^{\infty} < \{v_i\}_{i=0}^{\infty}$$

(*v.b*) Comme les suites $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$ convergent respectivement vers $U$ et $V$ dans $\mathbb{Q}$, il suit, comme on l'a montré en prouvant (*iv.b*), que les suites $\{U - u_i\}_{i=0}^{\infty}$ et $\{V - v_i\}_{i=0}^{\infty}$ sont nulles. Or, si ceci est le cas et $\{u_i\}_{i=0}^{\infty} < \{v_i\}_{i=0}^{\infty}$, alors, quel que soit le nombre rationnel positif $\varepsilon$, qu'on pourra poser égal à $2\xi$, $\xi$ étant à son tour un nombre rationnel strictement positif quelconque, il y aura trois nombres naturels $n$, $n'$ et $m$, tels que

$$i > Max\{n, n', m\} \Rightarrow \begin{cases} |U - u_i| = |u_i - U| < \xi \\ |V - v_i| < \xi \\ u_i - v_i < 0 \end{cases}$$

c'est-à-dire

$$i > Max\{n, n', m\} \Rightarrow \begin{cases} |(u_i - U) + (V - v_i)| = |(V - U) + (u_i - v_i)| < 2\xi = \varepsilon \\ u_i - v_i < 0 \end{cases}$$

ce qui est possible seulement si $V - U > 0$, ou bien $U < V$. □

À partir de ce théorème et des définitions de l'addition, de la multiplication et de la relation $\leq$ sur $\mathbb{R}$, il est facile de démontrer que le sous-ensemble de $\mathbb{R}$ formé par toutes les classes

d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ forme, avec les opérations $+$ et $\cdot$ et la relation $\leq$, un corps commutatif totalement ordonné. Encore une fois la démonstration complète de cette affirmation est laissée au lecteur comme exercice. Les classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ forment donc un sous-ensemble de $\mathbb{R}$ qui, comme on le dit, est « isomorphe » à $\mathbb{Q}$ et peut ainsi être identifié formellement avec ce dernier ensemble (pris avec toutes les opérations, relations et fonctions définies sur lui). Cela nous permet de comprendre en quel sens on peut dire que l'ensemble $\mathbb{R}$, défini en accord à la 4.5, est une extension de $\mathbb{Q}$. Si on pense donc $\mathbb{Q}$ comme un sous-ensemble de $\mathbb{R}$, les opérations et la relation d'ordre définies sur $\mathbb{R}$ s'appliquent automatiquement aux éléments de $\mathbb{R}$ qui sont aussi des éléments de $\mathbb{Q}$. Faire opérer et/ou comparer des rationnels avec des réels revient donc à faire opérer et/ou comparer des réels entre eux. Du fait qu'on a démontré que les suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ se comportent les unes par rapport aux autres comme leurs limites rationnelles se comportent les unes par rapport aux autres, et que deux suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ sont égales si et seulement si leurs limites sont égales, et finalement du fait qu'il est facile de démontrer (et le lecteur pourra le faire tout seul sans aucune difficulté) que si $K$ est une constante rationnelle quelconque, alors la suite à termes dans $\mathbb{Q}\,\{K\}_{i=0}^{\infty} = K, K, K, \ldots$ est une suite de Cauchy, et converge vers $K$ dans $\mathbb{Q}$, il suit en fait qu'il est parfaitement légitime d'identifier chaque nombre réel $\mathfrak{q}$ qui appartient à $\mathbb{Q}$ avec la classe d'équivalence $Cl\,(\{\mathfrak{q}\}_{i=0}^{\infty})$. C'est ce qu'on appelle « principe de plongement de $\mathbb{Q}$ dans $\mathbb{R}$ ». On se servira de ce principe dans la preuve du théorème 4.2.

Pour comprendre maintenant en quel sens on peut traiter l'ensemble $\mathbb{R}$ défini comme ci-dessus comme un ensemble de nombres, il suffit seulement de montrer que l'extension qui conduit de $\mathbb{Q}$ à $\mathbb{R}$ conserve la propriété du quadruplet $< \mathbb{Q}, +, \cdot, \leq >$ d'être un corps commutatif totalement ordonné, c'est-à-dire que le quadruplet $< \mathbb{R}, +, \cdot, \leq >$ est, lui aussi, un corps commutatif totalement ordonné. La démonstration de ceci n'est pas difficile, mais elle est nécessairement longue. Le lecteur, qui aura déjà démontré que $\mathbb{R}$ est fermé par rapport à la somme, la soustration et le produit, et que $\mathbb{R} - \{0\}$ est fermé par rapport à la division n'aura aucune difficulté à compléter cette preuve, en s'appuyant, si nécessaire, sur le théorème 5.1. Quant à moi, je me limiterai à observer que, comme le théorème 5.1 nous dit que deux suites de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$, convergent vers la même limite $U$ dans $\mathbb{Q}$ seulement si elles sont égales, on pourra conjecturer que l'élément neutre de l'addition dans $\mathbb{R}$ est l'élément 0 et l'élément neutre de la multiplication dans $\mathbb{R}$ est la classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers 1 dans $\mathbb{Q}$. Le prouver ne sera pas, ensuite, très difficile.

Une fois qu'il aura prouvé que $< \mathbb{R}, +, \cdot, \leq >$ est un corps commutatif totalement ordonné, le lecteur ne devrait plus avoir de difficultés à accepter le fait que la définition 4.5 n'est nullement paradoxale. Pourtant, rien dans ce qu'on a dit jusqu'ici, ne nous assure ni qu'une suite à termes dans $\mathbb{Q}$ converge vers une limite dans $\mathbb{R}$ si et seulement si c'est une suite de Cauchy, ni, *a fortiori*, qu'une suite à termes dans $\mathbb{R}$ converge vers une limite dans $\mathbb{R}$ si et seulement si c'est une suite de Cauchy. Une manière simple et fort naturelle de démontrer la première équivalence est de démontrer que toute suite de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$, converge vers $Cl(\{u_i\}_{i=0}^{\infty})$ dans $\mathbb{R}$, et de démontrer ensuite, en employant l'argument qu'on a utilisé ci-dessus pour des suites à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$, qu'une suite à termes dans $\mathbb{Q}$ qui converge vers une limite dans $\mathbb{R}$ est une suite de Cauchy. Comme $\mathbb{R}$ est une extension de $\mathbb{Q}$, une suite à termes dans $\mathbb{Q}$ est en même temps une suite à termes dans $\mathbb{R}$, et donc il ne sera pas difficile, à partir des définitions précédentes, de comprendre ce qu'on doit entendre lorsqu'on dit qu'une suite à termes dans $\mathbb{Q}$ converge vers une limite dans $\mathbb{R}$. Il suffira de spécifier que

la distance entre deux éléments de $\mathbb{R}$, à laquelle on réfère implicitement une telle convergence, est celle qui est donnée par la valeur absolue de la différence de ces termes. Ce n'est pourtant qu'après qu'on aura donné de manière explicite des définitions convenables, qu'il sera possible de prouver rigoureusement la première des deux équivalences précédentes, et surtout l'implication non banale qui y intervient : si $\{u_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{Q}$, alors elle converge vers $Cl(\{u_i\}_{i=0}^{\infty})$ dans $\mathbb{R}$. Bien que cette preuve ne permette pas encore de conclure qu'une suite à termes dans $\mathbb{R}$ converge vers une limite dans $\mathbb{R}$ si et seulement si c'est une suite de Cauchy, elle fait partie de la preuve habituellement donnée pour ce théorème plus général, qui est le seul qui nous intéresse vraiment (car il comprend la première équivalence comme une cas particulier). C'est exactement cette preuve, pour ainsi dire standard, que j'exposerai ci-dessous. Le lecteur pourra vérifier qu'elle se sert, comme d'un lemme, du théorème qui affirme que si $\{u_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{Q}$, alors elle converge vers $Cl(\{u_i\}_{i=0}^{\infty})$ dans $\mathbb{R}$.

Je commencerai par étendre à $\mathbb{R}$ les définitions 2.4, 2.6 et 4.2. Pour ceci, on pensera $\mathbb{R}$ comme une extension de $\mathbb{Q}$, et on notera les éléments de $\mathbb{R}$ qui appartiennent à $\mathbb{Q}$ par le même symbole par lequel ils sont notés en tant qu'éléments de $\mathbb{Q}$. On a déjà adopté cette convention pour le symbole « 0 » et on ne fera donc que la généraliser. Ainsi, pour ne faire qu'un exemple, le symbole « 1 » référé à un élément de $\mathbb{R}$ indiquera la classe d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers le nombre rationnel 1 dans $\mathbb{Q}$. On aura alors, tout naturellement, les définitions suivantes (où la valeur absolue d'un élément de $\mathbb{R}$ est supposée définie de manière analogue à la valeur absolue d'un élément de $\mathbb{Q}$) :

Définition 4.11. *On dit qu'une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ converge vers $R$* dans $\mathbb{R}$ *si et seulement s'il y a un élément $R$ de $\mathbb{R}$, tel que, pour tout $\varepsilon$ appartenant à $\mathbb{R}$, tel que $0 < \varepsilon$, il y a un nombre naturel $n$, tel que, si $i > n$, alors $|R - r_i| < \varepsilon$ ; en symboles :*

$$(\varepsilon \in \mathbb{R}) \Rightarrow [0 < \varepsilon \Rightarrow (\exists n \in \mathbb{N} \text{ tel que } i > n \Rightarrow |R - r_i| < \varepsilon)]$$

*Si une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ converge vers $R$ dans $\mathbb{R}$, alors on dit que $R$ est la limite de $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$. Si une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{Q}$ est telle qu'il n'y a aucun élément $R$ de $\mathbb{R}$ qui satisfait à la condition précédente, alors on dit que cette suite ne converge vers aucune limite dans $\mathbb{R}$ ou est divergente dans $\mathbb{R}$.*

Définition 4.12. *On dit qu'une série $\sum_{i=0}^{\infty} r_i$ à termes dans $\mathbb{R}$ converge vers $R$ dans $\mathbb{R}$ si et seulement si la suite $\left\{\sum_{i=0}^{j} r_i\right\}_{j=0}^{\infty}$ de ses réduites partielles (qui sera alors une suite à termes dans $\mathbb{R}$) converge vers $R$ dans $\mathbb{R}$. Si une série $\sum_{i=0}^{\infty} r_i$ à termes dans $\mathbb{R}$ converge vers $R$ dans $\mathbb{R}$, alors on dit que $R$ est la limite de $\sum_{i=0}^{\infty} r_i$ dans $\mathbb{R}$. Si une série $\sum_{i=0}^{\infty} r_i$ à termes dans $\mathbb{R}$ est telle qu'il n'y a aucun élément $R$ de $\mathbb{R}$ qui satisfait à la condition précédente, alors on dit que cette série ne converge vers aucune limite dans $\mathbb{R}$ ou est divergente dans $\mathbb{R}$.*

Définition 4.13. *On dit qu'une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ est une suite de Cauchy si et seulement si pour tout $\varepsilon$ appartenant à $\mathbb{R}$, tels que $0 < \varepsilon$, il y a un nombre naturel $n$, tel que, si $i > n$ et $j \in \mathbb{N}$, alors $|r_{i+j} - r_i| < \varepsilon$ ; en symboles :*

$$(\varepsilon \in \mathbb{R}) \Rightarrow [0 < \varepsilon \Rightarrow (\exists n \in \mathbb{N} \text{ tel que } [(i > n) \wedge (j \in \mathbb{N})] \Rightarrow |r_{i+j} - r_i| < \varepsilon)]$$

*On dit ensuite qu'une série $\sum_{i=0}^{\infty} r_i$ à termes dans $\mathbb{R}$ est une série de Cauchy si et seulement si la suite $\left\{\sum_{i=0}^{j} r_i\right\}_{j=0}^{\infty}$ à termes dans $\mathbb{R}$ est une suite de Cauchy.*

À partir des définitions 4.11 et 4.13, on peut ensuite démontrer le théorème annoncé :

THÉORÈME 4.2. *Une série à termes dans $\mathbb{R}$ est convergente vers une certaine limite $R$ dans $\mathbb{R}$ si et seulement si c'est une suite de Cauchy.*

**Preuve.** Pour prouver que si une série à termes dans $\mathbb{R}$ est convergente vers une certaine limite $R$ dans $\mathbb{R}$ alors c'est une suite de Cauchy, il suffit de répéter le même argument déjà utilisé, dans ce même but, pour des suites à termes dans $\mathbb{Q}$. Le lecteur pourra rédiger explicitement cette preuve à titre d'exercice. La preuve de l'implication réciproque est par contre un peu plus difficile. Une manière fort naturelle de la conduire est de montrer comment on peut construire, à partir de n'importe quelle suite de Cauchy à termes dans $\mathbb{R}$, une classe d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$ (et donc un nombre réel) qui soit la limite de la suite donnée. C'est ce qu'on fera ci-dessous.

On commencera par démontrer deux lemmes. Voici le premier

*Lemme 1* Quel que soit le nombre réel $Cl(\{u_i\}_{i=0}^{\infty})$, toute suite de Cauchy à termes dans $\mathbb{Q}$ (et donc dans $\mathbb{R}$, $\mathbb{Q}$ étant, comme on l'a vu, un sous-ensemble de $\mathbb{R}$), qui appartient à $Cl(\{u_i\}_{i=0}^{\infty})$ converge vers $Cl(\{u_i\}_{i=0}^{\infty})$ dans $\mathbb{R}$.

Comme, quelles que soient les suites de Cauchy à termes dans $\mathbb{Q}$, $\{u_i\}_{i=0}^{\infty}$ et $\{v_i\}_{i=0}^{\infty}$, $\{u_i\}_{i=0}^{\infty} = \{v_i\}_{i=0}^{\infty}$ si et seulement si la classe $Cl(\{u_i\}_{i=0}^{\infty})$ est identique à la classe $Cl(\{v_i\}_{i=0}^{\infty})$, pour prouver ce lemme, il suffit de prouver que $\{u_i\}_{i=0}^{\infty}$ converge vers $Cl(\{u_i\}_{i=0}^{\infty})$ dans $\mathbb{R}$. Pour plus de simplicité appelons « $r$ » la classe $Cl(\{u_i\}_{i=0}^{\infty})$. Il s'agit alors de prouver que $\{u_i\}_{i=0}^{\infty}$ converge vers $r$ dans $\mathbb{R}$.

Comme $\{u_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{Q}$, il y aura, pour tout nombre rationnel strictement positif $\eta$, un nombre naturel $n$, tel que, pour tout nombre naturel $p$,

$$i > n \Rightarrow |u_i - u_{i+p}| < \eta \tag{100}$$

Soit alors $\mu$ un nombre naturel déterminé, plus grand que $n$ quel que soit le nombre naturel $m$ plus grand que $\mu$, on aura alors

$$|u_\mu - u_m| < \eta$$

c'est-à-dire

$$-\eta < u_\mu - u_m < \eta$$

et donc

$$\begin{aligned} u_\mu - u_m + \eta &= (u_\mu + \eta) - u_m > 0 \\ \eta - u_\mu + u_m &= (\eta - u_\mu) + u_m > 0 \end{aligned} \tag{101}$$

Considérons alors les suites

$$\{(u_\mu + \eta) - u_m\}_{m=0}^{\infty} \qquad \text{et} \qquad \{(\eta - u_\mu) + u_m\}_{m=0}^{\infty} \tag{102}$$

Il est facile de voir que ces suites sont des suites à termes dans $\mathbb{Q}$, car $\eta$, $u_\mu$ et $u_m$ $(m = 0, 1, 2, ...)$ sont tous des nombres rationnels et $\mathbb{Q}$ est fermé par rapport à l'addition et à la soustraction. On a déjà observé, de surcroît, que pour toute constante $K$, dans $\mathbb{Q}$, la suite $\{K\}_{m=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{Q}$, donc, $\mu$ etant un nombre naturel déterminé, les suites

$$\{u_\mu + \eta\}_{m=0}^{\infty} \qquad \text{et} \qquad \{\eta - u_\mu\}_{m=0}^{\infty}$$

sont des suites de Cauchy à termes dans $\mathbb{Q}$. Mais aussi la suite $\{u_m\}_{m=0}^{\infty}$ est par hypothèse une suite de Cauchy à termes dans $\mathbb{Q}$. Comme

$$\begin{aligned} \{(u_\mu + \eta) - u_m\}_{m=0}^{\infty} &= \{u_\mu + \eta\}_{m=0}^{\infty} - \{u_m\}_{m=0}^{\infty} \\ \{(\eta - u_\mu) + u_m\}_{m=0}^{\infty} &= \{\eta - u_\mu\}_{m=0}^{\infty} + \{u_m\}_{m=0}^{\infty} \end{aligned} \tag{103}$$

et, comme l'ensemble des suites de Cauchy à termes dans $\mathbb{Q}$ est fermé par rapport à l'addition et à la soustraction, il en résulte que les suites (102) sont toutes les deux des suites de Cauchy à termes dans $\mathbb{Q}$. Donc les classes d'équivalence

$$Cl\left(\{(u_\mu+\eta)-u_m\}_{m=0}^{\infty}\right) \qquad \text{et} \qquad Cl\left(\{(\eta-u_\mu)+u_m\}_{m=0}^{\infty}\right)$$

sont deux nombres réels, disons respectivement $s$ et $s'$, et de (101), il suit que ces nombres sont tous les deux positifs. Or, de (103), il suit :

$$\begin{aligned} Cl\left(\{(u_\mu+\eta)-u_m\}_{m=0}^{\infty}\right) &= Cl\left(\{u_\mu+\eta\}_{m=0}^{\infty}-\{u_m\}_{m=0}^{\infty}\right) \\ &= Cl\left(\{u_\mu+\eta\}_{m=0}^{\infty}\right)-Cl\,\{u_m\}_{m=0}^{\infty} \\ Cl\left(\{(\eta-u_\mu)+u_m\}_{m=0}^{\infty}\right) &= Cl\left(\{\eta-u_\mu\}_{m=0}^{\infty}+\{u_m\}_{m=0}^{\infty}\right) \\ &= Cl\left(\{\eta-u_\mu\}_{m=0}^{\infty}\right)+Cl\,\{u_m\}_{m=0}^{\infty} \end{aligned}$$

Il suffira alors de se réclamer du principe de plongement de $\mathbb{Q}$ dans $\mathbb{R}$ pour conclure que :

$$\begin{aligned} s &= u_\mu+\eta-r\geq 0 \\ s' &= \eta-u_\mu+r\geq 0 \end{aligned}$$

c'est-à-dire

$$\begin{aligned} r-u_\mu &\leq \eta \\ r-u_\mu &\geq -\eta \end{aligned}$$

ou

$$|r-u_\mu|\leq\eta$$

Quel que soit le nombre réel strictement positif $\varepsilon$, il suffira alors de prendre un nombre rationnel strictement positif $\eta$ plus petit que $\varepsilon$, et de choisir un nombre naturel $n$ qui satisfait à (100), pour en conclure que

$$i>n\Rightarrow|r-u_i|=|u_i-r|<\varepsilon$$

ce qui nous permettrait de conclure que la suite de Cauchy à termes dans $\mathbb{Q}\,\{u\}_{i=0}^{\infty}$ converge vers $r$ dans $\mathbb{R}$, ce qu'il s'agissait de démontrer.

Rien dans ce qu'on a dit jusqu'ici nous assure pourtant que, quel que soit le nombre réel strictement positif $\varepsilon$, il y a un nombre rationnel strictement positif $\eta$ plus petit que $\varepsilon$, ou bien, comme on le dit, que les rationnels sont denses dans les réels. Avant de conclure la preuve de notre lemme, il faut donc démontrer qu'il en est bien ainsi. Ceci peut se faire de la manière suivante.

Quel que soit le nombre réel strictement positif $\varepsilon$, il sera une classe d'équivalence $Cl\,(\{v_i\}_{i=0}^{\infty})$, la suite $\{v_i\}_{i=0}^{\infty}$ étant une suite de Cauchy à termes dans $\mathbb{Q}$ strictement positive. Comme cette suite est positive, quel que soit le nombre rationnel strictement positif $\xi$, il y aura alors, par définition, un nombre naturel $n$, tel que

$$i>n\Rightarrow v_i>-\xi$$

mais, comme elle n'est pas nulle, il y aura aussi un nombre rationnel strictement positif $\zeta$, tel que, quel que soit $i$,

$$|0-v_i|=|v_i|\geq\zeta$$

c'est-à-dire

$$v_i\geq\zeta \qquad \text{ou} \qquad v_i\leq-\zeta$$

De là il suit que, quel que soit le nombre naturel $i$, la suite est telle que

$$v_i\geq\zeta$$

De la densité de $\mathbb{Q}$, il suit alors qu'il y a un nombre rationnel strictement positif $\eta$ plus petit que $\zeta$, et que pour tout nombre naturel $i$, il est possible de prendre un nombre rationnel strictement positif $w_i$ tel que

$$v_i - w_i = \eta$$

La suite

$$\{v_i - w_i\}_{i=0}^{\infty} = \{\eta\}_{i=0}^{\infty}$$

est donc une suite à termes constants dans $\mathbb{Q}$. Elle sera donc une suite de Cauchy qui converge vers la limite $\eta$ dans $\mathbb{Q}$, et comme

$$\{v_i - w_i\}_{i=0}^{\infty} = \{\eta\}_{i=0}^{\infty} < \{v_i\}_{i=0}^{\infty}$$

il s'ensuit que

$$\eta < \varepsilon$$

comme il s'agissait de démontrer. Cela conclut la preuve du lemme 1.

Considérons maintenant une suite de Cauchy à termes dans $\mathbb{R}$, $\{r_j\}_{j=0}^{\infty}$. Quel que soit le nombre naturel $j$, le terme $r_j$ de cette suite sera une classe d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$, disons $Cl\left([\{u_i\}_{i=0}^{\infty}]_j\right)$, les $[\{u_i\}_{i=0}^{\infty}]_j$ $(j = 0, 1, 2, ...)$ étant justement des suites de Cauchy à termes dans $\mathbb{Q}$. Du lemme 1, il suit que, quel que soit le nombre naturel $j$, la suite $[\{u_i\}_{i=0}^{\infty}]_j$ converge vers $r_j$ dans $\mathbb{R}$. Donc, quels que soient le nombre naturel $j$ et le nombre réel strictement positif $\varepsilon$, il y aura un nombre naturel $N_j$ tel que

$$i > N_j \Rightarrow \left| r_j - [u_i]_j \right| < \varepsilon$$

Or, quel que soit $j$, les termes $[u_i]_j$ $(i = N_j+1, N_j+2, ...)$ des suites $[\{u_i\}_{i=0}^{\infty}]_j$ sont des nombres rationnels. Donc, si pour chaque nombre naturel $j$, on choisit ainsi une valeur convenable de $i$ plus grande que $N_j$, disons $\nu_j$, on pourra former une suite $\left\{u_{\nu_j}\right\}_{j=0}^{\infty}$ dont les termes sont tous des rationnels, dont la distance de $r_j$ est, quel que soit $j$, plus petite que $\varepsilon$. Pour plus de simplicité posons, pour chaque $j$, $u_{\nu_j} = \mathfrak{q}_j$. Le second lemme qu'il faut prouver est alors le suivant :

*Lemme 2* La suite à termes dans $\mathbb{Q}$ $\{\mathfrak{q}_j\}_{j=0}^{\infty}$ est une suite de Cauchy.

La preuve de ce lemme est fort simple. Il suffit d'observer que si $m$ est un nombre naturel quelconque plus grand que $j$, alors, à cause de ce qu'on vient de dire et du fait que la suite $\{r_j\}_{j=0}^{\infty}$ est une suite de Cauchy, quel que soit le nombre réel strictement positif $\varepsilon$, il y aura trois nombres naturels $n, n'$ et $n''$, tels que

$$\begin{aligned} j &> n \Rightarrow |\mathfrak{q}_j - r_j| < \varepsilon \\ j &> n' \Rightarrow |r_j - r_m| < \varepsilon \\ j &> n'' \Rightarrow |\mathfrak{q}_m - r_m| = |r_m - \mathfrak{q}_m| < \varepsilon \end{aligned}$$

et donc

$$j > Max(n, n', n'') \Rightarrow \left\{ \begin{array}{rcl} |\mathfrak{q}_j - \mathfrak{q}_m| & = & |(\mathfrak{q}_j - r_j) + (r_j - r_m) + (r_m - \mathfrak{q}_m)| \\ & \leq & |\mathfrak{q}_j - r_j| + |r_j - r_m| + |r_m - \mathfrak{q}_m| < 3\varepsilon \end{array} \right.$$

Comme $3\varepsilon$ est un nombre réel strictement positif quelconque, ceci conclut la démonstration du lemme 2.

Ce lemme ayant été démontré, il suffit, pour conclure la preuve du théorème, de démontrer que la suite de Cauchy à termes dans $\mathbb{R}$ $\{r_j\}_{j=0}^{\infty}$ converge vers $Cl\left(\{\mathfrak{q}_j\}_{j=0}^{\infty}\right)$ dans $\mathbb{R}$. Cela est pourtant, à ce point, fort facile.

Qu'on appelle, par simplicité, cette dernière classe d'équivalence « $R$ ». Alors, par le lemme 1, la suite de Cauchy à termes dans $\mathbb{Q}\left\{\mathfrak{q}_j\right\}_{j=0}^{\infty}$ converge vers $R$ dans $\mathbb{R}$, donc, pour tout nombre réel strictement positif $\varepsilon$, il y a un nombre naturel $n'''$, tel que

$$j > n''' \Rightarrow |R - \mathfrak{q}_j| < \varepsilon$$

Mais, quel que soit $\varepsilon$, on vient de voir qu'il y a aussi un nombre naturel $n$ tel que

$$j > n \Rightarrow |\mathfrak{q}_j - r_j| < \varepsilon$$

et donc

$$j > Max(n, n''') \Rightarrow \left\{ \begin{array}{rcl} |R - r_j| & = & |(R - \mathfrak{q}_j) + (\mathfrak{q}_j - r_j)| \\ & \leq & |R - \mathfrak{q}_j| + |\mathfrak{q}_j - r_j| < 2\varepsilon \end{array} \right.$$

ce qui, $2\varepsilon$ étant un nombre réel strictement positif quelconque, conclue la preuve. □

NOTE HISTORIQUE 6.13. En 1872 parurent cinq travaux de cinq auteurs différents, tous consacrés à la construction de l'ensemble des nombres réels à partir de l'ensemble des nombres rationnels, ou, plus précisément, à la définition des nombres irrationnels (les nombres réels non rationnels) en termes de nombres rationnels.

A. M. Kossac, dans *Die Elemente der Arithmetik*, exposa d'abord la théorie des irrationnels qu'il avait apprise par Weierstrass, dont il avait suivi les leçons à l'université de Berlin (cf. la note historique 6.7). En réalité Weierstrass avait déjà abordé ce sujet, dans ses cours d'analyse, dès 1860, mais il n'avait jamais rien publié sur l'argument, et ne publiera jamais rien par la suite (on n'a même pas retrouvé les notes de ses cours sur ce sujet) ; il accueillit de surcroît assez froidement la publication de Kossac où il ne reconnut pas précisément ses idées. Les leçons berlinoises de Weierstrass, différemment assimilées par ses étudiants et ses collègues, furent pourtant, sans aucun doute, à l'origine des différentes propositions de définition de $\mathbb{R}$.

*Grosso modo*, la même théorie reconstruite par Kossac fut aussi présentée, la même année, par C. Méray, dans son *Nouveau précis d'analyse infinitésimale*. Celui-ci avait d'ailleurs déjà présentée l'essentiel de sa théorie, en 1869, dans un article paru dans la *Revue des Sociétés Savantes*.

Toujours en 1872, dans le premier paragraphe d'un article consacré aux séries trigonométriques, « Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen » (Sur l'extension d'une proposition de la théorie des séries trigonométriques), Cantor revint assez rapidement sur la définition de Weierstrass, dont il proposa une nouvelle formulation, faisant intervenir les suites de Cauchy de rationnels. La définition de Cantor fut ensuite exposée à nouveau, dans une formulation plus précise, en 1883 dans un article publié sur les *Mathematische Annalen*.

Une théorie très proche de celle de Cantor fut présentée, toujours en 1872, par E. Heine, dans son article « Die Elemente der Funtionenlehre » (Les éléments de la théorie des fonctions). L'article de Cantor de 1872 se présentait d'ailleurs, déjà comme un commentaire d'un article précédent de Heine.

Finalement, une théorie assez différente, autant de celle de Weierstrass que de sa reformulation par Cantor et Heine, fut présentée, toujours en 1872, par R. Dedekind dans le mémoire *Stetigkeit und Irrationale Zahlen* (Continuité et nombres irrationnels). Je reviendrais plus loin sur la théorie de Dedekind (cf. en particulier la note historique 6.15). Ici, je ne voudrais faire que quelques courtes observations à propos des théories de Weierstrass et Cantor.

L'idée essentielle de Weierstrass était de définir un nombre réel positif à partir de la considération des suites $\{u_i\}_{i=0}^{\infty}$ des nombres rationnels telles que la suite $\left\{\sum_{i=0}^{j} u_i\right\}$ de toutes les sommes d'un nombre fini quelconque de termes de ces suites soit supérieurement bornée dans $\mathbb{Q}^+$ par un nombre naturel strictement positif. Parmi ces suites, Weierstrass propose en particulier de considérer des suites dont les termes ne soient que des fractions de l'unité et il propose d'associer à chacune de ces suites un « nombre » qui est totalement déterminé par cette même suite. On observe que ce nombre n'est pas défini comme la somme d'une série telle que $\sum_{i=0}^{\infty} u_i$, ce qui aurait causé une circularité, en demandant de s'assurer de l'existence de cette somme avant d'avoir défini l'ensemble auquel elle appartient. L'idée de Weierstrass est plutôt celle de considérer le « nombre » associé aux suites $\{u_i\}_{i=0}^{\infty}$ comme un objet dont les propriétés relationnelles, vis-à-vis d'autres objets de la même nature, sont complètement déterminées par les propriétés de la suite à laquelle il est associé. Pour reconnaître cet objet comme un nombre, en particulier un nombre réel positif, Weierstrass n'a ainsi qu'à définir convenablement une égalité, une relation d'ordre, une addition et une multiplication sur ces suites, à partir évidemment des relations et des opérations définies sur l'ensemble des nombres rationnels positifs.

Comme on le voit, la théorie de Weierstrass est fort similaire à celle qu'on a exposée ci-dessus et qu'on a attribuée à Cantor. La considération des suites de Cauchy de rationnels permet tout simplement d'alléger la construction et de la rendre plus immédiate. Cantor introduit d'abord ces suites sous le nom de « suites fondamentales », tout en les définissant comme on l'a fait dans la définition 4.2. Il définit ensuite, exactement comme on l'a fait ci-dessus, une égalité, une relation d'ordre, une addition et une multiplication sur les suites fondamentales, mais, au lieu de définir un nombre réel comme une classe d'équivalence de suites fondamentales (comme on le fait aujourd'hui avec un gain considérable de précision et de clarté) il le définit, à la manière de Weierstrass (auquel il reconnaît le mérite d'avoir été le premier à éviter la circularité qu'on a évoquée ci-dessus), comme un « nombre » associé à ces suites, qu'il appelle « limite » de celles-ci.

**Lectures possibles** : J. Cavaillès, « Remarques sur la formation de la théorie abstraite des ensembles », *in* J. Cavaillès, *Philosophie mathématique*, Hermann, Paris, 1962, pp. 23-176.

**4.2. Définition implicite des réels : l'axiome de Dedekind.** Dans le paragraphe précédent, on a montré que les suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ se comportent, relativement les unes aux autres, comme leurs limites rationnelles se comportent relativement les unes aux autres. Si on considère $\mathbb{Q}$ comme un sous-ensemble de $\mathbb{R}$ et qu'on définit ce dernier ensemble en accord avec la définition 4.5, ces limites ne sont pourtant que des classes d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$. Remplacer toutes les suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ par leurs limites rationnelles ne signifie alors, à la rigueur, que les remplacer par des classes d'équivalence de suites de Cauchy à termes dans $\mathbb{Q}$. Si on veut penser le passage d'une de ces suites à sa limite rationnelle comme un passage d'une suite à un objet mathématique qui n'est ni une suite ni une classe de suites et, tout de même, définir $\mathbb{R}$ en accord avec la définition 4.5, il faut donc penser $\mathbb{Q}$ non pas comme un sous-ensemble de $\mathbb{R}$, mais comme un ensemble indépendant, dont on pourrait éventuellement montrer qu'il est isomorphe avec un sous-ensemble de $\mathbb{R}$. Le remplacement de toute suite de Cauchy à termes dans $\mathbb{Q}$ (ou de quelques-unes de ces suites) par

sa limite rationnelle pourrait alors être pensée comme un remplacement d'un sous-ensemble de $\mathbb{R}$ même par un autre ensemble, défini de manière indépendante, dont on pourrait montrer qu'il est isomorphe à l'ensemble qu'il substitue. Pourtant, pour rendre cette substitution légitime, relativement à l'ensemble $\mathbb{R}$ pris comme un tout, il faudrait encore expliquer comment les nombres rationnels (définis de manière indépendante) se comportent face aux suites de Cauchy à termes dans $\mathbb{Q}$ qui divergent dans $\mathbb{Q}$. Ceci est naturellement possible, et le lecteur ne sera pas surpris d'apprendre que cette explication peut être telle qu'aucun des résultats trouvés dans $\mathbb{R}$ pour les opérations définies sur cet ensemble, une fois qu'on a opéré la substitution indiquée, ne contredit ceux trouvés dans $\mathbb{Q}$ pour les mêmes opérations restreintes à $\mathbb{Q}$.

Pourtant, si on décide de distinguer entre les classes d'équivalence des suites de Cauchy à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$ et les limites rationnelles de ces suites, il est beaucoup plus naturel de distinguer aussi entre les (classes d'équivalence des) suites de Cauchy à termes dans $\mathbb{Q}$ qui divergent dans $\mathbb{Q}$ et quelque chose qu'on pourrait identifier avec leur limite non rationnelle, ou « irrationnelle », comme on le dit en général. Pour ce faire, il faut pourtant penser $\mathbb{R}$ non plus comme un ensemble de classes d'équivalence de suites à termes dans $\mathbb{Q}$ (c'est-à-dire comme un ensemble d'ensembles de sous-ensembles de $\mathbb{Q}$), mais comme un ensemble qui contient, à côté des éléments de $\mathbb{Q}$, aussi d'autres éléments qui peuvent être traités comme les limites dans $\mathbb{R}$ des suites de Cauchy à termes dans $\mathbb{Q}$, qui divergent dans $\mathbb{Q}$. Pour ce faire, ou peut, ou bien chercher une manière d'étendre $\mathbb{Q}$, distincte de celle qu'on a adoptée ci-dessus, ou bien définir directement, sans aucunement se réclamer de la donnée préalable de $\mathbb{Q}$ (et donc d'aucune suite à termes dans $\mathbb{Q}$), un nouvel ensemble d'objets qu'on peut penser comme des nombres, et tel qu'un sous-ensemble convenable d'un tel ensemble soit isomorphe à $\mathbb{Q}$, et le faire de sorte qu'il demeure possible d'écrire une égalité entre toute suite de Cauchy à termes dans $\mathbb{Q}$ et un élément de ce nouvel ensemble. C'est justement le but de la définition axiomatique de $\mathbb{R}$ qu'on va exposer ci-dessous.

Comme on a déjà vu que l'ensemble $\mathbb{N}$ R, lorsqu'il est défini d'après la définition 4.5 (c'est-à-dire à la manière de Cantor), forme, avec les opérations $+$ et $\cdot$ et la relation $\leq$ définies comme ci-dessus, un corps commutatif totalement ordonné, la chose la plus naturelle à faire est de définir d'emblée l'ensemble $\mathbb{R}$ comme un ensemble satisfaisant en même temps aux deux conditions suivantes :

*i)* le quadruplet $< \mathbb{R}, +, \cdot, \leq >$ est un corps commutatif totalement ordonné ;

*ii)* l'ensemble $\mathbb{R}$ est fermé par rapport à l'opération de passage à la limite des séries de Cauchy à termes dans $\mathbb{R}$.

Si on fait abstraction de ce qu'on a dit ci-dessus, on ne peut comprendre la condition (*ii*) qu'en la confrontant à la condition (*i* ), car c'est justement parce que le quadruplet $< \mathbb{R}, +, \cdot, \leq >$ est supposé être un corps (commutatif) totalement ordonné, au même titre que le quadruplet $< \mathbb{Q}, +, \cdot, \leq >$, qu'on peut parler de suites de Cauchy à termes dans $\mathbb{R}$. Les définitions 2.4 et 4.2, respectivement des suites à termes dans $\mathbb{Q}$ qui convergent vers une limite dans $\mathbb{Q}$, et des suites de Cauchy à termes dans $\mathbb{Q}$, ne s'appuient en fait que sur des propriétés que l'ensemble $\mathbb{Q}$ possède en tant qu'il participe d'un corps totalement ordonné. Une fois qu'on suppose que le quadruplet $< \mathbb{R}, +, \cdot, \leq >$ est un corps (commutatif) totalement ordonné, on peut donc répéter ces définitions à la lettre en changeant $\mathbb{Q}$ par $\mathbb{R}$. C'est justement ce qu'on a fait dans les définitions 4.11 et 4.13, si bien qu'on peut se réclamer ici de ces mêmes définitions et leur rapporter la condition (*ii*).

Le problème est donc de comprendre à quelle condition l'ensemble $\mathbb{R}$, intervenant dans le corps commutatif totalement ordonné $< \mathbb{R}, +, \cdot, \leq >$, est fermé par rapport à l'opération de passage à la limite des suites de Cauchy à termes dans $\mathbb{R}$. La réponse à cette question est la clef de la stratégie suivie par Dedekind pour définir l'ensemble des nombres réels.

Pour comprendre cette réponse, revenons sur la définition 4.11, supposons que l'ensemble $\mathbb{R}$ des nombres réels soit donné, par exemple d'après la construction de Cantor, et imaginons qu'une suite de Cauchy à termes dans $\mathbb{R}$, $\{r_i\}_{i=0}^{\infty}$, soit telle que pour tout $\Lambda$ appartenant à $\mathbb{R}$, il y ait un nombre naturel $m$, tel que $u_m > \Lambda$. Fixons alors un nombre réel $\varepsilon$, et prenons un nombre naturel $n = n_\varepsilon$ tel que si $p \in \mathbb{N}$, alors pour tout $i > n_\varepsilon$, $|r_{i+p} - r_i| < \varepsilon$. Comme on a supposé que $\{r_i\}_{i=0}^{\infty}$ est une suite de Cauchy, quel que soit $\varepsilon$, il est possible de trouver un nombre naturel tel que celui-ci. Il est clair que la suite $\{r_i\}_{i=0}^{\infty}$ ne comporte que $n_\varepsilon + 1$ termes $r_i$, tels que $i \leq n_\varepsilon$. La collection $\{r_i\}_{i=0}^{n_\varepsilon} = \{r_0, r_1, ..., r_{n_\varepsilon}\}$ de ces termes possède donc certainement un terme maximal, c'est-à-dire qu'il existe un nombre naturel $h$, tel que $r_h \in \{r_i\}_{i=0}^{n_\varepsilon}$ (c'est-à-dire que $0 \leq h \leq n_\varepsilon$) et que si $0 \leq i \leq n_\varepsilon$, alors $r_i \leq r_h$. Prenons alors un nombre réel $\Lambda'$ plus grand que $r_h$ . D'après notre hypothèse, il doit évidemment y avoir un nombre naturel $m'$, tel que $r_{m'} > \Lambda'$. Quel que soit ce nombre, il doit nécessairement être plus grand que $n_\varepsilon$, de sorte que le terme $r_{m'}$ de $\{r_i\}_{i=0}^{\infty}$ appartient à la collection $\{r_i\}_{i=n_\varepsilon+1}^{\infty}$ correspondant à des valeurs de $i$ plus grandes que $n_\varepsilon$. Pourtant la collection $\{r_i\}_{i=0}^{m'}$ est, elle aussi, finie et elle possède donc, à son tour, un terme maximal. Or, comme $r_{m'} > \Lambda' > r_h$, ce terme doit appartenir à la collection $\{r_i\}_{i=n_\varepsilon+1}^{m'}$. On aura donc un nombre naturel $k$, plus grand que $n_\varepsilon$ et plus petit ou égal à $m'$, tel que $n_\varepsilon < i \leq m' \Rightarrow r_i \leq r_k$. Ceci établi, considérons un nouveau nombre réel $\Lambda''$ plus grand que $r_k$ et tel que $\Lambda'' - r_k \geq \varepsilon$. D'après notre hypothèse, il doit évidemment y avoir aussi un nombre naturel $m''$ tel que $r_{m''} > \Lambda''$, et quel que soit ce nombre, il doit nécessairement être plus grand que $m'$ et donc plus grand que $n_\varepsilon$. Il s'ensuit que la différence $|r_{i+j} - r_i|$ s'identifie, pour un certain $i$ plus grand que $n_\varepsilon$ et un certain $j$ naturel, à la différence $|r_{m''} - r_k|$, qui, parce que $r_{m''} > \Lambda'' > r_k$ et $\Lambda'' - r_k \geq \varepsilon$, ne pourra pas être plus petite que $\varepsilon$. Donc, ou bien la suite $\{r_i\}_{i=n_\varepsilon+1}^{\infty}$ n'est pas une suite de Cauchy, ou bien elle n'est pas telle que pour tout $\Lambda$ appartenant à $\mathbb{R}$, il y ait un nombre naturel $m$, tel que $r_m > \Lambda$.

Si une suite $\{r_i\}_{i=0}^{\infty}$ à termes en $\mathbb{R}$ est une suite de Cauchy, il y aura donc toujours un nombre réel $\Lambda$ , tel qu'aucun des termes de cette suite est plus grand que $\Lambda$. Encore une fois on a démontré ceci, en utilisant une preuve par l'absurde qui n'emploie pas le tiers exclu, mais, pour le faire, on a supposé que l'ensemble $\mathbb{R}$ des nombres réels était préalablement donné. Pourtant, même si on fait abstraction de cette condition essentielle pour notre preuve, rien ne nous empêche de considérer la propriété que notre preuve assigne à toute suite de Cauchy à termes dans $\mathbb{R}$, comme une propriété remarquable dont certaines suites à termes dans quelque ensemble $E$ peuvent jouir. Cette propriété mérite une définition :

Définition 4.14. *On dit qu'une suite $\{u_i\}_{i=0}^{\infty}$ à termes dans un ensemble totalement ordonné $E$ est supérieurement bornée dans $E$ (ou, inversement, inférieurement bornée), s'il y a un élément $\Lambda$ de $E$, tel que, quel que soit le nombre naturel $i$, $u_i \leq \Lambda$ (ou, inversement, $\Lambda \leq u_i$) ; plus généralement on dit qu'un sous-ensemble $E'$ de $E$ est supérieurement born dans $E$ (ou, inversement, inférieurement borné), s'il y a un élément $\Lambda$ de $E$ tel que $x \in E' \Rightarrow x \leq \Lambda$ (inversement $\Lambda \leq x$). $\Lambda$ sera alors dite « majorant » (ou, inversement, « minorant » ) de $E'$ et $E'$ sera dit aussi « majoré » (ou inversement « minoré » ) par $\Lambda$.*

Ce qu'on vient de montrer, à partir de l'hypothèse de la donnée préalable de $\mathbb{R}$, est donc que toute suite de Cauchy à termes dans $\mathbb{R}$ est supérieurement bornée dans $\mathbb{R}$. Analoguement, on aurait pu démontrer que toute suite de Cauchy à termes dans $\mathbb{R}$ est inférieurement bornée dans $\mathbb{R}$. Le lecteur pourra conduire cette preuve comme exercice. Il n'est pas non plus difficile de constater que la même preuve qu'on vient de donner pour des suites de Cauchy à termes dans $\mathbb{R}$ peut être répétée pour des suites de Cauchy à termes dans $\mathbb{Q}$. Ce qui pourtant distingue $\mathbb{R}$ de $\mathbb{Q}$ est une propriété dont l'ensemble des majorants ou des minorants d'une suite de Cauchy à termes dans $\mathbb{R}$ ou dans $\mathbb{Q}$ jouit dans $\mathbb{R}$, mais pas dans $\mathbb{Q}$.

REMARQUE 6.19. Pour expliciter cette propriété, on raisonnera ci-dessous sur des suites de Cauchy respectivement à termes dans $\mathbb{Q}$ et dans $\mathbb{R}$. Le lecteur doit pourtant garder à l'esprit que $\mathbb{Q}$ n'est qu'un sous-ensemble de $\mathbb{R}$, donc toute suite à termes dans $\mathbb{Q}$ est, en même temps, une suite à termes dans $\mathbb{R}$, bien que la réciproque ne vaille pas. La propriété dont on va parler concerne d'ailleurs les ensembles $\mathbb{R}$ et $\mathbb{Q}$, non pas en tant qu'ensembles auxquels appartiennent les termes d'une suite de Cauchy, mais en tant qu'ensembles auxquels appartiennent ou éventuellement n'appartiennent pas des minorants ou des majorants particuliers d'une suite, autant à termes dans $\mathbb{Q}$ qu'à termes dans $\mathbb{R}$.

Imaginons qu'une suite de Cauchy, à termes respectivement dans $\mathbb{Q}$ ou dans $\mathbb{R}$, soit majorée par un nombre $\Lambda$, respectivement rationnel ou réel, alors elle sera aussi majorée par tout nombre $\Lambda'$, respectivement rationnel ou réel, plus grand que $\Lambda$. Toute suite de Cauchy à termes dans $\mathbb{Q}$ ou dans $\mathbb{R}$ a donc une infinité de majorants, et, de même, une infinité de minorants. Pour fixer les idées et simplifier la situation, imaginons que la suite en question soit croissante. Alors, elle sera sans doute minorée par un de ses termes et par tout nombre, respectivement rationnel ou réel, plus petit que ce terme (encore une fois, la preuve est laissée au lecteur comme exercice) ; de surcroît, aucun nombre, respectivement rationnel ou réel, plus grand que ce terme ne pourra être un minorant de cette suite, car, quel que soit ce nombre, il y aura au moins un terme de la suite qui est plus petit que lui. L'ensemble des minorants de notre suite sera donc, non seulement supérieurement borné, mais contiendra aussi un élément maximale, respectivement dans $\mathbb{Q}$ ou dans $\mathbb{R}$ : il y aura un nombre, respectivement rationnel ou réel, qui est le plus grand des minorants de cette suite et ce nombre n'est rien d'autre qu'un terme de la suite, le plus petit de ces termes. Cela devra être clair, et ne demande pas d'autres explications. La question qui se pose est en revanche autre : est on sûr qu'une suite de Cauchy croissante, à termes dans $\mathbb{Q}$ ou dans $\mathbb{R}$, soit telle que l'ensemble de ses majorants ne soit pas vide et possède un élément minimal, respectivement dans $\mathbb{Q}$ ou dans $\mathbb{R}$ ; qu'il y ait un nombre, respectivement rationnel ou réel, qui est le plus petit des majorants de cette suite ? La réponse est différente, selon que l'on cherche ce majorant minimal dans $\mathbb{Q}$ ou dans $\mathbb{R}$.

Si notre suite est une suite à termes dans $\mathbb{Q}$, et qu'on cherche ce majorant minimal dans $\mathbb{Q}$, rien ne nous assure que ceci soit le cas. Si on considère deux segments incommensurables, on choisit le premier de ces segments comme unité de mesure, alors la suite des mesures approchées du deuxième segment relatives à cette unité de mesure, obtenues par le biais de la procédure exposée dans le paragraphe 1, est certainement une suite de Cauchy croissante et elle est superieurement bornée dans $\mathbb{Q}$, mais l'ensemble de ses majorants n'a pas de termes minimale dans $\mathbb{Q}$. Le lecteur pourra vérifier ceci à titre d'exercice. Si par exemple, on considère le côté et la diagonale d'un carré, on prend le premier de ces segments comme unité de mesure et on pose, quel que soit le nombre naturel strictement positif $i$, $m_i = 10$, on obtient la suite

$$1, \frac{14}{10}, \frac{141}{100}, \frac{1.414}{1.000}, \frac{14.142}{10.000}, \frac{141.421}{100.000}, \ldots$$

qui est sans doute une suite de Cauchy supérieurement bornée dans $\mathbb{Q}$ (étant, par exemple, majorée par le nombre rationnel 2), mais qui est aussi telle que l'ensemble de ses majorants n'a pas de terme minimal dans $\mathbb{Q}$.

Considérons en revanche une suite de Cauchy croissente à termes dans $\mathbb{R}$ (ou même seulement dans $\mathbb{Q}$), $\{r_1\}_{i=0}^{\infty}$ et cherchons ce majorant minimal dans $\mathbb{R}$. On peut raisonner comme il suit. Une suite de Cauchy à termes dans $\mathbb{R}$ (et, *a fortiori*, dans $\mathbb{Q}$) a sans doute une limite $r$ dans $\mathbb{R}$. Or, comme cette suite est croissante, il y aura un nombre naturel $n$ tel que $i > n \Rightarrow r_{i+1} > r_i$. Il est alors claire que $r$, est aussi plus grand que tout terme $r_i$ de la suite, tel que $i > n$. Il sera donc un majorant de la suite $\{r_i\}_{i=n+1}^{\infty}$ (le lecteur démontrera ceci sans

difficulté). Mais comme les termes de la suite s'approchent de plus en plus de cette limite, c'est-à-dire que, pour chaque nombre réel $\varepsilon$, il y a toujours un terme de la suite dont la distance avec la limite — c'est-à-dire la différence entre cette limite et ce terme (comme on parle de suite croissante, il ne sera pas nécessaire de parler de valeur absolue) — est plus petite que $\varepsilon$, il s'ensuit qu'aucun nombre réel plus petit que cette limite peut être un majorant d'une telle suite. Comme l'ensemble $\{r_i\}_{i=0}^{n}$ ne contient qu'un nombre fini d'éléments, et qu'il possède donc un terme maximale, il s'ensuit que l'ensemble des majorants de la suite $\{r_1\}_{i=0}^{\infty}$ possède un élément minimal dans $\mathbb{R}$ : il y a sans doute un nombre réel, qui est le plus petit des majorants de cette suite, et ce nombre est ou bien la limite $r$ de cette suite, ou bien un terme $r_i$ de cette suite, tel que $i \leq n$. En raisonnant de la même manière, on peut démontrer qu'une suite de Cauchy décroissante (c'est-à-dire telle qu'il existe un nombre naturel $n$, tel que, au-délà de l'$n$-ième terme de la suite, les termes de cette suite sont de plus en plus petits), à termes dans $\mathbb{R}$ (et, *a fortiori*, dans $\mathbb{Q}$) est telle que l'ensemble de ses minorants possède un élément maximal dans $\mathbb{R}$. Un raisonnement analogue, mais légèrement modifié, que le lecteur ne devra avoir, à ce stade, aucune difficulté à formuler, montre que si une suite de Cauchy à termes dans $\mathbb{R}$ (et, *a fortiori*, dans $\mathbb{Q}$) n'est ni croissante, ni décroissante (comme c'est le cas, par exemple, de la suite $\left\{1, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{8}, \ldots\right\} = \left\{(-1)^i \frac{1}{2^i}\right\}_{i=0}^{\infty}$), alors elle est telle que les ensembles respectivement de ses minorants et de ses majorants possèdent un extrême (c'est-à-dire respectivement un élément maximal et un élément minimal) dans $\mathbb{R}$ (qui sera dans les deux cas un terme de la suite ; dans l'exemple précédent, respectivement le terme $u_1 = (-1)\frac{1}{2} = -\frac{1}{2}$ et le terme $u_0 = (-1)^0 \frac{1}{2^0} = 1$). On vient donc de démontrer qu'une suite de Cauchy à termes dans $\mathbb{R}$ (et, *a fortiori*, dans $\mathbb{Q}$) est toujours telle que les ensembles respectivement de ses minorants et de ses majorants possèdent un extrême dans $\mathbb{R}$.

Cette propriété remarquable de $\mathbb{R}$ n'est pas une propriété de $\mathbb{Q}$.

L'idée clef de la méthode de Dedekind est justement de caractériser axiomatiquement $\mathbb{R}$ comme un ensemble qui forme, avec les opérations $+$ et $\cdot$ et la relation $\leq$, un corps commutatif totalement ordonné, et qui satisfait de surcroît à une condition supplémentaire (qui n'est pas satisfaite par $\mathbb{Q}$) et qui n'est rien d'autre qu'une généralisation convenable (formulée sans se réclamer de suites de Cauchy à termes dans $\mathbb{R}$) de la propriété dont on vient de démontrer, en partant de la supposition que $\mathbb{R}$ est donné préalablement, qu'elle est une propriété de de ce dernier ensemble (mais non de $\mathbb{Q}$). Une fois que cela sera fait, il sera ensuite possible de démontrer que l'ensemble $\mathbb{R}$, ainsi caractérisé, est fermé par rapport à l'opération de passage à la limite des suites de Cauchy à termes dans ce même ensemble.

Ceci peut se faire (au moins) de deux manières différentes, mais équivalentes entre elles.

En premier lieu, on peut stipuler que si $A$ et $B$ sont deux sous-ensembles non vides de $\mathbb{R}$, tels que : *i)* chaque élément de $A$ est plus petit que chaque élément de $B$, c'est-à-dire, en symboles,

$$(x \in A) \wedge (y \in B) \Rightarrow x < y$$

(ce qui implique que l'intersection $A \cap B$ de ces ensembles est vide) ; *ii)* chaque élément de $\mathbb{R}$ appartient soit à $A$, soit à $B$, c'est-à-dire, en symboles,

$$x \in \mathbb{R} \Rightarrow (x \in A) \vee (y \in B)$$

(ce qui implique que l'union $A \cup B$ de ces ensembles s'identifie à $\mathbb{R}$ lui-même, c'est-à-dire que $B$ coïncide avec le complémentaire, « $A_{\mathbb{R}}^{C}$ », de $A$ par rapport à $\mathbb{R}$) ; alors, il y a dans $\mathbb{R}$ un élément $z$, qui est en même temps plus grand ou égal à tous les éléments de $A$ et plus petit ou égal à tous les éléments de $B$, c'est-à-dire, en symboles,

$$\exists z \in \mathbb{R} \text{ tel que } : [(x \in A) \wedge (y \in B) \Rightarrow x \leq z \leq y]$$

C'est le contenu de ce qu'on appelle généralement « axiome de la coupure », ou même « axiome de Dedekind », car la propriété énoncée par cet axiome fut justement observée pour la première fois par Dedekind dans un mémoire de 1872.

En deuxième lieu, on peut stipuler que si $A$ est un sous-ensemble de $\mathbb{R}$ supérieurement borné dans $\mathbb{R}$, alors il y a dans $\mathbb{R}$ un élément $\overline{\overline{\Lambda}}$ qui est le plus petit des majorants de $A$.

Pour rendre plus clair le contenu de cette dernière stipulation, posons d'abord la définition suivante :

Définition 4.15. *Si un sous-ensemble $E'$ d'un ensemble $E$ totalement ordonné est supérieurement borné dans $E$ (inversement, inférieurement borné dans $E$), et que le sous-ensemble de $E$ composé par tous les majorants de $E'$ (inversement, par tous les minorants de $E'$) possède un élément minimal (inversement maximal), alors on dit que $E'$ possède une borne supérieure (inversement, une borne inférieure) dans $E$, on appelle justement cet élément minimal (inversement maximal) « borne supérieure de $E'$ dans $E$ » (inversement, « borne inférieure de $E'$ dans $E$ » ), et on le note par le symbole « $\overline{\overline{\Lambda}}_{E'\subseteq E}$ » (inversement, « $\underline{\underline{\Lambda}}_{E'\subseteq E}$ » ). La borne supérieure $\overline{\overline{\Lambda}}_{E'\subseteq E}$ de $E'$ dans $E$ est donc un élément $z$ de $E$, tel que*

$$[(x \in E') \Rightarrow (x \leq z)] \wedge \{(y \in E) \Rightarrow [(y < z) \Rightarrow \exists v \in E' \text{ tel que } v \geq y]\}$$

*En revanche, la borne inférieure $\underline{\underline{\Lambda}}_{E'\subseteq E}$ de $E'$ dans $E$ est un élément $z$ de $E$, tel que*

$$[(x \in E') \Rightarrow (z \leq x)] \wedge \{(y \in E) \Rightarrow [(z < y) \Rightarrow \exists v \in E' \text{ tel que } y \geq v]\}$$

La stipulation précédente revient alors à poser que si $A$ est un sous-ensemble de $\mathbb{R}$ non vide supérieurement borné dans $\mathbb{R}$, alors $A$ possède une *borne supérieure* $\overline{\overline{\Lambda}}_{A\subseteq\mathbb{R}}$ dans $\mathbb{R}$ (évidemment la stipulation réciproque pour les sous-ensembles de $\mathbb{R}$ inférieurement limités est équivalente et peut être déduite comme théorème, une fois qu'on a posé que tout sous-ensemble $A$ de $\mathbb{R}$ non vide et supérieurement borné dans $\mathbb{R}$ possède une *borne supérieure* ; le lecteur est invité à prouver cette équivalence à titre d'exercice). C'est le contenu de ce qu'on appelle généralement « axiome de la borne supérieure ».

L'équivalence entre l'axiome de la coupure et celui de la borne supérieure est facile à prouver.

On imagine d'abord que $A$ est un sous-ensemble de $\mathbb{R}$ supérieurement borné dans $\mathbb{R}$. Soit alors $M[A]$ l'ensemble des majorants de $A$ dans $\mathbb{R}$ et $M[A]^C_{\mathbb{R}}$ le complémentaire de $M[A]$ par rapport à $\mathbb{R}$. De la définition même de l'ensemble complémentaire d'un ensemble donné, il est clair que tout élément $x$ de $\mathbb{R}$ appartient soit à $M[A]$, soit à $M[A]^C_{\mathbb{R}}$. De surcroît, si $x$ est un élément de $\mathbb{R}$ qui appartient à $M[A]$, alors $x$ est un majorant de $A$ dans $\mathbb{R}$, et donc — comme tout élément de $\mathbb{R}$ qui est plus grand qu'un majorant de $A$ dans $\mathbb{R}$ est à son tour un majorant de $A$ — il s'ensuit que tout élément de $M[A]^C_{\mathbb{R}}$ est plus petit que tout élément de $M[A]$. Les deux ensembles $M[A]$ et $M[A]^C_{\mathbb{R}}$ satisfont donc aux conditions $(i)$ et $(ii)$ intervenant dans l'énoncé de l'axiome de coupure. Si on suppose donc cet axiome, il s'ensuit qu'il y a un élément $\alpha$ de $\mathbb{R}$, tel que

$$\left[\left(x \in M[A]^C_{\mathbb{R}}\right) \wedge (y \in M[A]) \Rightarrow x \leq \alpha \leq y\right]$$

Comme l'union de $M[A]$ et de $M[A]^C_{\mathbb{R}}$ coïncide avec $\mathbb{R}$, il est clair que $\alpha$, étant un élément de $\mathbb{R}$, appartient soit à $M[A]$, soit à $M[A]^C_{\mathbb{R}}$, mais comme l'intersection de ces ensembles est vide, il ne peut qu'appartenir à un seul de ces ensembles. S'il appartenait à $M[A]^C_{\mathbb{R}}$, alors ce ne serait pas un majorant de $A$, et il y aurait donc un élément $a$ de $A$, tel que $\alpha < a$. Mais si ceci était

le cas, alors, comme $< \mathbb{R}, +, \cdot, \leq >$ est un corps totalement ordonné,

$$\begin{aligned} \alpha + a &< a + a \\ \alpha + \alpha &< a + \alpha \end{aligned}$$

et donc

$$\alpha < \frac{\alpha + a}{2} < a \tag{104}$$

L'élément $\frac{\alpha+a}{2}$ de $\mathbb{R}$ serait donc plus grand que $\alpha$ et donc il devrait appartenir à $M[A]$, mais il serait aussi plus petit que l'élément $a$ de $A$ et donc il ne pourrait pas être un majorant de $A$ et il devrait donc appartenir à $M[A]^C_{\mathbb{R}}$. De l'hypothèse que $\alpha$ appartient à $M[A]^C_{\mathbb{R}}$, il suit donc une contradiction et donc $\alpha$ n'appartient pas à $M[A]^C_{\mathbb{R}}$ et il appartient par conséquence à $M[A]$. $\alpha$ est ainsi l'élément minimal de $M[A]$ et il est donc la borne supérieure de $A$. On a donc prouvé que si $A$ est un sous-ensemble de $\mathbb{R}$ supérieurement borné et l'axiome de la coupure est supposé, alors $A$ possède une borne supérieure dans $\mathbb{R}$.

On suppose maintenant l'axiome de la borne supérieure et on considère deux sous-ensembles $A$ et $B$ de $\mathbb{R}$ qui satisfont aux conditions $(i)$ et $(ii)$ intervenant dans l'énoncé de l'axiome de coupure. Il est alors clair que $A$ est superieurement borné dans $\mathbb{R}$, car tout élément de $B$ est un majorant de $A$ dans $\mathbb{R}$. Il possède donc une borne supérieure $\alpha$ qui ne pourra être plus grande qu'aucun élément de $B$, car tout élément de $B$ est un majorant de $A$. Donc $\alpha$ ne pourrait qu'être telle que

$$A \leq \alpha \leq B$$

comme le veut justement l'axiome de la coupure.

REMARQUE 6.20. On observe que la preuve de la deuxième des deux implications précedentes peut être répétée pour n'importe quel ensemble totalement ordonné. On peut donc dire que tout ensemble totalement ordonné qui satisfait à l'axiome de la borne supérieure satisfait aussi à l'axiome de la coupure. En revanche pour conduire la preuve de la première implication, on s'est réclamé de certaines propriétés auxquelles l'ensemble $\mathbb{R}$ satisfait en tant qu'il participe d'un corp totalemnt ordonné. Il est pourtant clair qu'on s'est réclamé de ces propriétés seulement pour construire l'élément $\frac{\alpha+a}{2}$ de $\mathbb{R}$ qui satisfait à (104). Pour s'assurer qu'il y a un élément $\beta$ de $\mathbb{R}$ tel que

$$\alpha < \beta < a$$

on aurait pourtant pû ne se réclamer que de la densité de $\mathbb{R}$. Donc notre preuve peut s'appliquer à tout ensemble totalement ordonné dense. On en tire que tout ensemble totalement ordonné et dense qui satisfait à l'axiome de la coupure, satisfait aussi à l'axiome de la borne supérieure.

Imaginons maintenant que $< \mathbb{R}, +, \cdot, \leq >$ soit un corps (commutatif) totalement ordonné, que $\mathbb{R}$ satisfasse à l'axiome de la borne supérieure, et qu'il y ait de surcroît deux éléments $x$ et $y$ de $\mathbb{R}$, strictement positifs, tels que, quel que soit le nombre naturel strictement positif $n$,

$$\underbrace{x + x + x + \ldots + x}_{n \text{ fois}} \leq y$$

On observe d'abord que si on note par le symbole « 1 » l'élément neutre de la multiplication dans $\mathbb{R}$, alors, par effet de la distributivité de la multiplication sur l'addition on a

$$\underbrace{x + x + x + \ldots + x}_{n \text{ fois}} = \underbrace{(1 + 1 + 1 + \ldots + 1)\, x}_{n \text{ fois}}$$

et si on note par « $\widetilde{n}$ » la somme de l'addition

$$\underbrace{1+1+1+\ldots+1}_{n \text{ fois}}$$

qui, $<\mathbb{R},+,\cdot,\leq>$ étant un corps, est sans doute un élément de $\mathbb{R}$, on tire l'égalité

$$\underbrace{x+x+x+\ldots+x}_{n \text{ fois}} = \widetilde{n}x$$

L'hypothèse (4.2) se réduit donc à la condition :

$$\widetilde{n}x \leq y$$

Le sous-ensemble $\left\{0x, 1x, \widetilde{2}x, \widetilde{3}x, \ldots\right\}$ (où 0 et 1 sont évidemment les éléments neutres respectivement de l'addition et de la multiplication dans $\mathbb{R}$, et $\widetilde{2}, \widetilde{3}, \ldots$ et $\widetilde{2}x, \widetilde{3}x, \ldots$ sont définis comme on vient de voir) serait alors supérieurement limité dans $\mathbb{R}$. Par l'axiome de la borne supérieure, il admettrait ainsi une borne supérieure. Soit $X$ cette borne supérieure. Alors, quel que soit le nombre naturel $m$, on aurait

$$\widetilde{(m+1)}x \leq X$$

c'est-à-dire (comme, par définition, $\widetilde{(m+1)} = \widetilde{m}+1$),

$$\widetilde{m}x \leq X - x$$

et $X - x < X$ serait alors un majorant de $\left\{0x, 1x, \widetilde{2}x, \widetilde{3}x, \ldots\right\}$ et $X$ ne pourrait donc pas être la borne supérieure de ce sous-ensemble de $\mathbb{R}$.

Il s'ensuit que, quels que soient les éléments $x$ et $y$ de $\mathbb{R}$, strictement positifs, il y a un nombre naturel strictement positif $n$, tel que $\widetilde{n}x > y$.

De surcroît, $<\mathbb{R},+,\cdot,\leq>$ étant un corps totalement ordonné, il n'est pas possible qu'il y ait un nombre naturel strictement positif $\nu$, tel que, pour quelque nombre naturel $\mu$ plus petit que $\nu$, $\widetilde{\nu} = \widetilde{\mu}$, et donc les éléments $\widetilde{i}$ $(i = 2, 3, \ldots)$ de $\mathbb{R}$ se comportent les uns par rapport aux autres, et tous par rapport aux éléments neutres de l'addition et de la multiplication dans $\mathbb{R}$, 0 et 1, comme les nombres naturels $2, 3, \ldots$ se comportent les uns par rapport aux autres, et tous par rapport aux nombres naturels 0 et 1. En d'autres termes le sous-ensemble $\left\{0, 1, \widetilde{2}, \widetilde{3}, \ldots\right\}$ de $\mathbb{R}$ est isomorphe à $\mathbb{N}$ et peut donc être pris pour cet ensemble, de sorte que $\mathbb{N}$ résulte être un sous-ensemble de $\mathbb{R}$. On a ainsi démontré le théorème suivant, énonçant le principe dit « d'Archimède » pour tout corps (commutatif) totalement ordonné :

THÉORÈME 4.3. *Si $<\mathbb{R},+,\cdot,\leq>$ est un corps (commutatif) totalement ordonné et $\mathbb{R}$ satisfait à l'axiome de la borne supérieure, alors, quels que soient $x$ et $y$ appartenant à $\mathbb{R}$ et strictement positifs, il y a un nombre naturel strictement positif $n$, tel que*

$$nx > y$$

On verra que ce théorème sera utile par la suite.

NOTE HISTORIQUE 6.14. Parmi les définitions qui ouvrent le V$^{\text{ème}}$ livre des *Éléments*, juste avant d'énoncer la célèbre définition 5, introduisant la notion d'égalité des rapports (cf. la note historique 6.3), Euclide donne la définition suivante, qui est donc, la définition 4 du livre V : « Des grandeurs sont dites *avoir un rapport l'une relativement à l'autre* quand elles sont capables, étant multipliées, de se dépasser l'une l'autre ». Naturellement, l'expression « étant multipliées » se réfère ici à la multiplication par des nombres entiers positifs, de sorte que la définition 4 du livre V des

*Éléments* doit s'interpréter ainsi : des grandeurs $x$ et $y$ sont dites *avoir un rapport l'une relativement à l'autre* quand il existe un nombre naturel strictement positif $n$, tel que $nx > y$. Il s'ensuit que cette définition se réclame de la condition que, dans le théorème précédent, on a assignée aux éléments strictement positifs de $\mathbb{R}$, pour caractériser la relation binaire '$x$ a un rapport avec $y$' référée à des grandeurs (qui ne sont d'ailleurs, pour Euclide, que des quantités, en particuliers des quantités continues, qu'on qualifierait aujourd'hui de strictement positives).

Le rôle qu'on assigne à cette définition, dans le cadre de la théorie euclidienne des grandeurs dépend naturellement de la manière dont on interprète la notion euclidienne de rapport, qui est introduite par Euclide dans la définition V.3 et qui fera l'objet de la définition V.5. La définition V.3 est la suivante : « Un *rapport* est la relation, telle ou telle, selon la taille qu'il y a entre deux grandeurs du même genre ».

Cette définition est fort problématique, et il est possible d'interpréter la théorie exposée dans le V$^{\text{ème}}$ livre des *Éléments* de telle sorte qu'elle n'y joue aucun rôle. Comme on l'a vu dans la note historique 6.3, on peut d'abord fusionner les définitions 3.1 et 4.1 et interpréter directement la première comme une définition de proportionnalité. Ensuite, on peut remplacer, toutes les fois qu'elle apparaît dans le livre V, l'expression « avoir (ou être dans) le même rapport » par une périphrase convenable ne faisant pas intervenir la notion de rapport, mais seulement celle de proportionnalité. Cela revient au fond à comprendre la définition 3.1 comme une définition contextuelle de la relation 'être dans le même rapport', qui ne demande aucunement une définition préalable de la notion de rapport entre deux grandeurs. Cette définition se trouverait de cette manière être, *de facto*, exclue de la structure logique du livre V. Elle y subsisterait ainsi purement comme la marque d'une incertitude locale, effacée ensuite, et on pourrait même soupçonner qu'elle ne dérive que d'une interpolation.

Même s'il maintint (sous une autre numérotation) la définition 3.1, Commandinus avait déjà montré, au XVI$^{\text{ème}}$ siècle, par son édition des *Éléments* que cette, lecture est possible. Une lecture opposée à celle de, plus ou moins contemporaine de celle-ci, fut en revanche proposée par Clavius qui, dans son édition des *Éléments*, insista par contre sur le rôle central que, d'après lui, la notion de rapport de deux grandeurs, joue dans le livre V. Bien que, sur plusieurs points, la lecture de Clavius confère à la théorie d'Eudoxe et Euclide une richesse bien plus grande que celle à laquelle la confine la lecture de Commandinus, elle ne sait pas résoudre la principale difficulté : comment interpréter l'énigmatique définition V.3 ? comment définir un rapport entre deux grandeurs dans le cadre des mathématiques euclidiennes ? Ces questions ont été l'objet de longues discussions au cours des siècles, avant et après la querelle intellectuelle qui a opposé Commandinus et Clavius, des discussions qu'ici on ne saurait même pas résumer.

Si, comme je pense qu'il est correct de le faire, on se place dans la lignée de l'interprétation de Commandinus, la définition 2.1 vient à assumer un rôle fondamental. Après avoir effacé ou mis entre parenthèses la définition 1.3, avec sa référence à la notion de grandeurs du même genre (que cette définition semble supposer comme primitive), on pourrait penser que la définition 2.1 fonctionne dans la structure logique du livre V, comme une définition opérationnelle de l'homogénéité. Pensée de cette manière, cette définition ne servirait aucunement à exclure du domaine des grandeurs qui ont un rapport entre elles des grandeurs infiniment grandes ou infiniment petites, car la non-existence d'un nombre entier positif $n$, tel que $nx > y$ ne dépendrait pas du fait que $x$ est une grandeur infiniment plus petite que $y$, mais du fait, bien plus

simple à imaginer, que $x$ et $y$ n'appartiennet pas au même domaine de grandeurs. Personne ne pourrait alors s'étonner de retrouver justement cette définition parmi les définitions et non pas parmi les postulats ou les notions communes (les suppositions non démontrées qui constituent la base de la structure déductive des *Éléments*).

On justifierait aussi, de cette manière, l'usage traditionnel consistant à associer le nom d'Archimède à la condition sur laquelle porte le théorème précédent. Le cinquième parmi les postulats que Archimède énonce au début de son traité *De la sphère et du cylindre*, est en fait le suivant : « De plus, parmi les lignes inégales, les surfaces inégales, les corps inégaux, le plus grand dépasse le plus petit d'une grandeur telle que, ajoutée à elle-même, elle peut dépasser toute grandeur donnée ayant un rapport avec les grandeurs comparées entre elles ». Par ce postulat, Archimède semble bien inverser la définition V.4 d'Euclide : supposer savoir au préalable ce que signifie que deux grandeurs $x$ et $y$ ont un rapport entre elles, et postuler que si deux grandeurs ont un rapport entre elles (c'est-à-dire, apparemment, qu'elles sont homogènes), alors il y a toujours un nombre entier strictement positif $n$ qui, multiplié avec la plus petite de ces grandeurs, produit une grandeur (homogène à celle-ci) plus grande que la plus grande des grandeurs données. Le théorème qu'on vient de démontrer montre alors que si on entend par grandeur un élément d'un corps (commutatif) totalement ordonné, satisfaisant à l'axiome de la borne supérieure, alors le postulat d'Archimède se transforme en un théorème, qu'il n'est d'ailleurs pas difficile de démontrer.

On observe, pour conclure, que cela n'exclut pas que, dans un certain corps (commutatif) totalement ordonné, il puisse y avoir des éléments $x$ et $y$ dont le premier se comporte comme un infiniment petit par rapport au second. Cela est d'ailleurs le cas du corps commutatif totalement ordonné $< {}^*\mathbb{R}, +, \cdot, \leq >$ dont traite l'analyse non standard (cf. la note historique 6.11). Il suffit pour rendre ceci possible que dans ce même corps il y ait des entiers strictement positifs qui se comportent comme des nombres infinis par rapport à la taille de $y$. Le nombre $n$ satisfaisant à la condition $nx > y$ serait alors, tout simplement, un de ces entiers.

**Lectures possibles** : B. Vitrac, « Notice sur la Définition V.4 et l'axiome d'Archimède », *in* Euclide, *Les Éléments*, traduction et commentaires par B. Vitrac, vol. II, PUF, Paris, 1994, pp. 135-141 ; E. Giusti, *Euclides reformatus*, Bollati-Boringhieri, Torino, 1992.

Pour justifier la définition axiomatique de Dedekind, il ne nous reste à ce stade qu'à prouver que si $< \mathbb{R}, +, \cdot, \leq >$ est un corps commutatif totalement ordonné et qu'on suppose que $\mathbb{R}$ satisfait de surcroît ou bien à l'axiome de la coupure, ou bien à l'axiome de la borne supérieure (ce qui, grâce à l'équivalence de ces axiomes implique qu'il satisfait aux deux), alors cet ensemble est fermé par rapport à l'opération de passage à la limite des suites de Cauchy à termes dans $\mathbb{R}$. C'est l'objet du théorème suivant :

THÉORÈME 4.4. *Si $\mathbb{R}$ est un ensemble tel que $< \mathbb{R}, +, \cdot, \leq >$ est un corps commutatif totalement ordonné, qui satisfait de surcroît à l'axiome de la borne supérieure, alors toute suite à termes dans $\mathbb{R}$ converge vers une limite $R$ dans $\mathbb{R}$ si et seulement si c'est une suite de Cauchy.*

**Preuve.** Pour prouver qu'une suite à termes dans $\mathbb{R}$ qui converge vers une limite dans $\mathbb{R}$ est une suite de Cauchy, il suffit de répéter (avec les changements convenables, que le lecteur pourra apporter seul) l'argument qu'on a déjà utilisé ci-dessus pour prouver qu'une suite à termes dans $\mathbb{Q}$ qui converge vers une limite dans $\mathbb{Q}$ est une suite de Cauchy. Ainsi il ne reste à prouver que l'implication inverse, qui est d'ailleurs ce qui fait l'intérêt du théorème : toute suite

de Cauchy à termes dans $\mathbb{R}$ converge vers une limite dans $\mathbb{R}$. Voici comment on peut procéder pour conduire cette preuve.

Ci-dessus, on a montré, en supposant que l'ensemble $\mathbb{R}$ des nombres réels a été préalablement donné, avec toutes ses propriétés, que si une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ est une suite de Cauchy, alors il y a un nombre réel $\Lambda$, tel qu'aucun des termes de cette suite n'est plus grand que $\Lambda$. Or, il est facile de voir que la démonstration qu'on a donné de cette implication ne dépend aucunement du fait que $\mathbb{R}$ est fermé par rapport au passage à la limite des suites de Cauchy à termes dans $\mathbb{R}$. Cette démonstration pourrait donc être répétée ici et accompagnée d'une démonstration analogue prouvant que si une suite $\{r_i\}_{i=0}^{\infty}$ à termes en $\mathbb{R}$ est une suite de Cauchy, alors il y a un nombre réel $\Lambda'$, tel qu'aucun des termes de cette suite n'est plus petit que $\Lambda'$. Pourtant pour plus de clarté, on va démontrer ci-dessous ces deux implications d'une manière plus rapide et compacte, en ne se réclamant que du fait que $< \mathbb{R}, +, \cdot, \leq >$ est un corps (commutatif) totalement ordonné. Cela fera l'objet du lemme suivant :

*Lemme 1* Toute suite de Cauchy à termes dans $\mathbb{R}$ est aussi bien supérieurement qu'inférieurement bornée dans $\mathbb{R}$ ; pour plus de simplicité, on dira alors qu'elle est bornée dans $\mathbb{R}$.

Si $\{r_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{R}$, alors, pour tout nombre réel $\varepsilon$, il y a un nombre naturel $n_\varepsilon$, tel que, si $i$ et $m$ sont plus grands que $n_\varepsilon$, alors

$$|r_i - r_m| < \varepsilon$$

Mais, si $< \mathbb{R}, +, \cdot, \leq >$ est un corps, alors il y a dans $\mathbb{R}$ un élément neutre de la multiplication, que par simplicité on pourra noter « 1 », comme ci-dessus. On pose alors $\varepsilon = 1$ et soit $n_1$ un nombre naturel tel que, si $i$ et $m$ sont plus grands que $n_1$, alors

$$|r_i - r_m| < 1$$

Soit alors $m = N > n_1$, il suit que si $i > n_1$, alors

$$|r_i - r_N| < 1 \tag{105}$$

On pose alors

$$M = |r_1| + |r_2| + ... + |r_N| + 1$$

Il est clair que si $i \leq N$, alors $|r_i| < M$, et donc $-M < r_i < M$. Par ailleurs, si $i > N$, alors de la (105), il suit que

$$-1 < r_i - r_N < 1$$

et donc

$$r_N - 1 < r_i < r_N + 1 \tag{106}$$

Mais le lecteur pourra démontrer seul que

$$\begin{aligned} r_N - 1 &\geq -|r_N| - 1 \\ r_N + 1 &\leq |r_N| + 1 \end{aligned}$$

et donc de la (106), il suit

$$-|r_N| - 1 < r_i < |r_N| + 1$$

c'est-à-dire

$$|r_i| < |r_N| + 1 \leq M$$

Donc, quel que soit $i$,

$$|r_i| < M$$

ou bien

$$-M < r_i < M$$

($M$ étant évidemment un réel strictement positif). Donc, quel que soit $i$, $r_i$ est plus petit que $M$ et plus grand que $-M$, comme il s'agissait de prouver. Ceci conclut la preuve du lemme 1.

Le lemme 1 n'est pas le seul lemme qu'il faut démontrer au cours de la preuve du théorème 4.4. Avant d'énoncer, puis de démontrer un nouveau lemme, il est néanmoins souhaitable d'introduire une terminologie convenable.

À partir d'une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ (mais on pourrait répéter le même argument pour n'importe quel autre ensemble sur lequel on peut définir des suites), il est toujours possible de construire une autre suite $\{s_i\}_{i=0}^{\infty}$ à termes dans le même $\mathbb{R}$, dont les termes soient tous des termes de $\{r_i\}_{i=0}^{\infty}$, pris dans l'ordre dans lequel ils apparaissent dans la suite $\{r_i\}_{i=0}^{\infty}$, sans pour autant que tous les termes de $\{r_i\}_{i=0}^{\infty}$ soient des termes de $\{s_i\}_{i=0}^{\infty}$. Pour cela il suffit de construire une application de $\mathbb{N}$ sur $\mathbb{N}$ qui associe à chaque nombre naturel $i$ un nombre naturel $k_i$, tel que, quels que soient les nombres naturels $\nu$ et $\mu$,

$$\nu < \mu \Rightarrow k_\nu < k_\mu$$

et de poser,

$$s_i = r_{k_i}$$

On dira alors que la suite $\{s_i\}_{i=0}^{\infty}$ est une *sous-suite de la suite* $\{r_i\}_{i=0}^{\infty}$, ou même une *sous-suite extraite de la suite* $\{r_i\}_{i=0}^{\infty}$.

Considérons maintenant une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ et imaginons que $H$ soit un nombre réel et qu'il y ait un nombre naturel $n$, tel que

$$i > n \Rightarrow r_i \leq H$$

alors on dit que $H$ est un *majorant définitif* de la suite $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$. Évidemment, tout majorant dans $\mathbb{R}$ d'une suite $\{r_i\}_{i=0}^{\infty}$ est un majorant définitif de cette suite dans $\mathbb{R}$ (de sorte que toute suite bornée dans $\mathbb{R}$ a un majorant définitif dans $\mathbb{R}$), mais il est possible que la suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ soit telle que certains des majorants définitifs de cette suite dans $\mathbb{R}$ ne sont pas des majorants de cette suite dans $\mathbb{R}$ (par exemple, le nombre réel $\frac{1}{5}$ est un majorant définitif dans $\mathbb{R}$ de la suite $\left\{\frac{1}{i+1}\right\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$, car, si $i > 3$, alors $\frac{1}{i+1} \leq \frac{1}{5}$, mais il n'est pas un majorant dans $\mathbb{R}$ de cette suite, car, si $0 \leq i \leq 3$, $\frac{1}{i+1} > \frac{1}{5}$). Or, si une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ est bornée dans $\mathbb{R}$, alors il y a un nombre réel $K$, tel que, quel que soit le nombre naturel $i$, $r_i > K$ et ni $K$ ni aucun autre nombre réel plus petit que $K$ ne peut donc être un majorant définitif de cette suite. D'autre part, une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ bornée dans $\mathbb{R}$ a sans doute des majorants, donc elle a sans doute des majorants définitifs. L'ensemble des majorants définitifs d'une suite $\{r_i\}_{i=0}^{\infty}$ à termes dans $\mathbb{R}$ bornée dans $\mathbb{R}$ est donc non vide et inférieurement borné. D'après l'axiome de la borne inférieure, il a donc une borne inférieure. On appelle cette borne inférieure « limite maximale de la suite $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$ ». Ces définitions ayant été données, il est maintenant facile d'énoncer, puis de prouver le lemme suivant :

*Lemme 2.* Si $\{r_i\}_{i=0}^{\infty}$ est une suite à termes dans $\mathbb{R}$ bornée dans $\mathbb{R}$, alors il y a une sous-suite de $\{r_i\}_{i=0}^{\infty}$ qui converge vers une limite dans $\mathbb{R}$.

On vient de prouver que si $\{r_i\}_{i=0}^{\infty}$ est une suite à termes dans $\mathbb{R}$ bornée dans $\mathbb{R}$, alors elle a une limite maximale dans $\mathbb{R}$, disons $R$. Mais, si un nombre réel $R$ est la limite maximale d'une suite $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$, alors, par la définition même de la limite maximale, tout nombre réel plus grand que $R$ est un majorant définitif de $\{r_i\}_{i=0}^{\infty}$ et donc, quel que soit le nombre réel strictement positif $\varepsilon$, il y aura un nombre naturel $n$, tel que

$$i > n \Rightarrow r_i \leq R + \varepsilon$$

Mais, s'il y avait un nombre naturel $m$ plus grand que $n$, tel que, pour tout nombre naturel $i$ plus grand ou égal à $m$, $r_i = R + \varepsilon$, alors aucun nombre réel plus petit que $R + \varepsilon$ ne pourrait être un majorant définitif de $\{r_i\}_{i=0}^{\infty}$, et donc $R+\varepsilon$ serait la limite maximale dans $\mathbb{R}$ de $\{r_i\}_{i=0}^{\infty}$,

contre l'hypothèse d'après laquelle $R$ est cette limite maximale. Donc, quel que soit le nombre réel strictement positif $\varepsilon$, il y aura un nombre naturel $n'$, tel que

$$i > n' \Rightarrow r_i < R + \varepsilon$$

D'un autre côté, toujours d'aprés la définition même de la limite maximale, aucun nombre réel plus petit que $R$ ne peut être un majorant définitif de $\{r_i\}_{i=0}^{\infty}$, et donc, quel que soit le nombre réel strictement positif $\varepsilon$, il y aura une infinité de valeurs de $i$ pour lesquelles

$$r_i > R - \varepsilon$$

car, si il n'y avait qu'un nombre fini de valeurs de $i$ qui satisfont à cette condition, alors $R - \varepsilon$ serait un majorant définitif de $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$, puisqu'il suffit de prendre un nombre naturel plus grand que n'importe laquelle de ces valeurs et de poser que $i$ est plus grand que ce nombre, pour en conclure que $r_i \leq R - \varepsilon$. Il s'ensuit que si $R$ est la limite maximale d'une suite $\{r_i\}_{i=0}^{\infty}$ dans $\mathbb{R}$, alors, pour tout nombre réel strictement positif $\varepsilon$, il y a une infinité de valeurs de $i$ qui satisfont à la condition

$$R - \varepsilon < r_i < R + \varepsilon$$

Qu'on pose alors $\varepsilon = 1$, comme ci-dessus. Il s'ensuit qu'on pourra trouver un nombre naturel $k_0$ tel que

$$R - 1 < r_{k_0} < R + 1$$

et donc

$$|r_{k_0} - R| < 1$$

De même, si on pose $\varepsilon = \frac{1}{2}$, on peut trouver un nombre naturel $k_1 > k_0$ tel que

$$R - \frac{1}{2} < r_{k_1} < R + \frac{1}{2}$$

et donc

$$|r_{k_1} - R| < \frac{1}{2}$$

Encore, si on pose $\varepsilon = \frac{1}{3}$, on peut trouver un nombre naturel $k_2 > k_1$ tel que

$$|r_{k_2} - R| < \frac{1}{3}$$

et ainsi de suite.

Il suffit alors de poser, pour tout nombre naturel $i$, $s_i = r_{k_i}$ et de choisir les nombres naturels $k_i$ $(i = 0, 1, 2, ...)$ comme on vient de dire pour obtenir une sous-suite $\{s_i\}_{i=0}^{\infty}$ de $\{r_i\}_{i=0}^{\infty}$, telle que, quel que soit le nombre naturel $h$, il y a un nombre naturel $n$, tel que

$$i > n \Rightarrow |s_i - R| < \frac{1}{h}$$

Mais, quel que soit le nombre réel strictement positif $\xi$, du théorème 4.3, il suit qu'il y a un nombre naturel strictement positif $k$, tel que

$$k\xi > 1$$

et donc, quel que soit le nombre réel strictement positif $\xi$ , il y a un nombre naturel strictement positif $k$, tel que

$$\frac{1}{k} < \xi$$

De là il suit que $\{s_i\}_{i=0}^{\infty}$ est telle que, quel que soit le nombre réel strictement positif $\xi$, il y a un nombre naturel $n$, tel que

$$i > n \Rightarrow |s_i - R| < \xi$$

et cette série est donc convergente vers la limite $R$ dans $\mathbb{R}$. Cela clôt la preuve du lemme 2.

De la conjonction du lemme 1 et du lemme 2, il suit que, si $\{r_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{R}$, alors il y a une sous-suite $\{s_i\}_{i=0}^{\infty}$ de $\{r_i\}_{i=0}^{\infty}$ qui converge vers une limite $R$ dans $\mathbb{R}$. Une suite de Cauchy à termes dans $\mathbb{R}$, $\{r_i\}_{i=0}^{\infty}$ étant donnée, on considère une sous-suite $\{s_i\}_{i=0}^{\infty}$ de $\{r_i\}_{i=0}^{\infty}$ qui converge vers une limite $R$ dans $\mathbb{R}$. Comme la suite $\{r_i\}_{i=0}^{\infty}$ est une suite de Cauchy à termes dans $\mathbb{R}$, quel que soit le nombre réel strictement positif $\varepsilon$, qu'on pourra bien prendre égale à $\frac{\eta}{2}$, $\eta$ étant un nombre réel strictement positif quelconque, il y a un un nombre naturel $n$, tel que, quel que soit le nombre naturel $m$, plus grand que $n$,

$$i > n \Rightarrow |r_i - r_m| < \varepsilon = \frac{\eta}{2}$$

Mais — comme, d'après la construction de la sous-suite $\{s_i\}_{i=0}^{\infty}$ de $\{r_i\}_{i=0}^{\infty}$, $s_i = r_{k_i}$, avec $k_i \geq i$ — on pourra poser $m = k_i$, et en conclure que

$$i > n \Rightarrow |r_i - s_i| < \varepsilon = \frac{\eta}{2}$$

De surcroît, comme la suite $\{s_i\}_{i=0}^{\infty}$ converge vers la limite $R$ dans $\mathbb{R}$, il y aura aussi, pour le même nombre réel strictement positif $\varepsilon$, un nombre naturel $n'$, tel que :

$$i > n' \Rightarrow |s_i - R| < \varepsilon = \frac{\eta}{2}$$

Et de là, il est facile de conclure que, quel que soit le nombre réel strictement positif $\eta$ :

$$i > Max(n, n') \Rightarrow |r_i - R| = |(r_i - s_i) + (s_i - R)| \leq |r_i - s_i| + |s_i - R| < \eta$$

et donc $\{r_i\}_{i=0}^{\infty}$ aussi converge vers la limite $R$ dans $\mathbb{R}$. □

La preuve précédente nous assure que l'ensemble $\mathbb{R}$ intervenant dans le corps commutatif totalement ordonné $< \mathbb{R}, +, \cdot, \leq >$ et satisfaisant à l'axiome de la borne supérieure (et donc aussi à celui de la coupure) est fermé par rapport à l'opération de passage à la limite des suites convergentes à termes dans $\mathbb{R}$ et satisfait ainsi à nos *desiderata*. Comme on peut aussi prouver que tous les ensembles qui satisfont à ces conditions sont isomorphes entre eux, ceci justifie la plus classique des définitions axiomatiques de $\mathbb{R}$ :

DÉFINITION 4.16. *L'ensemble des nombres réels est un ensemble, noté « $\mathbb{R}$ », tel que :*
*I) sont définies sur lui :*
*I.i) une relation d'ordre total, c'est-à-dire une relation, notée « $\leq$ » telle que :*
*I.i.i) si $x$ et $y$ sont des éléments de $\mathbb{R}$, alors ou bien $x \leq y$, ou bien $y \leq x$ ;*
*I.i.ii) si $x$, $y$ et $z$ sont des éléments de $\mathbb{R}$, et si $x \leq y$ et $y \leq z$, alors $x \leq z$ ;*
*I.i.iii) si $x$ et $y$ sont des éléments de $\mathbb{R}$, et si $x \leq y$ et $y \leq x$, alors $x = y$ ;*
*I.i.iv) si $x$ est un élément de $\mathbb{R}$, alors $x \leq x$ ;*
*I.ii) une addition commutative et associative, qui admet un (et un seul) élément neutre dans $\mathbb{R}$, et relativement à laquelle tous les éléments de $\mathbb{R}$ sont inversibles, c'est-à-dire une opération notée « + » telle que :*
*I.ii.i) si $x$ et $y$ sont des éléments de $\mathbb{R}$, alors $x + y$ est un élément de $\mathbb{R}$ ;*
*I.ii.ii) si $x$ et $y$ sont des éléments de $\mathbb{R}$, alors $x + y = y + x$ ;*
*I.ii.iii) si $x$, $y$ et $z$ sont des éléments de $\mathbb{R}$, alors $x + (y + z) = (x + y) + z$ ;*
*I.ii.iv) il y a un (et un seul) élément $0$ de $\mathbb{R}$ (dit « élément neutre de l'addition dans $\mathbb{R}$ » ), tel que si $x$ est un élément de $\mathbb{R}$, alors $x + 0 = 0 + x = x$ ;*
*I.ii.v) si $x$ est un élément de $\mathbb{R}$, alors il y a un et un seul élément $[-x]$ de $\mathbb{R}$, tel que $x + [-x] = [-x] + x = 0$ ;*
*I.iii) une multiplication, commutative et associative, qui admet un (et un seul) élément neutre dans $\mathbb{R}$ (différent de $0$), et relativement à laquelle tous les éléments de $\mathbb{R}$, sauf $0$, sont inversibles, c'est-à-dire une opération notée « $\cdot$ » telle que :*
*I.iii.i) si $x$ et $y$ sont des éléments de $\mathbb{R}$, alors $x \cdot y$ est un élément de $\mathbb{R}$ ;*

*I.iii.ii) si $x$ et $y$ sont des éléments de $\mathbb{R}$, alors $x \cdot y = y \cdot x$ ;*

*I.ii.iii) si $x$, $y$ et $z$ sont des éléments de $\mathbb{R}$, alors $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ ;*

*I.iii.iv) il y a un (et un seul) élément $1$ de $\mathbb{R}$ (dit « élément neutre de la multiplication dans $\mathbb{R}$ » ), tel que si $x$ est un élément de $\mathbb{R}$, alors $x \cdot 1 = 1 \cdot x = x$ ;*

*I.iii.v) si $x$ est un élément de $\mathbb{R}$, différent de $0$, alors il y a un et un seul élément $x^{-1}$ de $\mathbb{R}$, tel que $x \cdot x^{-1} = x^{-1} \cdot x = 1$ ;*

*II) si $x$, $y$ et $z$ sont des éléments de $\mathbb{R}$ et $x \leq y$, alors $x + z \leq y + z$ ;*

*III) si $x$ et $y$ sont des éléments de $\mathbb{R}$, $0 \leq x$ et $0 \leq y$, alors $0 \leq x \cdot y$ ;*

*IV) si $x$, $y$ et $z$ sont des éléments de $\mathbb{R}$, alors $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ ;*

*V) si $A$ est un sous-ensemble non vide de $\mathbb{R}$ supérieurement borné dans $\mathbb{R}$, alors il possède une borne supérieure dans $\mathbb{R}$.*

Le lecteur est invité à reconnaître dans les clauses *(I)*-$(\ IV)$ les conditions qui nous assurent que le quadruplet $< \mathbb{R}, +, \cdot, \leq >$ est un corps totalement ordonné. Ces clauses sont aussi satifaites par le quadruplet $< \mathbb{Q}, +, \cdot, \leq >$. Ce qui caractérise $\mathbb{R}$ et le distingue de manière essentielle de $\mathbb{Q}$, est la condition $(\ V)$ qui, dans la définition qu'on a finalement choisie, correspond à l'axiome de la borne supérieure. C'est cet axiome qui fait que $\mathbb{R}$ contient la limite de toute suite de Cauchy à termes dans $\mathbb{R}$. Du fait que $\mathbb{R}$ et $\mathbb{Q}$ ne diffèrent que par cet axiome, le théorème 4.1 (qui a été démontré en employant seulement des propriétés de $< \mathbb{Q}, +, \cdot, \leq >$ que ce quadruplet partage avec tout corps commutatif complètement ordonné) vaut aussi pour les suites de Cauchy à termes dans $\mathbb{R}$ et pour leurs limites réelles (et peut être prouvé dans ces cas de la même manière que pour les suites de Cauchy à termes dans $\mathbb{Q}$ et pour leurs limites rationnelles). Ainsi étendu, ce théorème constitue la base de la théorie des suites et des séries réelles, un des chapitres les plus fondamentaux de l'analyse réelle, comme on appelle généralement la théorie mathématique qui a pour objet les nombres réels et leurs relations.

NOTE HISTORIQUE 6.15. Bien que le nom de Dedekind soit traditionnellement lié à l'axiome de la coupure et, par là, à la définition axiomatique des nombres réels, la définition originaire que Dedekind lui-même proposa, dans son mémoire de 1872, *Stetigkeit und Irrationale Zahlen*, n'est guère axiomatique. Elle se présente plutôt, de même que la définition de Cantor, comme une construction à partir de la donnée de $\mathbb{Q}$.

Le but explicite de Dedekind était de fournir une définition purement arithmétique de la continuité. Voici ce qu'il écrit au troisième paragraphe de son mémoire : « [...] la manière dont les nombres irrationnels sont d'habitude introduits est basée directement sur la conception des grandeurs extensives — qui n'est à son tour nulle part définie soigneusement — et explique un nombre comme le résultat de l'acte de mesurer une telle grandeur au moyen d'une autre de la même espèce. Je prétends en revanche que l'arithmétique se développe par elle-même. » Dedekind se propose donc de comprendre quelle propriété d'une droite fait que celle-ci soit conçue comme continue, de chercher à généraliser cette propriété et de l'assigner ensuite à un ensemble, qui devra ainsi être à son tour conçu comme continu. Pour ce qui est du premier point, voici ce qu'il écrit quelques lignes plus loin : « Je trouve l'essence de la continuité [...] dans le principe suivant : ÒSi tous les points d'une ligne droite tombent dans deux classes, telles que chaque point de la première classe demeure à la droite de chaque point de la seconde classe, alors il existe un et un seul point qui produit cette division de tous les points en deux classes, en séparant la ligne droite en deux portionsÓ. » Le lecteur reconnaîtra dans ce principe une version géométrique de l'axiome de la coupure.

Pour pouvoir assigner la propriété énoncée par ce principe à un ensemble de nombres, Dedekind suppose que l'ensemble $\mathbb{Q}$ des nombres rationnels est donné, et définit sur cet ensemble ce qu'il appelle des « coupures », c'est-à-dire des couples $< A_1, A_2 >$ de sous-ensembles de $\mathbb{Q}$, tels que chaque élément de $A_1$ est plus petit que chaque élément de $A_2$ et l'union de $A_1$ et $A_2$ coïncide avec $\mathbb{Q}$. Soit alors $< A_1, A_2 >$ une certaine coupure dans $\mathbb{Q}$. Il est possible qu'il y ait un nombre rationnel $a$ qui appartient soit à $A_1$, soit à $A_2$ et qui est ou bien le plus grand des éléments de $A_1$, ou bien le plus petit des éléments de $A_2$. Dans ce cas, on dit que le nombre rationnel $a$ produit la coupure $< A_1, A_2 >$. Mais il est aussi facile de construire des coupures $< A_1, A_2 >$ telles qu'aucun nombre rationnel soit ou bien le plus grand des éléments de $A_1$, ou bien le plus petit des éléments de $A_2$. Un exemple très simple et immédiat est donné par une coupure définie comme il suit. Soit $n$ un nombre naturel différent de zéro tel qu'il n'y a aucun nombre naturel $m$ tel que $m^2 = n$. La position $n = 2$ ferait par exemple l'affaire. Pour chaque nombre rationnel $q$ on dira alors que $q$ appartient à $A_2$ si et seulement si $q^2 > n$ ; autrement, il appartient à $A_1$. Le couple $< A_1, A_2 >$ est alors une coupure, mais aucun nombre rationnel $a$ est ou bien le plus grand des éléments de $A_1$, ou bien le plus petit des éléments de $A_2$. Chaque fois qu'une coupure de cette sorte se produit dans $\mathbb{Q}$, nous dit Dedekind, « nous créons un nouveau nombre *irrationnel* $\alpha$, qui correspond à cette coupure, ou produit cette coupure ». De cette manière, toute coupure dans $\mathbb{Q}$ est produite soit par un nombre rationnel, soit par un nombre irrationnel. L'ensemble des nombres réels n'est alors pour Dedekind que l'ensemble des nombres rationnels ou irrationnels qui produisent des coupures dans $\mathbb{Q}$.

On voit que les coupures jouent ici le même rôle que les classes d'équivalence des suites de Cauchy dans la construction de Cantor. Pour parvenir, à la suite de cette définition, à une caractérisation de $\mathbb{R}$ qui assigne à cet ensemble les propriétés d'un corps ordonné, il faut ainsi étendre aux nombres irrationnels les opérations d'addition et de multiplication et la relation d'ordre définies sur les rationnels. Pour ce faire, Dedekind définit ces opérations et cette relation sur les coupures dans $\mathbb{Q}$ en transposant ensuite ces définitions aux nombres réels correspondants. Le lecteur n'aura aucune peine à imaginer comment ceci peut être fait.

**Lectures possibles** : R. Dedekind, *Essays on the Theory of Numbers*, Chicago, Open Court, 1901 (réimpression : Dover, New York, 1963).

### 5. Cardinalité de l'ensemble des réels

Malgré les analogies profondes entre $\mathbb{R}$ et $\mathbb{Q}$, le fait que $\mathbb{R}$ contient (selon qu'on le définit explicitement, en suivant la méthode de Cantor, ou si on le define implicitement par les axiomes intervenant dans la définition 4.16) ou bien toute suite de Cauchy à termes dans $\mathbb{Q}$, ou bien la limite de toute suite de Cauchy à termes dans $\mathbb{Q}$, marque une différence profonde entre ces deux ensembles. Il y a plusieurs manières de qualifier cette différence. La plus commune, déjà évoquée au début du paragraphe 4, consiste à dire que $\mathbb{R}$ n'est pas seulement, comme $\mathbb{Q}$, dense par rapport à $<$, mais qu'il est aussi continu : il ne comporte pas de lacunes ou, si on préfère le dire ainsi, il contient un élément pour tout segment qu'on peut prendre sur une droite à partir d'une origine donnée, et ses éléments se comportent, les uns relativement aux autres, comme les extremités de ces segments se comportent, les uns relativement aux autres. Cela explique la raison pour laquelle on représente généralement $\mathbb{R}$ par une droite et ses éléments par des points sur cette droite.

On pourrait croire que la différence entre la densité et la continuité n'est pas profonde et qu'en passant de $\mathbb{Q}$ à $\mathbb{R}$, on n'ait fait au fond que remplir quelques trous. Malgré le fait que ces deux propriétés aient souvent été confondues avant les travaux de Cantor et Dedekind (c'est par exemple, comme on l'a déjà rappelé, le cas de Kant, lors de sa célèbre définition de la continuité dans la *Critique de la raison pure*), ceci est faux. Une manière de le comprendre est de raisonner sur la cardinalité de $\mathbb{R}$. Comme $\mathbb{Q}$, dont il est une extension, $\mathbb{R}$ est évidemment un ensemble infini, mais, à la différence de $\mathbb{Q}$, il n'est pas dénombrable, c'est-à-dire qu'il n'est pas possible de le mettre en bijection avec l'ensemble $\mathbb{N}$ des nombres naturels. Non seulement il est plus grand que $\mathbb{N}$ (dans le sens que $\mathbb{N}$ est une partie propre de $\mathbb{R}$), mais il est, pour ainsi dire, tellement plus grand qu'il n'est pas possible d'ordonner tous ses éléments dans une suite infinie, dont chaque terme corresponde à un élément de $\mathbb{N}$, comme on peut par contre faire (et comme on l'a fait) pour $\mathbb{Q}$. C'est l'objet du théorème suivant, le dernier de ce cours :

THÉORÈME 5.1. *L'ensemble $\mathbb{R}$ n'est pas dénombrable, c'est-à-dire que ses éléments ne peuvent pas être rangés dans une suite dont chaque terme corresponde à un élément différent de $\mathbb{N}$, en étant l'image d'un élément différent de $\mathbb{N}$ selon une bijection. Ceci est aussi le cas de tout intervalle de $\mathbb{R}$, c'est-à-dire de tout sous-ensemble de $\mathbb{R}$ formé par tous les éléments de $\mathbb{R}$ compris (selon la relation $\leq$) entre deux éléments différents quelconques $x$ et $y$ de $\mathbb{R}$.*

La preuve de ce théorème qu'on va exposer ci-dessous est due à Cantor ; elle emploie une technique qui est devenue ensuite classique en logique et en mathématique, dite généralement « technique de diagonalisation ». Le lecteur comprendra tout seul la raison de cette appellation. En suivant la version originaire de cette preuve, je ne considérerai que l'intervalle de $\mathbb{R}$ compris entre 0 et 1 (ces limites étant incluses), c'est-à-dire le sous-ensemble, noté « $[0, 1]$ », de tous les éléments $x$ de $\mathbb{R}$, tels que $0 \leq x \leq 1$, qu'on dit, par le fait de contenir ces extrêmes, être un *intervalle fermé*de $\mathbb{R}$. Mais il est facile de comprendre qu'un argument analogue vaut pour tout autre intervalle de $\mathbb{R}$ (un intervalle étant évidemment dit « intervalle ouvert », ou simplement « ouvert », s'il ne contient pas ses extrêmes).

REMARQUE 6.21. Avant d'exposer cette preuve, il est pourtant nécessaire d'introduire un éclaircissement qui permettra de comprendre pourquoi ce même argument ne s'applique à aucun intervalle de $\mathbb{Q}$, et donc ne s'applique pas à $\mathbb{Q}$ tout entier.

Comme on l'a vu, un nombre rationnel quelconque peut s'écrire sous la forme du quotient $p : q = \frac{p}{q}$ de deux nombres relatifs $p$ et $q$, dont le deuxième est différent de 0. Pour simplifier, on ne considérera ici que les nombres rationnels positifs, c'est-à-dire les nombres rationnels qui peuvent s'écrire comme le quotient $p : q = \frac{p}{q}$ de deux nombres naturels $p$ et $q$, dont le second est différent de 0. Si $p = q \neq 0$, le nombre rationnel positif $\frac{p}{q}$ est égal à 1 ; si $p > q > 0$, il est plus grand que 1 ; et si enfin $q > p > 0$, il est plus petit que 1. Comme on ne considérera plus tard que les nombres réels compris entre 0 et 1, on écartera ici la deuxième possibilité et on posera donc $0 \leq p \leq q$ ; $q \neq 0$.

Imaginons qu'on veuille écrire le nombre rationnel positif $\frac{p}{q}$ comme la limite d'une suite telle que

$$\left\{ \sum_{i=0}^{j} \frac{p_i}{m^i} \right\}_{j=0}^{\infty}$$

(ou d'une série telle que $\sum_{i=0}^{\infty} \frac{p_i}{m^i}$), $m$ et $p_i$ $(i = 0, 1, 2, ...)$ étant des nombres naturels, tels que, quel que soit $i$, on ait $0 \leq p_i < m$ (il est clair que si, pour un certain nombre naturel $\nu$, $i \geq \nu \Rightarrow p_i = 0$, alors cette suite ne contient que des termes constants au-delà de son $i$-ième terme ; ce cas est naturellement possible et ne doit pas être écarté). Pour simplifier,

on adoptera la convention habituelle et on posera $m = 10$, ce qui fait que les nombres $p_i$ ne sont, pour toute valeur de $i$, que des nombres naturels choisis entre $0, 1, 2, ..., 9$. On dira alors que la suite

$$\left\{\sum_{i=0}^{\infty} \frac{p_i}{m^i}\right\}_{j=0}^{\infty} = \left\{\sum_{i=0}^{j} \frac{p_i}{10^i}\right\}_{j=0}^{\infty}$$

(ou la série $\sum_{i=0}^{\infty} \frac{p_i}{m^i} = \sum_{i=0}^{\infty} \frac{p_i}{10^i}$ ) fournit une écriture décimale du nombre $\frac{p}{q}$. Si $0 \leq p \leq q$; $q \neq 0$, cette écriture prendra (comme il sera facile de comprendre à partir de ce qu'on a observé à la fin du chapitre 1) la forme suivante

$$0, p_1 p_2 p_3 ...$$

(où 0 est la valeur de $p_0$ et les $p_i$ $(i = 1, 2, 3, ...)$ ne sont rien d'autre que des chiffres choisis parmi $0, 1, 2, ..., 9$, et dont la signification dépend de leur position, comme dans toute écriture numérique positionnelle).

Une manière simple de déterminer la suite $\{p_i\}_{i=1}^{\infty}$ de ces chiffres est d'appliquer l'algorithme de la division pour trouver le quotient de $p$ et $q$, ce qui donnera, comme chacun le sait pour l'avoir appris à l'école primaire :

$$\begin{array}{rcl} & p \;:\; q \;=\; 0, p_1 p_2 p_3 \ldots & \\ 10 \cdot [p - (0 \cdot q)] = & 10 \cdot p & \\ 10 \cdot [(10 \cdot p) - (p_1 \cdot q)] = & 10 \cdot r_1 & \\ 10 \cdot [(10 \cdot r_1) - (p_2 \cdot q)] = & 10 \cdot r_2 & \\ 10 \cdot [(10 \cdot r_2) - (p_3 \cdot q)] = & 10 \cdot r_3 & \\ \ldots & \ldots & \end{array}$$

Or, il est clair que si, pour un certain nombre naturel $h \neq 0$, le reste $r_h$ est égal à 0, c'est-à dire que $10 \cdot r_{h-1} = p_h \cdot q$, le quotient trouvé est un nombre décimal fini :

$$\frac{p}{q} = 0, p_1 p_2 p_3 ... p_h = \sum_{i=0}^{h} \frac{p_i}{10^i}$$

Mais, il se peut que ceci ne soit jamais le cas, comme il arrive, par exemple, lorsque $p = 1$ et $q = 3$. Il est en revanche toujours le cas que, quel que soit $i$, le reste $r_i$ respecte la condition $0 \leq r_i < q$, de sorte que, si ce reste n'est jamais nul, alors, parmi les premiers $q + 1$ restes, il y en aura sans doute au moins deux qui seront égaux entre eux. Or, il est facile de voir que si $r_h = r_k$, alors, le dénominateur $q$ étant constant dans la division, $p_{h+1} = p_{k+1}$ et donc $r_{h+1} = r_{k+1}$ et ainsi $p_{h+2} = p_{k+2}$ et $r_{h+2} = r_{k+2}$ et ainsi de suite, de sorte que, pour tout couple de nombres naturels différents de 0, $h$ et $k$, et tout nombre naturel $j$, on aura

$$r_h = r_k \Rightarrow p_{h+j} = p_{k+j}$$

On peut donc en conclure que le nombre décimal $0, p_1 p_2 p_3, ...$ ou bien s'arrête après une certaine décimale, ou bien présente, après une certaine décimale, une suite de décimaux qui se répète périodiquement (ce qu'on exprime en disant qu'il est *périodique*). Il ne pourra donc que s'écrire sous l'une ou l'autres des formes suivantes :

$$\begin{array}{rcl} \frac{p}{q} & = & 0, p_1 p_2 p_3 ... p_h \\ \frac{p}{q} & = & 0, p_1 p_2 p_3 ... \overline{p_h p_{h+1} p_{h+2} ... p_{k-1}} \end{array}$$

où la barre sous la succession de chiffres $p_h p_{h+1} p_{h+2} ... p_{k-1}$ indique que cette succession de chiffres se répète indéfiniment (c'est-à-dire qu'elle est la période du nombre en question). On note que, comme

$$0, p_1 p_2 p_3 \dots p_h = 0, p_1 p_2 p_3 \dots p_h 000 \dots = 0, p_1 p_2 p_3 \dots p_h \overline{0}$$

le premier cas se réduit, en vérité, au second ; ici on n'a distingué les deux cas que par souci de clarté (on note que si tous les $p_i$ sont égaux à 0, alors $0, p_1 p_2 p_3 ... = 0, 0000... = 0$, tandis que s'ils sont tous égaux à 9, alors $0, p_1 p_2 p_3 ... = 0, 9999... = 1$, de sorte que si on n'exclut pas ces deux cas, on doit comprendre dans notre intervalle également ses bornes 0 et 1).

Le point qu'il nous importe de retenir est le suivant : les nombres décimaux qui expriment des nombres rationnels ne sont pas quelconques ; ou bien ils sont finis, ou bien ils sont périodiques (il est en fait facile de répéter l'argument précédent pour n'importe quel couple de nombres relatifs $\pm p$ et $\pm q$, même si ce n'est que le cas des nombres rationnels positifs plus petits ou égaux à 1 qui nous intéresse ici). Ce n'est pourtant pas le cas des nombres décimaux correspondant à des nombres réels quelconques, car n'importe quelle suite $\left\{ \sum_{i=0}^{j} \frac{p_i}{10^i} \right\}_{j=0}^{\infty}$ (et donc n'importe quelle série $\sum_{i=0}^{\infty} \frac{p_i}{10^i}$), où l'on aura posé $p_0 = 0$ et $0 \leq p_i \leq 9$, est une suite (ou une série) de Cauchy à termes dans $\mathbb{Q}$, et elle correspond donc à un nombre réel compris entre 0 et 1, qui pourrait s'écrire ainsi :

$$0, p_1 p_2 p_3 ... \qquad (0 \leq p_i \leq 9 \ ; \ i = 1, 2, ...) \tag{107}$$

les décimaux $p_i$ $(i = 1, 2, ...)$ formant une suite quelconque.

Cette dernière remarque constitue la base de la preuve du théorème 5.1, qu'on va présenter maintenant. Celle-ci est, encore une fois, une preuve par l'absurde qui n'utilise pas le tiers exclu.

**Preuve du théorème 5.1.** Considérons les nombres réels compris entre 0 et 1, qu'on peut écrire sous la forme (107). En fait, on pourrait démontrer que ceux-ci sont tous les nombres réels compris entre 0 et 1 (limites incluses), mais ceci n'est pas important pour la preuve qui suit, car s'il existait d'autres nombres réels compris dans le même intervalle, la conclusion qu'on va tirer de cette preuve vaudrait *a fortiori*. Imaginons que l'ensemble de ces nombres soit dénombrable. On pourrait alors ranger la totalité de ces nombres dans un certain ordre et associer le premier de ces nombres à 1, le deuxième à 2, le troisième à 3, et ainsi de suite. Si on note alors par « $0, p_{1,i} p_{2,i} p_{3,i} ...$ » l'$i$-ième nombre réel dans cet ordre, chacun de ces nombres sera compris dans la liste suivante

$$\begin{aligned}
r_1 &= 0, p_{1,1} p_{2,1} p_{3,1} p_{4,1} p_{5,1} ... p_{n,1} ... \\
r_2 &= 0, p_{1,2} p_{2,2} p_{3,2} p_{4,2} p_{5,2} ... p_{n,2} ... \\
r_3 &= 0, p_{1,3} p_{2,3} p_{3,3} p_{4,3} p_{5,3} ... p_{n,3} ... \\
r_4 &= 0, p_{1,4} p_{2,4} p_{3,4} p_{4,4} p_{5,4} ... p_{n,4} ... \\
r_5 &= 0, p_{1,5} p_{2,5} p_{3,5} p_{4,5} p_{5,5} ... p_{n,5} ... \\
&\dots \\
r_n &= 0, p_{1,n} p_{2,n} p_{3,n} p_{4,n} p_{5,n} ... p_{n,n} ... \\
&\dots
\end{aligned}$$

$(0 \leq p_{n,i} \leq 9 \ ; \ i, n = 1, 2, ...)$. Ceci posé, considérons le nombre décimal $0, \lambda_1 \lambda_2 \lambda_3 \lambda_4, \lambda_5, \dots, \lambda_n \dots$ qu'on pourrait construire suivant la règle suivante : si $p_{1,1} = 1$, on pose $\lambda_1 = 2$ et si $p_{1,1} \neq 1$, on pose $\lambda_1 = 1$ ; si $p_{2,2} = 1$, on pose $\lambda_2 = 2$ et si $p_{1,1} \neq 1$, on pose $\lambda_2 = 1$ ; si $p_{3,3} = 1$, on pose $\lambda_3 = 2$ et si $p_{3,3} \neq 1$, on pose $\lambda_3 = 1$ ; ... ; si $p_{n,n} = 1$, on pose $\lambda_n = 2$ et si $p_{n,n} \neq 1$, on pose $\lambda_n = 1$, et ainsi de suite. Quel que soit le nombre naturel $\rho$ différent de 0, on aura donc $\lambda_\rho \neq p_{\rho,\rho}$. Or

il est facile de vérifier (et le lecteur pourra le faire comme exercice) que deux suites de Cauchy à termes dans $\mathbb{Q}$, $\left\{\sum_{i=0}^{j}\frac{\nu_i}{10^i}\right\}_{j=0}^{\infty}$ et $\left\{\sum_{i=0}^{j}\frac{\mu_i}{10^i}\right\}_{j=0}^{\infty}$ (et donc deux séries de Cauchy à termes dans $\mathbb{Q}$, $\sum_{i=0}^{\infty}\frac{\nu_i}{10^i}$ et $\sum_{i=0}^{\infty}\frac{\mu_i}{10^i}$), telles que $0 \leq \nu_i \leq 9$ et $0 \leq \mu_i \leq 9$ ne peuvent être égales, suivant la définition 4.4, qu'à condition que $\nu_i = \mu_i$ pour tout nombre naturel $i$. Il s'ensuit alors que le nombre décimal $0, \lambda_1\lambda_2\lambda_3\lambda_4\lambda_5, \ldots, \lambda_n \ldots$, qui est sans doute un nombre réel compris entre 0 et 1 (et correspond à la suite de Cauchy à termes dans $\mathbb{Q}\left\{\sum_{i=0}^{j}\frac{\lambda_i}{10^i}\right\}_{j=0}^{\infty}$ $(1 \leq \lambda_i \leq 2\ ; i = 1, 2, \ldots)$, et donc à la série de Cauchy à termes dans $\mathbb{Q}\sum_{i=0}^{\infty}\frac{\lambda_i}{10^i}$ $(1 \leq \lambda_i \leq 2\ ; i = 1, 2, \ldots)$), n'est égal à aucun nombre de la liste précédente, quel que soit l'ordre qu'on ait donné à cette liste, car, quel que soit le nombre naturel $i$, différent de 0, son $i$-ième décimal $\lambda_i$ sera, par construction, différent du $i$-ième décimal $p_{i,i}$ du $i$-ième nombre de cette liste. Donc cette liste ne contient pas ce nombre et elle ne contient donc pas tous les nombres réels compris entre 0 et 1 donc l'ensemble $[0, 1]$ n'est pas dénombrable. *A fortiori*, l'ensemble $\mathbb{R}$ ne peut donc pas l'être.

NOTE HISTORIQUE 6.16. Dans la note historique 4.6, j'ai fait référence à l'article de 1874, où Cantor démontre qu'il y a des nombres réels non algébriques. Comme je l'ai dit à cette occasion, la preuve de Cantor utilise de deux lemmes : i) l'ensemble des nombres réels algébriques est dénombrable ; ii) l'ensemble des nombres réels n'est pas dénombrable. Pour démontrer le second lemme, Cantor se sert d'un argument auquel il était parvenu en décembre 1873. Le 7 décembre il avait écrit à Dedekind une lettre qui commençait ainsi : « Ces derniers jours, j'ai eu le temps d'étudier, d'une façon un peu plus suivie, ma conjecture dont je vous avais parlé ; c'est seulement aujourd'hui que j'en ai terminé, me semble-t-il, avec cette affaire ; si je devais pourtant me tromper, je ne trouverais certainement pas de juge plus indulgent que vous. Je prends donc la liberté de soumettre à votre jugement ce que j'ai couché sur le papier, dans toute l'imperfection de ce premier jet ».

La conjecture dont parle Cantor est la non dénombrabilité de $\mathbb{R}$. La suite de la lettre esquisse une preuve de cette conjecture. La preuve est sans doute correcte, mais elle est aussi alourdie par un long argument initial qui n'est guère indispensable. Cantor ne prend pourtant pas plus de deux jours pour comprendre (peut-être grâce à une suggestion de Dedekind, qui lui répond le 8 décembre) que sa preuve peut être simplifiée, et le 9 décembre il écrit de nouveau à son correspondant : « J'ai déjà trouvé, pour le théorème démontré dernièrement, une démonstration simplifiée ». Cantor ne présente pas dans sa lettre cette preuve simplifiée dans les détails, mais ce qu'il en dit est largement suffisant pour comprendre qu'il s'agit pour l'essentiel de la même preuve qu'il présentera quelques mois plus tard dans son article à propos de l'existence de nombres réels non algébriques.

La preuve en question n'est pas celle qu'on vient de donner pour le théorème 4.2. Même si elle est sans aucun doute plus élégante et aussi plus apte à montrer — comme l'observe Cantor lui-même à la fin de sa première lettre à Dedekind — la « raison » pour laquelle l'ensemble $\mathbb{R}$ n'est pas dénombrable, elle est aussi moins immédiate et élémentaire que celle-ci. Cantor ne parvint à cette dernière preuve qu'en 1890 et l'exposa dans une courte note intitulée : « ?ber eine elementare Frage der Mannigfaltigkeitslehre » (Sur une question élémentaire de la théorie des multiplicités).

Comme celle de 1890, la preuve de 1873 est une preuve par l'absurde, et ne concerne que les nombres réels compris entre 0 et 1, même si, dans ce cas, les extrêmes 0 et 1 de cet intervalle sont exclus. Voici comment on peut la formuler.

Imaginons que les nombres réels appartenant à l'intervalle ouvert $(0,1)$ peuvent être comptés et rangés, par conséquence, dans une suite $\{r_i\}_{i=0}^{\infty}$ qui comprend la totalité de ces nombres. Évidemment, à cause de la densité de $\mathbb{Q}$, et donc de $\mathbb{R}$, par rapport à la relation $\leq$, l'ordre total exhibé par cette séquence devra être différent de l'ordre totale induit par cette dernière relation. Mais la densité de $\mathbb{R}$ par rapport à $\leq$ permet aussi de prendre dans l'intervalle $(0,1)$, deux nombres réels $\alpha$ et $\beta$ tels que $\alpha < \beta$, et de former ainsi l'intervalle ouvert $(\alpha, \beta)$ contenu dans $(0,1)$. Soient alors $\alpha' = r_{h'}$ et $\beta' = r_{k'}$ ($h'$, $k' \in \mathbb{N}$) les deux premiers termes de $\{r_i\}_{i=0}^{\infty}$ qui appartiennent à $(\alpha, \beta)$. Si $\{r_i\}_{i=0}^{\infty}$ contient la totalité des réels appartenant à $(0,1)$, comme $\mathbb{R}$ est dense par rapport à $\leq$, il y a certainement deux termes différents tels que ceux-ci, et comme ces termes sont justement différents entre eux, on peut supposer que $\alpha' < \beta'$. Si on considère alors l'intervalle ouvert $(\alpha', \beta')$, contenu dans $(\alpha, \beta)$, on peut réitérer la même opération et former l'intervalle ouvert $(\alpha'', \beta'')$ contenu dans $(\alpha', \beta')$, tel que $\alpha'' = r_{h''}$ et $\beta'' = r_{k''}$ ($h''$, $k'' \in \mathbb{N}$) sont les deux premiers termes de $\{r_i\}_{i=0}^{\infty}$ qui appartiennent $(\alpha', \beta')$. Dans ce cas aussi, la densité de $\mathbb{R}$ par rapport à $\leq$ et l'hypothèse dont on est parti, garantissent l'existence des termes $\alpha''$ et $\beta''$ et nous permettent de supposer que $(\alpha'' < \beta'')$. En continuant de cette manière, on pourra alors construire une suite $\{\alpha^{(i)}, \beta^{(i)}\}_{i=0}^{\infty}$ d'intervalles emboîtés, tous contenus dans $(0,1)$. Or, comme, par construction, quels que soient les indices $\mu$ et $\nu$, $\alpha^{(\mu)} < \beta^{(\nu)}$, les suites respectivement croissante et décroissante $\{\alpha^{(i)}\}_{i=0}^{\infty}$ et $\{\beta^{(i)}\}_{i=0}^{\infty}$ sont respectivement supérieurement et inférieurement bornées dans $\mathbb{R}$. D'après l'axiome de la borne supérieure, elles possèdent donc respectivement une borne supérieure $\alpha^{(\infty)}$ et une borne inférieure $\beta^{(\infty)}$ dans $\mathbb{R}$. Il n'est pas difficile de comprendre que, par construction, $\alpha^{(\infty)} \leq \beta^{(\infty)}$. Or, si $\alpha^{(\infty)} < \beta^{(\infty)}$, alors il y a un intervalle ouvert $(\alpha^{(\infty)}, \beta^{(\infty)})$, contenu dans $(0,1)$, qui ne peut, à son tour, contenir aucun terme de la suite $\{r_i\}_{i=0}^{\infty}$. Mais, comme $\mathbb{R}$ est dense par rapport à $\leq$, cet intervalle devra contenir au moins un nombre réel appartenant à $(0,1)$. Donc, s'il en était ainsi, de l'hypothèse d'après laquelle la suite $\{r_i\}_{i=0}^{\infty}$ comprend tous les nombres réels appartenant à l'intervalle ouvert $(0,1)$, il suivrait qu'il y a au moins un nombre réel appartenant à cet intervalle qui n'est pas compris dans la suite $\{r_i\}_{i=0}^{\infty}$. D'autre part, si $\alpha^{(\infty)} = \beta^{(\infty)}$ alors, pour la construction des intervalles $(\alpha^{(i)}, \beta^{(i)})$, il n'est pas possible que $\alpha^{(\infty)}(= \beta^{(\infty)})$ soit compris dans la suite $\{r_i\}_{i=0}^{\infty}$. En effet, s'il en était ainsi, alors il y aurait un indice $n$, tel que $r_n = \alpha^{(\infty)} = \beta^{(\infty)}$, et, quel que soit cet indice, ce serait un nombre naturel fini, et il ne pourrait donc pas y avoir une infinité de termes de la suite $\{r_i\}_{i=0}^{\infty}$ précédant $r_n$, tous plus petits que $\alpha^{(\infty)}(= \beta^{(\infty)})$, ni une infinité des termes de la suite $\{r_i\}_{i=0}^{\infty}$ précédant $r_n$ tous plus grands que $\beta^{(\infty)}(= \alpha^{(\infty)})$, comme le veut par contre la construction des intervalles $(\alpha^{(i)}, \beta^{(i)})$. Encore une fois, s'il en était ainsi, de l'hypothèse d'après laquelle la suite $\{r_i\}_{i=0}^{\infty}$ comprend tous les nombres réels appartenant à l'intervalle ouvert $(0,1)$, il suivrait qu'il y a au moins un nombre réel appartenant à cet intervalle qui n'est pas compris dans la suite $\{r_i\}_{i=0}^{\infty}$. Mais les deux cas considérés sont les seuls possibles, et donc l'hypothèse d'après laquelle la suite $\{r_i\}_{i=0}^{\infty}$ comprend tous les nombres réels appartenant à l'intervalle ouvert $(0,1)$ implique sa négation, et doit donc être rejetée.

Telle qu'on vient de la formuler, la preuve précédente emploie l'axiome de la borne supérieure et montre donc comment et pourquoi la non dénombrabilité de $\mathbb{R}$

dépend du fait que $\mathbb{R}$ satisfait à cet axiome, tout en étant dense par rapport à $\leq$. Il n'est pourtant pas difficile de formuler la même preuve de manière à y faire intervenir directement l'axiome de la coupure, duquel on ferait ainsi directement découler la non dénombrabilité de $\mathbb{R}$. C'est une confirmation indirecte de l'équivalence de ces deux axiomes.

**Lectures possibles** : J. Cavaillès (éd.) « Correspondance Cantor-Dedekind », *in* J. Cavaillès, *Philosophie mathématique*, Hermann, Paris, 1962, pp. 177-251 ; J. W. Dauben Dauben, *Georg Cantor. His Mathematics and Philosophy of the Infinite*, Princeton Univ. Press, Princeton, 1979.

On exprime souvent le contenu du théorème précédent, en disant que $\mathbb{R}$ a la « cardinalité du continu ». En effet, la non dénombrabilité de $\mathbb{R}$ est une conséquence du fait que $\mathbb{R}$ satisfait à la condition exprimée par l'axiome de la coupure (ou par l'axiome de la borne supérieure). Ces deux conditions ne sont pas, pour autant, équivalentes : un ensemble peut ne pas être dénombrable et ne pas satisfaire non plus à la condition exprimée par l'axiome de la coupure (ou par l'axiome de la borne supérieure). Un exemple fort connu est donné par un ensemble défini pour la première fois par G. Cantor, qu'on appelle de ce fait « ensemble de Cantor » ou parfois simplement « cantor ».

Considérons l'intervalle fermé $[0, 1]$ de $\mathbb{R}$, qu'on appellera « $I$ », par soucis de briévité, et, pour rendre la construction plus tangible, imaginons de représenter cet intervalle par un segment $\mathsf{AB}$, dans lequel on inclura les extremités $\mathsf{A}$ et $\mathsf{B}$, ce que, comme on a vu ci-dessus, il est permis de faire. Considérons maintenant les nombres rationnels $\frac{1}{3}$ et $\frac{2}{3}$ ; ce sont bien sûr des nombres réels et il appartiennent à $I$ ; les points de $\mathsf{AB}$ qui correspondent à ces nombres, disons respectivement $\mathsf{A}_1$ et $\mathsf{B}_1$, partagent de surcroît ce segment en trois parties égales. Éliminons alors de $I$ l'intervalle fermé $[\frac{1}{3}, \frac{2}{3}]$, ou de $\mathsf{AB}$ le segment $\mathsf{A}_1\mathsf{B}_1$, incluant ses limites. Ils restera les deux demi-ouverts $[0, \frac{1}{3})$ et $(\frac{2}{3}, 1]$, c'est-à-dire les deux segments, privés d'une de leurs extremités, $\mathsf{AA}_1$ et $\mathsf{B}_1\mathsf{B}$. Considérons l'union de ces intervalles et formons l'ensemble $I_1 = [0, \frac{1}{3}) \cup (\frac{2}{3}, 1]$ qui ne sera évidemment pas un intervalle. Qu'on accomplisse maintenant la même opération qu'on a accomplie sur $I$ ou sur $\mathsf{AB}$, sur les deux parties de cet ensemble, c'est-à-dire sur les deux intervalles $[0, \frac{1}{3})$ et $(\frac{2}{3}, 1]$ ou sur les deux segments $\mathsf{AA}_1$ et $\mathsf{B}_1\mathsf{B}$, en partageant le premier par les nombres $\frac{1}{9}$ et $\frac{2}{9}$ et le deuxième par les nombres $\frac{7}{9}$ et $\frac{8}{9}$, correspondant respectivement aux points $\mathsf{A}_2$ et $\mathsf{A}_3$ et $\mathsf{B}_2$ et $\mathsf{B}_3$. En prenant encore l'union des intervalles restant après avoir éliminé les intervalles $[\frac{1}{9}, \frac{2}{9}]$ et $[\frac{7}{9}, \frac{8}{9}]$, ou bien les segments $\mathsf{A}_2\mathsf{A}_3$ et $\mathsf{B}_2\mathsf{B}_3$, incluant leurs limites, on aura l'ensemble $I_2 = [0, \frac{1}{9}) \cup (\frac{2}{9}, \frac{1}{3}) \cup (\frac{2}{3}, \frac{7}{9}) \cup (\frac{8}{9}, 1]$, qui ne sera pas non plus un intervalle. Pour construire l'ensemble de Cantor, il n'y a qu'à réitérer cette procédure à l'infini, en obtenant un ensemble $I_\infty$ qui résultera formé par l'union d'une infinité d'éléments ou points.

Or, comme à chaque étape de la construction, on dédouble le nombre des termes qui composent l'union $I_\nu$, par rapport à l'étape précédente, il s'ensuit que, aprés $\nu$ étapes, on aura un ensemble formé par l'union de $2^\nu$ intervalles ou segments. L'ensemble $I_\infty$ de Cantor, qu'on note généralement par la lettre « $C$ » en l'honneur de Cantor même, sera ainsi formé, par $2^{\aleph_0}$ éléments, (cf. la note historique 6.10). On comprendra ainsi, mais la chose peut être prouvée formellement sans difficulté, que le cantor n'est pas dénombrable. De plus, comme l'ensemble $\mathbb{R}$ des nombres réels peut être défini comme l'ensemble de toutes les classes d'équivalences de suites de Cauchy à termes en $\mathbb{Q}$, il peut être pensé comme un ensemble d'ensembles de sous-ensembles de $\mathbb{Q}$ et il n'est pas difficile de montrer que sa cardinalité est celle de l'ensemble de tous les sous-ensembles de $\mathbb{Q}$. Mais comme $\mathbb{Q}$ est dénombrable, c'est-à-dire qu'il a la même cardinalité que $\mathbb{N}$, et qu'un ensemble de $\nu$ éléments contient exactement $2^\nu$ sous-ensembles (le lecteur pourra le vérifier comme exercice), il n'est pas difficile de prouver que la cardinalité de $\mathbb{R}$ est, elle-aussi, $2^{\aleph_0}$. Donc le cantor peut être mis en bijection avec $\mathbb{R}$.

D'autre part, on peut aussi comprendre que le cantor, ne présente l'aspect ni d'un intervale, ni d'une union d'intervalles. En effet, on peut prouver qu'aucun sous-intervalle de $I$ est inclus dans le cantor, c'est-à-dire que, quels que soient les éléments $x$ et $y$ de $I$ qui sont aussi des éléments de $C$, l'intervalle $(x, y)$ n'est pas un sous-ensemble de $C$.

Comme l'ensemble $C$ de Cantor peut être mis en bijection avec $\mathbb{R}$, il peut être aussi mis en bijection avec l'ensemble des points qu'on peut distinguer géométriquement sur une droite. Il ne possède pas pourtant une propriété essentielle d'une droite qui fait qu'elle est continue : ses éléments (ou points) sont tous déconnectés les uns des autres. Cet exemple nous permet de comprendre qu'on ne peut pas définir la propriété de continuité pour un ensemble de telle sorte que cette propriété ne dépende que de la cardinalité de cet ensemble, c'est-à-dire de la possibilité de mettre cet ensemble en bijection avec l'ensemble des points qu'on peut distinguer géométriquement sur une droite. Si on accepte que $\mathbb{R}$ est un ensemble continu, on doit en conclure que les conditions qui caractérisent $\mathbb{R}$ sont essentiellement plus fortes que les conditions qui caractérisent un ensemble dont la cardinalité est $2^{\aleph_0}$, c'est-à-dire qu'elle est égale à la cardinalité de l'ensemble de tous les sous-ensembles possibles d'un ensemble dénombrable. Dit en d'autres termes : la propriété de continuité d'un ensemble n'est pas simplement une question de dimension de cet ensemble, elle dépend aussi, essentiellement, de la manière selon laquelle les éléments de cet ensemble se comportent les uns par rapport aux autres.

Du fait qu'on ne peut pas faire dépendre la continuité d'un ensemble de sa seule cardinalité, il suit que l'ensemble $\mathbb{R}$ ne peut qu'être caractérisé comme un ensemble intervenant dans une structure. Les considérations précédentes nous suggèrent trois manières pour caractériser la propriété de continuité d'un ensemble ; d'autres sont connues, mais elle ne seront pas évoquées ici. Selon qu'on choisit l'une ou l'autre de ces manières, il faut supposer que l'ensemble qu'on veut qualifier de continu participe d'une structure plus ou moins complexe. Si on se limite aux caractérisations suggérées par les considérations précédentes, on aura par exemple la situation suivante. Si on veut dire qu'un ensemble est continu si et seulement s'il est dense par rapport à la relation d'ordre $\leq$ et satisfait à l'axiome de la coupure, il faut supposer que cet ensemble est totalement ordonné relativement à la relation $\leq$. De même, si on veut dire qu'un ensemble est continu si et seulement s'il est dense par rapport à la relation d'ordre $\leq$ et satisfait à l'axiome de la borne supérieure. Si on veut dire, en revanche, qu'un ensemble est continu si et seulement si une suite à termes dans cet ensemble est convergente vers une limite dans cet ensemble si et seulement si c'est une suite de Cauchy, alors, il faut suposer qu'un tel ensemble participe d'une structure qui rende possible d'y définir des suites de Cauchy et de dire à quelles conditions une suite à terme dans cet ensemble converge vers une limite dans ce même ensemble. Comme on l'a déjà dit, cela peut être fait sans qu'il soit nécessaire de définir sur cet ensemble une relation d'ordre ; la définition d'une distance convenable est suffisante. Ainsi la différence entre cette dernière définion et les deux autres est qu'elle fait dépendre la propriété de continuité d'un ensemble, non pas de l'ordre défini sur cet ensemble, mais de sa structure métrique. C'est la raison pour laquelle certains préfèrent cette dernière définition aux deux autres. Expliquer convenablement les raisons de cette préférence nous éloignerait pourtant trop des objectifs du présent cours.

Le lecteur pourra considérer les observations précédentes comme une manière d'indiquer une des problématiques qui sont liées au choix d'une définition de la propriété de continuité d'un ensemble, et qui font de la question de la détermination de ce choix une des questions les plus passionantes autant de la logique mathématique que de la philosophie des mathématiques. Pour donner un cadre précis à la discussion, qui, depuis les acquisitions de Cantor et Dedekind, s'est développée autour de cette question, il faudrait pourtant ouvrir un chapitre assez complexe de logique mathématique et de théorie des ensembles.

Je préfère donc, pour l'instant, m'arrêter là.

7

# Index Analytique

**B**



**C**

**D**

**E**

**F**

**N**

**O**



**P**

**Q**



**R**

**S**

**T**

# Index