Théorie des grandeurs, arithmétisation, théorie de la divisibilité

Stefan Neuwirth

Le Barboux, 18 janvier 2016

Je montrerai dans une première partie comment les Grecs et les Arabes ont développé une théorie des grandeurs géométriques (longueur, aire, volume) qui a abouti à leur arithmétisation, c'est-à-dire à leur réduction aux nombres entiers. Dans une deuxième partie, je décrirai les deux approches concurrentes de Dedekind et de Kronecker pour l'extension d'une théorie de la divisibilité des nombres entiers aux nombres algébriques après Kummer et je développerai les options philosophiques de ces deux mathématiciens du 19$^{\text{e}}$ siècle.

Début du cinquième livre des *Éléments* d'Euclide, dit livre des proportions.

Les *Éléments* datent des premières décennies du 3$^{\text{e}}$ siècle avant l'ère chrétienne.

Définition V.1. Une grandeur est une *partie* d'une grandeur, la plus petite de la plus grande, quand elle mesure la plus grande.

Définition V.2. Et *multiple*, la plus grande de la plus petite, quand elle est mesurée par la plus petite.

Définition V.3. Un *rapport* est la relation, telle ou telle, selon la taille, [qu'il y a] entre deux grandeurs du même genre.

{**Définition V.3bis.** Et une *proportion* est l'identité des rapports.}

Définition V.4. 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.

Définition V.5. Des grandeurs sont dites *être dans le même rapport*, une première relativement à une deuxième et une troisième relativement à une quatrième quand des 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.

Extrait de la traduction du second livre du commentaire d'al-Khayyām sur les *Éléments* d'Euclide, *Exposé sur le rapport et la notion de proportionnalité, et sur leur véritable nature.*

Ce commentaire date de 1077. Les mots entre chevrons sont ceux que le traducteur a rajoutés pour la clarté de la phrase.

§ 2. [...] En effet, chaque fois que l'on a deux grandeurs homogènes, ou bien elles sont égales, ou bien elles sont différentes. Et la différence a des limites et des divisions. C'est-à-dire que la plus petite est ou bien une partie de la plus grande – en effet elle la mesure et la remplit exhaustivement lors de la mise en relation –, ou bien elle est des parties, ou bien elle est selon une autre manière. Une des propriétés de la quantité est de <pouvoir> y considérer l'égalité et l'inégalité. Le rapport est donc cette considération elle-même lorsque l'on met en relation les <grandeurs> homogènes, ainsi que la considération d'une autre chose qui est jointe à elle, à savoir, la grandeur de ce rapport en tant qu'il est rapport entre grandeurs.

§ 3. Cela est particulièrement clair dans le cas des choses numériques ; et le premier lieu où l'on trouve cette notion, je veux dire le rapport, c'est dans les choses numériques. C'est-à-dire que l'on considéra les nombres rapportés les uns aux autres, et l'on trouva qu'ils étaient ou bien égaux entre eux, ou bien inégaux. (Cela fait partie des propriétés de la quantité.) On considéra ensuite l'inégalité, et l'on trouva

— ou bien que la plus petite mesurait la plus grande – par exemple trois relativement à neuf. On rechercha alors la quantité de la mesure de neuf par trois, et l'on trouva que c'était trois. Donc trois mesure neuf trois fois. On dériva alors de cette notion un nom conformément aux langues, et l'on dit : *C'est le tiers. Donc le rapport entre trois et neuf est le fait d'être un tiers.* Et c'est là la considération de l'égalité et de l'inégalité jointe à une autre considération, comme nous l'avons expliqué. Et le rapport entre neuf et trois est le trois multiplicatif. Mais l'on ne dériva pas de nom pour cela, et l'on se contenta du premier. Cela dépend de celui qui a posé <les règles> du langage.

— ou bien qu'elle ne mesurait pas la plus grande – par exemple le rapport de deux à sept. On les divisa alors en parties qui mesuraient tout ensemble sept et deux, et l'on ne trouva pas un autre nombre : au contraire, on trouva l'unité. On dit alors : *Le rapport de deux à sept est deux septièmes.*

On démontra ensuite que les nombres les plus petits étaient soit une partie, soit des parties des plus grands.

§ 4. Et lorsque l'on vit que le nombre était de même genre que la grandeur du fait qu'ils se subdivisaient tous deux sous le genre de la quantité, on rechercha aussi cette notion dans les grandeurs. Et l'on y trouva en plus de ces deux divisions-là une autre division. C'est-à-dire que les grandeurs ne sont pas composées de parties indivisibles, et il n'y a pas de limite définie à leur division comme pour le nombre.

§ 5. Car le nombre est composé de parties indivisibles, i. e. les unités. Chaque fois que l'on a deux nombres différents, on retranche du plus grand tous les multiples du plus petit, et l'on arrivera à un reste plus petit que le plus petit nombre ; on retranche ensuite du plus petit tous les multiples du reste, et l'on arrivera à un reste plus petit que le premier reste ; et l'on ne cesse de procéder ainsi ; on arrivera alors nécessairement à un reste qui mesure le reste qui le précède, ou bien à l'unité. C'est-à-dire que les deux nombres sont finis et donnés, et sont composés d'unités indivisibles. Et quand nous disons *composé* dans la définition du nombre, c'est de par la nécessité de l'expression. Car *combinaison*, *multiplicité*, *collection*, et *nombre* ont tous le même sens. Il a déjà mentionné cela en partie au début du septième <Livre> de son ouvrage. Et il te sera possible de le reconnaître avec un minimum de réflexion.

§ 6. Quant aux grandeurs, elles ne sont pas composées de parties indivisibles, et il n'y a pas de limite déterminée à leur division. Ainsi, cette notion ne s'ensuit pas pour tous les cas ; et il n'est pas nécessaire que l'on parvienne inévitablement à l'unité (puisqu'il n'y a pas dans leur cas d'unité), ni à un reste qui mesure celui qui le précède. Et ce n'est que par une démonstration que l'on saura si cette notion y existe. Euclide en a déjà longuement parlé dans le dixième <Livre> de son ouvrage, mais nous n'en avons absolument pas besoin dans cette explication.

§ 7. Et puisqu'il en est ainsi, il ne s'ensuivra pas nécessairement, chaque fois que l'on aura deux grandeurs, que la plus petite soit ou bien une partie de la plus grande, ou bien des parties. Il sera au contraire possible qu'elle soit selon une autre espèce qui n'est pas numérique mais propre aux grandeurs. Et si quelqu'un dit : Cette troisième division n'existe absolument pas ; au contraire, elle fait partie des deux divisions numériques ! nous lui répondrons et nous lui dirons : Il n'y aura aucun mal à ce que nous considérions les lois du rapport et de la proportionnalité dans le cas des grandeurs de ces trois points de vue. Si ensuite la division est abrogée par une démonstration, il n'y aura aucun reproche à nous faire. Mais si elle n'est abrogée, nous aurons alors avancé et épuisé toutes les divisions. C'est là un mystère d'où l'on découvrira des mystères de logique extrêmement profonds. Comprends-le donc.

§ 8. Il mentionne ensuite la proportionnalité en disant : *C'est la similitude des rapports.* C'est là, quant au langage, des propos excellents, si ce n'est qu'il s'est complètement écarté de la véritable nature de la proportionnalité en commentant cette expression. C'est-à-dire qu'il a dit : *Si l'on a quatre grandeurs homogènes, que l'on prenne à l'infini des équimultiples de la première et de la troisième, et des équimultiples de la deuxième et de la quatrième, quels qu'il soient, et qu'on les compare ; et que, lorsque le multiple de la première excède le multiple de la deuxième, le multiple de la troisième excède le multiple de la quatrième, et que lorsqu'il lui est égal, il lui est aussi égal, et que lorsqu'il est plus petit que lui, il est plus petit que lui, si on les compare successivement ; on dira alors que le rapport de la première à la deuxième est égal au rapport de la troisième à la quatrième. Et qu'elles soient appelées proportionnelles.*

§ 9. Mais cela n'est pas construit à partir de la proportionnalité véritable. Ne vois-tu pas que si quelqu'un pose une question, disant : Quatre grandeurs sont proportionnelles selon la proportionnalité euclidienne, et la première est la moitié de la deuxième ; est-ce que la troisième sera alors égale à la moitié de la quatrième, ou non ? Comment sera-t-il alors possible de démontrer que la troisième est aussi égale à la moitié de la quatrième par la méthode d'Euclide ? Et si l'on répond en disant : Il faut, si la première est égale à la moitié de la deuxième, que la troisième soit égale à la moitié de la quatrième, en raison de l'existence de la proportionnalité ; quelle est la démonstration que l'on a pour dire que ce qu'Euclide a expliqué appartient aux conséquences nécessaires de la véritable proportionnalité ?

. . . .

§ 12. Je dis : J'ai conçu la véritable nature du rapport entre grandeurs. C'est-à-dire que chaque fois que l'on a deux grandeurs, ou bien l'une d'elles est égale à l'autre, ou bien elle ne l'est pas. Et celle qui est inégale sera ou bien une partie de l'autre, ou bien des parties. (Ces trois constituent le rapport numérique.) Ou bien elle sera selon une autre sorte propre à la géométrie, comme nous l'avons déjà expliqué précédemment.

§ 13. Et si l'on a quatre grandeurs, et que la première est égale à la deuxième, et la troisième égale à la quatrième ; ou que la première est une partie de la deuxième, et la troisième cette même partie de la quatrième ; ou que la première est des parties de la deuxième, et la troisième ces mêmes parties de la quatrième ; alors le rapport de la première à la deuxième sera inévitablement égal au rapport de la troisième à la quatrième. Ce rapport est numérique.

§ 14. Et s'il n'en est pas selon ces trois manières, mais, que l'on retranche de la deuxième tous les multiples de la première jusqu'à ce que l'on arrive à un reste plus petit que la première, et que de même l'on retranche de la quatrième tous les multiples de la troisième jusqu'à ce que l'on arrive à un reste plus petit que la troisième, et que le nombre des multiples de la première contenus dans la deuxième soit égal au nombre des multiples de la troisième contenus dans la quatrième ; et que l'on retranche de la première tous les multiples du reste de la deuxième jusqu' à ce que l'on arrive à un reste plus petit que le reste de la deuxième, et que de même l'on retranche de la troisième tous les multiples du reste de la quatrième jusqu'à ce que l'on arrive à un reste plus petit que le reste de la quatrième, et que le nombre des multiples du reste de la deuxième soit égal au nombre des multiples du reste de la quatrième ; et que de même l'on retranche du reste de la deuxième tous les multiples du reste de la première, et que l'on retranche du reste de la quatrième tous les multiples du reste de la troisième, et que leur nombre soit égal ; et que de même l'on retranche successivement tous les multiples des restes les uns des autres comme nous l'avons expliqué, et que le nombre de chaque reste de la première et de la deuxième soit indéfiniment égal au nombre du reste correspondant de la troisième et de la quatrième ; alors, le rapport de la première à la deuxième sera inévitablement égal au rapport de la troisième à la quatrième. Voilà la véritable proportionnalité relative au type géométrique.

SUR

LES HYPOTHÈSES QUI SERVENT DE FONDEMENT A LA GÉOMÉTRIE.

Mémoires de la Société Royale des Sciences de Göttingue, t. XIII; 1867 (¹).
Œuvres de Riemann, 2ᵉ édit., p. 272. — (Traduction de J. Hoüel).

PLAN DE CETTE ÉTUDE.

On sait que la Géométrie admet comme données préalables non seulement le concept de l'espace, mais encore les premières idées fondamentales des constructions dans l'espace. Elle ne donne de ces concepts que des définitions nominales, les déterminations essentielles s'introduisant sous forme d'axiomes. Les rapports mutuels de ces données primitives restent enveloppés de mystère; on n'aperçoit pas bien si elles sont nécessairement liées entre elles, ni jusqu'à quel point elles le sont, ni même *a priori* si elles peuvent l'être.

Depuis Euclide jusqu'à Legendre, pour ne citer que le plus illustre des réformateurs modernes de la Géométrie, personne, parmi les mathématiciens ni parmi les philosophes, n'est parvenu à éclaircir ce mystère. La raison en est que le concept général des grandeurs de dimensions multiples, comprenant comme cas parti-

(¹) Ce Mémoire a été lu par l'Auteur le 10 juin 1854 à l'occasion de ses épreuves d'admission à la Faculté philosophique de Göttingue. Ainsi s'explique la forme de son exposition, où les recherches analytiques ne sont qu'indiquées. On trouvera quelques éclaircissements dans les Notes au Mémoire envoyé en réponse à une question mise au Concours par l'Institut de Paris. (*Voir* Riemann, 2ᵉ édit., p. 405). — (Weber et Dedekind.)

culier les grandeurs étendues, n'a jamais été l'objet d'aucune étude. En conséquence, je me suis posé d'abord le problème de construire, en partant du concept général de grandeur, le concept d'une grandeur de dimensions multiples. Il ressortira de là qu'une grandeur de dimensions multiples est susceptible de différents rapports métriques, et que l'espace n'est par suite qu'un cas particulier d'une grandeur de trois dimensions. Or, il s'ensuit de là nécessairement que les propositions de la Géométrie ne peuvent se déduire des concepts généraux de grandeur, mais que les propriétés, par lesquelles l'espace se distingue de toute autre grandeur imaginable de trois dimensions, ne peuvent être empruntées qu'à l'expérience. De là surgit le problème de rechercher les faits les plus simples au moyen desquels puissent s'établir les rapports métriques de l'espace, problème qui, par la nature même de l'objet, n'est pas complètement déterminé; car on peut indiquer plusieurs systèmes de faits simples, suffisants pour la détermination des rapports métriques de l'espace. Le plus important, pour notre but actuel, est celui qu'Euclide a pris pour base. Ces faits, comme tous les faits possibles, ne sont pas nécessaires; ils n'ont qu'une certitude empirique, ce sont des hypothèses. On peut donc étudier leur probabilité, qui est certainement très considérable dans les limites de l'observation, et juger d'après cela du degré de sûreté de l'extension de ces faits en dehors de ces mêmes limites, tant dans le sens des immensurablement grands que dans celui des immensurablement petits.

A. — Concept d'une grandeur de n dimensions.

En essayant maintenant de traiter le premier de ces problèmes, relatif au développement du concept d'une grandeur de dimensions multiples, je me crois d'autant plus obligé de solliciter l'indulgence des lecteurs, que je suis moins exercé dans les travaux philosophiques de cette nature, dont la difficulté réside plutôt dans la conception que dans la construction, et qu'à l'exception de quelques brèves indications données par M. Gauss dans son second Mémoire sur les résidus biquadratiques, dans les

Gelehrte Anzeigen de Gœttingue et dans son Mémoire de jubilé, et de quelques recherches philosophiques de Herbart, je n'ai pu m'aider d'aucun travail antérieur.

§ I.

Les concepts de grandeur ne sont possibles que là où il existe un concept général qui permette différents modes de détermination. Suivant qu'il est, ou non, possible de passer de l'un de ces modes de détermination à un autre, d'une manière continue, ils forment une variété [1] continue ou une variété discrète; chacun en particulier de ces modes de détermination s'appelle, dans le premier cas, un point, dans le second un élément de cette variété. Les concepts dont les modes de détermination forment une variété discrète sont si fréquents que, étant donnés des objets quelconques, il se trouve toujours, du moins dans les langues cultivées, un concept qui les comprend (et les mathématiciens étaient par conséquent en droit, dans la théorie des grandeurs discrètes, de prendre pour point de départ la condition que les objets donnés soient considérés comme de même espèce). Au contraire, les occasions qui peuvent faire naître les concepts dont les modes de détermination forment une variété continue sont si rares dans la vie ordinaire, que les lieux des objets sensibles et les couleurs sont à peu près les seuls concepts simples dont les modes de détermination forment une variété de plusieurs dimensions. C'est seulement dans les hautes Mathématiques que les occasions pour la formation et le développement de ces concepts deviennent plus fréquentes.

Une partie d'une variété, séparée du reste par une marque ou par une limite, s'appelle un quantum. La comparaison des quanta au point de vue de la quantité, s'effectue, pour les grandeurs discrètes, au moyen du dénombrement; pour les grandeurs continues, au moyen de la mesure. La mesure consiste dans une

(¹) *Varietas, Mannigfaltigkeit. Voir* GAUSS, *Theoria res. biquadr.*, t. II, et *Anzeige zu derselben* (*Werke*, t. II, p. 110, 116 et 118). — (J. HOUEL.)

superposition de grandeurs à comparer; il faut donc, pour mesurer, avoir un moyen de transporter la grandeur qui sert d'étalon de mesure pour les autres. Si ce moyen manque, on ne pourra alors comparer entre elles deux grandeurs, que si l'une d'elles est une partie de l'autre, et encore, dans ce cas, ne pourra-t-on décider que la question du plus grand ou du plus petit, et non celle du rapport numérique. Les recherches auxquelles un tel cas peut donner lieu forment une branche générale de la théorie des grandeurs, indépendante des déterminations métriques, et dans laquelle elles ne sont pas considérées comme existant indépendamment de la position, ni comme exprimables au moyen d'une unité, mais comme des régions dans une variété. De telles recherches sont devenues nécessaires dans plusieurs parties des Mathématiques, notamment pour l'étude des fonctions analytiques à plusieurs valeurs, et c'est surtout à cause de leur imperfection que le célèbre théorème d'Abel, ainsi que les travaux de Lagrange, de Pfaff, de Jacobi sur la théorie générale des équations différentielles, sont restés si longtemps stériles. Dans cette branche générale de la théorie des grandeurs étendues, où l'on ne suppose rien de plus que ce qui est déjà renfermé dans le concept de ces grandeurs, il nous suffira, pour notre objet actuel, de porter notre étude sur deux points, relatifs : le premier, à la génération du concept d'une variété de plusieurs dimensions; le second, au moyen de ramener les déterminations de lieu dans une variété donnée à des déterminations de quantité, et c'est ce dernier point qui doit faire clairement ressortir le caractère essentiel d'une étude de n dimensions.

§ II.

Etant donné un concept dont les modes de détermination forment une variété continue, si l'on passe, suivant une manière déterminée, d'un mode de détermination à un autre, les modes de détermination parcourus formeront une variété étendue dans un seul sens, dont le caractère essentiel est que, dans cette variété, on ne peut, en partant d'un point, s'avancer d'une manière continue

Le grand succès des recherches de Kummer, dans le domaine de la division du cercle, donnait lieu de présumer que les mêmes lois subsistaient dans *tous* les domaines numériques $\mathfrak{o}$ de l'espèce la plus générale, dont il a été question plus haut. Dans mes recherches, qui avaient pour but d'amener la question à une solution définitive, j'ai commencé par m'appuyer sur la théorie des congruences d'ordre supérieur, parce que j'avais déjà précédemment remarqué que par l'application de cette théorie les recherches de Kummer pouvaient être considérablement abrégées; mais, bien que ce moyen conduisît jusqu'à un point très-voisin du but de mes efforts, je n'ai pu toutefois réussir par cette voie à soumettre certaines exceptions apparentes aux lois constatées pour les autres cas. Je ne suis parvenu à la théorie générale et sans exceptions, que j'ai publiée pour la première fois au lieu indiqué plus haut, qu'après avoir entièrement abandonné l'ancienne marche plus formelle, et l'avoir remplacée par une autre partant de la conception fondamentale la plus simple, et fixant le regard immédiatement sur le but. Dans cette marche, je n'ai plus besoin d'aucune création nouvelle, comme celle du *nombre idéal* de Kummer, et il suffit complétement de la considération de ce *système de nombres réellement existants,* que j'appelle un *idéal.* La puissance de ce concept reposant sur son extrême simplicité, et mon dessein étant avant tout d'inspirer la confiance en cette notion, je vais essayer de développer la suite des idées qui m'ont conduit à ce concept.

Kummer n'a pas défini les nombres idéaux eux-mêmes, mais seulement la divisibilité par ces nombres. Si un nombre α possède une certaine propriété A, consistant toujours en ce que α satisfait à une ou plusieurs congruences, il dit que α est divisible par un nombre idéal déterminé, correspondant à la propriété A. Bien que cette introduction de nouveaux nombres soit tout à fait légitime, il est toutefois à craindre d'abord que, par le mode d'expression que l'on a choisi, dans lequel on parle de nombres idéaux déterminés et de leurs produits, et aussi par l'analogie présumée avec la théorie des nombres rationnels, on ne soit entraîné à des conclusions précipitées et par là à des démonstrations insuffisantes, et en effet cet écueil n'est pas toujours complétement évité. D'autre part, une définition exacte et qui soit commune à *tous* les nombres idéaux qu'il s'agit d'introduire dans un domaine numérique déterminé $\mathfrak{o}$, et en même temps une définition générale de leur multiplication paraissent

d'autant plus nécessaires, que ces nombres idéaux n'existent nullement dans le domaine numérique considéré $\mathfrak{o}$. Pour satisfaire à ces exigences, il sera nécessaire et suffisant d'établir une fois pour toutes le caractère commun de toutes les propriétés A, B, C, ..., qui toujours, et elles seules, servent à l'introduction de nombres idéaux déterminés, et ensuite d'indiquer généralement comment de deux de ces propriétés A, B, auxquelles correspondent deux nombres idéaux déterminés, on pourra déduire la propriété C qui doit correspondre au produit de ces deux nombres idéaux ([1]).

([1]) La légitimité ou plutôt la nécessité de telles exigences, qui devraient toujours s'imposer dans l'introduction ou la création de nouveaux éléments arithmétiques, deviendra encore plus évidente par la comparaison avec l'introduction des nombres *réels irrationnels,* objet dont je me suis occupé dans un écrit spécial (*Stetigkeit und irrationale Zahlen;* Brunswick, 1872). En admettant que l'arithmétique des nombres *rationnels,* dont nous désignerons l'ensemble par R, soit définitivement fondée, il s'agit de savoir de quelle manière on devra introduire les nombres irrationnels, et définir les opérations d'addition, de soustraction, de multiplication et de division à exécuter sur ces nombres. Comme première exigence, je reconnais que l'Arithmétique doit être maintenue exempte de tout mélange d'élements étrangers, et pour cette raison je rejette la définition d'après laquelle le nombre serait le rapport de deux grandeurs de même espèce; au contraire, la définition ou la création du nombre irrationnel doit être fondée uniquement sur des phénomènes que l'on puisse déjà constater clairement *dans le domaine* R. En second lieu, on devra exiger que tous les nombres réels irrationnels puissent être engendrés à la fois par une commune définition, et non successivement comme racines des équations, comme logarithmes, etc. La définition devra, en troisième lieu, être de nature à permettre aussi une définition parfaitement claire des calculs (addition, etc.) que l'on aura à faire sur les nouveaux nombres. On parvient à tout cela de la manière suivante, que je ne ferai ici qu'indiquer :

1° J'appelle *section* du domaine R un partage quelconque de tous les nombres rationnels en deux catégories, tel que chaque nombre de la première catégorie soit algébriquement moindre que chaque nombre de la seconde catégorie.

2° Tout nombre rationnel déterminé *a engendre* une section déterminée (ou deux sections, non essentiellement differentes), par cela qu'un nombre rationnel quelconque sera classé dans la première ou dans la seconde catégorie, suivant qu'il sera algébriquement plus petit ou plus grand que a (tandis que a lui-même pourra être inscrit à volonté dans l'une ou dans l'autre des deux catégories).

3° Il y a une infinité de sections qui *ne peuvent pas* être engendrées par des nombres rationnels, de la manière indiquée : pour toute section de cette espèce, on crée et l'on introduit dans l'arithmétique un nombre *irrationnel* spécial, correspondant à cette section (ou l'engendrant).

4° Soient α, β deux nombres quelconques réels (rationnels ou irrationnels); il est facile, d'après les sections qu'ils engendrent, de définir si l'on a $\alpha > \beta$ ou $\alpha < \beta$; de plus, on peut aisément définir, au moyen de ces deux sections, les quatre sections auxquelles doivent correspondre la somme, la différence, le produit, le quotient des deux nombres α, β. Par là sont définies sans aucune obscurité les quatre opérations

Ce problème est essentiellement simplifié par les réflexions suivantes. Comme une telle propriété caractéristique A sert à définir, non un nombre idéal lui-même, mais seulement la divisibilité des nombres contenus dans $\mathfrak{o}$ par un nombre idéal, on est conduit naturellement à considérer l'ensemble $\mathfrak{a}$ de *tous* ces nombres α du domaine $\mathfrak{o}$ qui sont divisibles par un nombre idéal déterminé ; j'appellerai dès maintenant, pour abréger, un tel système $\mathfrak{a}$ un *idéal,* de sorte que, à tout nombre idéal déterminé, correspond un *idéal* déterminé $\mathfrak{a}$. Maintenant comme, réciproquement, la propriété A, c'est-à-dire la divisibilité d'un nombre α par le nombre idéal, consiste uniquement en ce que α appartient à l'idéal correspondant $\mathfrak{a}$, on pourra, au lieu des propriétés A, B, C, ..., par lesquelles a été définie l'introduction des nombres idéaux, considérer les idéaux correspondants $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ..., pour établir leur caractère commun et exclusif. En ayant égard actuellement à ce que l'introduction des nombres idéaux n'a pas d'autre but que de ramener les lois de la divisibilité dans le domaine numérique $\mathfrak{o}$ à une complète conformité avec la théorie des nombres rationnels, il est évidemment nécessaire que les nombres réellement existants dans $\mathfrak{o}$, et qui toutefois se présentent en première ligne comme facteurs de nombres composés, ne soient considérés que comme un cas particulier des nombres idéaux ; si donc μ est un nombre déterminé de $\mathfrak{o}$, le système $\mathfrak{a}$ de tous les nombres $\alpha = \mu\omega$ du domaine $\mathfrak{o}$ divisibles par μ aura également le caractère essentiel d'un idéal, et il sera appelé un *idéal principal ;* ce système évidemment n'est pas altéré, quand on remplace μ par $\varepsilon\mu$, ε désignant une unité quelconque renfermée dans $\mathfrak{o}$. Maintenant, de la notion de nombre entier établie plus haut résultent immédiatement les deux théorèmes élémentaires suivants sur la divisibilité :

1° Si les deux nombres entiers $\alpha = \mu\omega$, $\alpha' = \mu\omega'$ sont divisibles par le nombre entier μ, leur somme $\alpha + \alpha' = \mu(\omega + \omega')$ et leur différence

fondamentales de l'Arithmetique pour deux nombres réels quelconques, et l'on peut *démontrer* réellement des propositions telles, par exemple, que l'égalité $\sqrt{2}.\sqrt{3} = \sqrt{6}$, ce qui n'a pas encore été fait, que je sache, dans le sens rigoureux du mot.

5° Les nombres irrationnels ainsi définis forment, réunis aux nombres rationnels, un domaine $\mathfrak{R}$ sans lacunes et *continu ;* toute section de ce domaine $\mathfrak{R}$ sera produite par un nombre determiné du même domaine ; il est impossible de classer encore de nouveaux nombres dans ce domaine $\mathfrak{R}$.

$\alpha - \alpha' = \mu(\omega - \omega')$ seront aussi divisibles par μ, puisque la somme $\omega + \omega'$ et la différence $\omega - \omega'$ de deux nombres entiers ω, ω' sont elles-mêmes aussi des nombres entiers.

2° Si $\alpha = \mu\omega$ est divisible par μ, tout nombre $\alpha\omega' = \mu(\omega\omega')$, divisible par α, sera aussi divisible par μ, puisque tout produit $\omega\omega'$ de deux nombres entiers ω, ω' est aussi lui-même un nombre entier.

Si l'on applique ces théorèmes, vrais pour tous les nombres entiers, aux nombres ω de notre domaine numérique $\mathfrak{o}$, en désignant par μ un de ces nombres déterminés, et par $\mathfrak{a}$ l'idéal principal qui lui correspond, on obtiendra les deux propriétés fondamentales suivantes d'un tel système numérique $\mathfrak{a}$:

I. *Les sommes et les différences de deux nombres quelconques du système* $\mathfrak{a}$ *sont toujours des nombres du même système* $\mathfrak{a}$.

II. *Tout produit d'un nombre du système* $\mathfrak{a}$ *par un nombre du système* $\mathfrak{o}$ *est un nombre du système* $\mathfrak{a}$.

Maintenant, comme nous poursuivons le but de ramener généralement, par l'introduction des nombres idéaux et d'un mode de langage correspondant, les lois de la divisibilité dans le domaine numérique $\mathfrak{o}$ à une complète conformité avec celles qui règnent dans le domaine des nombres entiers rationnels, il s'ensuit que les définitions des nombres idéaux et de la divisibilité par ces nombres devront s'énoncer de telle manière que les deux théorèmes élémentaires ci-dessus, 1° et 2°, continuent à subsister lors même que μ ne serait pas un nombre existant, mais un nombre idéal, et par suite les deux propriétés I et II appartiendront non-seulement aux idéaux principaux, mais aussi à *tous* les idéaux. Nous avons donc trouvé par là un caractère *commun* à tous les idéaux ; à tout nombre existant ou idéal correspond un idéal complétement déterminé $\mathfrak{a}$, jouissant toujours des deux propriétés I et II.

Mais un fait de la plus haute importance, et dont je n'ai pu démontrer rigoureusement la vérité qu'à la suite de nombreux et vains efforts et après avoir surmonté de grandes difficultés, c'est que, réciproquement, tout système $\mathfrak{a}$ qui jouit des propriétés I et II est aussi un idéal, c'est-à-dire que $\mathfrak{a}$ forme l'ensemble de tous les nombres α du domaine $\mathfrak{o}$ qui sont divisibles par un nombre existant déterminé, ou par un nombre idéal, indispensable pour compléter la théorie. Les deux propriétés I et II sont donc non-seulement les conditions nécessaires, mais encore les conditions suffisantes pour qu'un système numérique $\mathfrak{a}$ soit un idéal ; toute autre condition à laquelle on voudrait assujettir les systèmes numériques $\mathfrak{a}$, si elle n'était pas une simple conséquence des propriétés I et II, rendrait impossible l'explication complète de tous les phénomènes de la divisibilité dans le domaine $\mathfrak{o}$.

Cette constatation m'a conduit naturellement à fonder toute la théorie des nombres du domaine $\mathfrak{o}$ sur cette définition simple, entièrement délivrée de toute obscurité et de l'admission des nombres idéaux (1) :

Tout système $\mathfrak{a}$ *de nombres entiers du corps* Ω, *qui possède les propriétés I et II, est dit* UN IDÉAL DE CE CORPS.

La divisibilité d'un nombre α par un nombre μ consiste en ce que α est un nombre $\mu\omega$ de l'idéal principal, qui correspond au nombre μ et peut être convenablement désigné par $\mathfrak{o}(\mu)$ ou $\mathfrak{o}\mu$; et de la propriété II ou du théorème 2°, il résulte qu'en même temps tous les nombres de l'idéal principal $\mathfrak{o}\alpha$ sont aussi des nombres de l'idéal principal $\mathfrak{o}\mu$. Réciproquement, il est évident que α est certainement divisible par μ, quand tous les nombres de l'idéal $\mathfrak{o}\alpha$, et par suite aussi α lui-même, sont contenus dans l'idéal $\mathfrak{o}\mu$. De là on est conduit à établir la notion suivante de la *divisibilité,* non-seulement pour les idéaux principaux, mais encore pour tous les idéaux :

Un idéal $\mathfrak{a}$ *est dit* divisible *par un idéal* $\mathfrak{b}$, *ou un multiple de* $\mathfrak{b}$, *et* $\mathfrak{b}$ *un diviseur de* $\mathfrak{a}$, *lorsque tous les nombres de l'idéal* $\mathfrak{a}$ *sont en même temps contenus dans* $\mathfrak{b}$. *Un idéal* $\mathfrak{p}$, *différent de* $\mathfrak{o}$, *qui n'a aucun diviseur autre que* $\mathfrak{o}$ *et* $\mathfrak{p}$, *est dit un* idéal premier (1).

De cette divisibilité des idéaux, *qui comprend évidemment celle des nombres,* il faut d'abord bien séparer la notion suivante de la *multiplication* et des *produits* de deux idéaux :

Si α *parcourt tous les nombres d'un idéal* $\mathfrak{a}$, *et* β *tous les nombres d'un idéal* $\mathfrak{b}$, *tous les produits de la forme* $\alpha\beta$ *et toutes les sommes de ces produits formeront un idéal qui s'appellera le produit des idéaux* $\mathfrak{a}$, $\mathfrak{b}$, *et que l'on désignera par* $\mathfrak{ab}$ (2).

Or on voit immédiatement, il est vrai, que le produit $\mathfrak{ab}$ est divi-

---

(1) Il est naturellement permis, quoique ce ne soit aucunement nécessaire, de faire correspondre à tout *idéal* tel que $\mathfrak{a}$ un *nombre idéal* qui l'engendre, si ce n'est pas un idéal principal.

(2) En même temps le nombre idéal correspondant à l'idéal $\mathfrak{ab}$ s'appellerait *divisible* par le nombre idéal correspondant à l'idéal $\mathfrak{b}$; à un idéal premier correspondrait un nombre ideal *premier.*

ERRATA.

Pages.	Lignes.	*Au lieu de :*	*lisez :*
279	16	εx	$\varepsilon\alpha$
282	26	classe principale correspond,	classe correspond
286	15	système $\mathfrak{a}$ est	système $\mathfrak{o}$ est
287	25	(1)	(2)
287	32	(2)	(3)
287	37	$\mathfrak{a}^{\mathfrak{b}}$	$\mathfrak{a}$

Au bas de la page 287, rétablir la Note oubliée :

(3) Le nombre idéal correspondant à l'idéal $\mathfrak{ab}$ s'appellerait le *produit* des deux nombres idéaux correspondant à $\mathfrak{a}$ et $\mathfrak{b}$.

SUR UNE NOTION QUI COMPREND CELLE DE LA DIVISIBILITÉ ET SUR LA THÉORIE GÉNÉRALE DE L'ÉLIMINATION

PAR

J. MOLK
À STRASBOURG.

Introduction.

Les voies nouvelles ouvertes à l'Algèbre par les travaux de GAUSS, d'ABEL et de GALOIS ont été le point de départ des recherches de M. KRONECKER sur la théorie générale de l'élimination. Ces recherches sont intimement liées à celles qui ont pour objet l'étude des systèmes de diviseurs d'un système de fonctions entières. Je me suis proposé, dans ce mémoire, d'exposer les unes et les autres, en me plaçant au point de vue arithmétique de M. KRONECKER.

Pour bien faire saisir l'esprit des méthodes employées il m'a semblé nécessaire de préciser tout d'abord l'idée d'irréductibilité dans un domaine de rationalité donné. J'ai ensuite développé les premiers éléments de la théorie des systèmes de diviseurs dont l'introduction en Algèbre est due à M. KRONECKER. Après avoir exposé quelques théorèmes sur l'élimination d'une variable entre deux équations, j'ai enfin abordé l'objet même de ce mémoire, la théorie générale de l'élimination.

Je désirerais surtout éclaircir quelques points du grand mémoire que M. KRONECKER a publié, en Septembre 1881, à l'occasion du cinquantième

anniversaire du doctorat de M. KUMMER.[1] Ce mémoire semble appelé à imprimer une direction nouvelle à l'Algèbre. Le but que je me suis proposé serait entièrement atteint si mon travail pouvait amener quelques géomètres à approfondir les idées aussi difficiles que nombreuses qui y sont contenues.

C'est à ce mémoire, à quelques autres publications de M. KRONECKER et plus particulièrement à son Cours professé à l'Université de Berlin que j'ai emprunté presque tous les matériaux de ce travail. Je me suis efforcé de les grouper et de les éclairer, de les ordonner aussi méthodiquement que le comportait la nature du sujet, et de les rendre ainsi accessibles à tous. A cet effet, je n'ai pas hésité à répéter, à plusieurs reprises, des choses bien connues de tous ceux qui s'occupent d'Algèbre. D'autre part, j'ai cherché à caractériser et à bien mettre en évidence les questions qui, pour moi du moins, restent à résoudre. M. KRONECKER a bien voulu s'intéresser à mon travail et je lui dois les plus précieux encouragements pendant tout le temps que j'y ai consacré.

CHAPITRE I.

Méthodes particulières à l'Algèbre.

1. L'Arithmétique et l'Algèbre prennent une place à part dans l'ensemble des sciences mathématiques. Leur objet propre est, en dernière analyse, l'étude des propriétés des nombres entiers positifs et des fonctions entières à coefficients entiers, positifs, d'une ou de plusieurs variables indépendantes.

Ces deux études ne diffèrent pas essentiellement l'une de l'autre. Une fonction entière, à coefficients entiers, positifs, d'un certain nombre de variables représente, en effet, d'une manière commode, un système de nombres entiers et ne représente pas autre chose. On obtient ce système

(1) L. KRONECKER: *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* Festschrift zu Herrn E. E. KUMMERS Doctor-Jubiläum. Berlin, Reimer 1882.

en remplaçant successivement, dans la fonction entière considérée, les variables par tous les systèmes de valeurs entières plus petites qu'un entier, laissé, à dessein, *indéterminé* dans les recherches générales, afin de pouvoir être choisi convenablement dans chaque recherche particulière. L'indétermination du nombre *fini* d'entiers du système que l'on considère, et la manière d'obtenir facilement ces entiers, sont toutes deux mises en évidence en représentant ce système par une fonction entière.

L'Arithmétique et l'Algèbre ont ainsi un domaine bien défini; les nombres entiers, positifs, les systèmes de nombres entiers représentés par des fonctions entières à coefficients entiers, positifs, y sont considérés comme *existant,* tout comme le mouvement en cinématique et la matière dans les sciences naturelles. Les nombres rationnels, négatifs, imaginaires, ainsi que les nombres irrationnels et transcendants ne font pas partie de ce domaine. Ils n'ont du nombre que le nom; en réalité ce sont de purs symboles.

En Analyse le point de vue est différent. On commence par généraliser l'idée même de quantité. Gauss l'a le premier fait d'une manière systématique mais sans séparer entièrement le domaine de la Géométrie de celui de l'Arithmétique. Plus tard M. Weierstrass a suivi une méthode essentiellement différente où l'on ne s'attache d'abord à aucun domaine déterminé mais où, au contraire, le but que l'on se propose, en généralisant l'idée de quantité, est de *déterminer* le domaine nécessaire et suffisant dans lequel on puisse effectuer toutes les opérations directes et inverses qui se présentent dans les calculs. Mais que l'on se place au point de vue de Gauss ou à celui de M. Weierstrass il importe de remarquer que le désir de pouvoir répondre *positivement* à une série de questions, qui sont en partie du domaine de la Géométrie, a seul amené les mathématiciens à introduire successivement de nouveaux symboles en Analyse. On comprend alors qu'en se plaçant au point de vue spécial de l'Arithmétique, en assignant à cette science un domaine déterminé, celui des nombres entiers, positifs, et en ne voulant pas introduire dans tous les raisonnements une idée étrangère à l'objet que l'on a en vue, il convienne de n'employer qu'une partie des symboles de l'Analyse, celle qui ne nous fait quitter qu'en apparence le domaine de l'Arithmétique.

Les symboles dits rationnels, positifs et négatifs remplissent cette condition. A tout moment une égalité contenant des nombres rationnels,

positifs ou négatifs, peut être transformée en une égalité entièrement équivalente et ne contenant que des nombres entiers et positifs. Un nombre *fini* d'opérations permet toujours de grouper les symboles rationnels suivant les besoins du calcul et de remplacer ces groupes par des nombres entiers positifs à l'aide des égalités qui définissent ces symboles, égalités qui peuvent toujours être sous-entendues et qui seules ont une existence réelle en Arithmétique.

La même chose a lieu pour les fonctions entières ou rationnelles, à coefficients entiers ou rationnels, positifs ou négatifs, d'un nombre quelconque de variables. Aussi les adjoindrons-nous également au domaine de l'Arithmétique.

Les fonctions entières d'une variable, égalées à zéro, définissent de nouveaux nombres, les nombres algébriques. Mais nous remarquons une grande différence entre l'introduction de ces nombres et celle des nombres rationnels, car nous ne pouvons pas à tout moment remplacer une égalité contenant des nombres algébriques par une égalité équivalente et ne contenant que des nombres entiers et positifs. En réalité, lorsqu'on définit positivement les nombres algébriques, on quitte vraiment, et non plus en apparence seulement pour la commodité des calculs, le domaine de l'Arithmétique pour entrer dans un domaine plus vaste. Il convient donc d'éviter l'emploi de ces nombres. Leur introduction, en Arithmétique, est d'ailleurs inutile en théorie; nous verrons plus loin par quoi il faut chercher à les remplacer.

Cependant lorsqu'on fait de nouvelles recherches, il est presque indispensable, dans l'état actuel de la science, de se servir de nombres algébriques; c'est, il est vrai, un simple artifice de langage, mais il fait image et nous permet de séparer facilement dans notre pensée les différentes racines conjuguées et d'abréger ainsi les démonstrations. La même chose a lieu en Géométrie par exemple, où il est souvent bien commode de ne pas s'astreindre tout d'abord à faire de la Géométrie de position, mais, au contraire, de supposer connus certains éléments qui sont du domaine de la Mécanique.

Sans doute il est nécessaire, pour être en droit de séparer ainsi les racines et de les représenter *séparément* par des symboles, de montrer comment, après avoir ramené le cas général à celui de la recherche des racines réelles d'une équation à coefficients réels, on peut, dans ce cas particulier, *déterminer un intervalle dans lequel l'équation donnée ne saurait être vérifiée par plus d'un nombre rationnel, avec une approximation donnée, suffisamment grande.* Il faut, en un mot, montrer ce que l'on doit entendre par racine d'une équation algébrique, au point de vue arithmétique auquel nous nous sommes placés.

Mais ces considérations m'écarteraient par trop de l'objet que j'ai principalement en vue. Elles rentrent dans un autre ordre d'idées et il convient de les exposer avec la théorie des *Caractéristiques.* (1) En supposant cette lacune comblée, il n'y a aucun inconvénient, dans des recherches nouvelles, à se servir de ces symboles algébriques, si l'on a soin d'y joindre l'égalité qui les définit. Il est cependant toujours *nécessaire,* lorsqu'on se propose d'approfondir les principes de l'Algèbre, de se passer, autant que possible, de cet instrument étranger au domaine de cette science.

Ce que je dis des nombres algébriques s'applique mot pour mot aux fonctions algébriques.

2. Mais la faiblesse de notre esprit ne nous permet pas plus d'aborder directement les questions fondamentales de l'Algèbre que celles de l'Arithmétique. Il nous est nécessaire de saisir à la fois tout l'ensemble d'une question, toutes les faces sous lesquelles elle se présente, pour pouvoir tirer des conclusions; et notre puissance d'abstraction est, en général, si faible que nous avons besoin d'auxiliaires. Ces auxiliaires nous sont donnés par la nature elle-même. Ce sont les quantités indéterminées. C'est à Gauss que revient la gloire de les avoir introduites en Arithmétique. Poisson et plusieurs autres mathématiciens éminents, ont certainement aperçu, en partie du moins, leur importance; mais c'est à M. Kronecker qu'il était réservé de faire voir clairement le rôle fondamental qu'elles sont appelées à jouer en Algèbre.

Je distingue entre *indéterminées* et *variables.*

Nous ne pouvons pas disposer des indéterminées dans le cours d'une démonstration. Ce sont ou bien de simples liens destinés à joindre une série d'opérations à effectuer ou de valeurs à trouver, et alors nous n'avons aucune prise sur elles, ou bien encore des abstractions que nous laissons à dessein indéterminées dans une même recherche afin d'embrasser un grand nombre de cas particuliers dans un seul calcul et alors, le calcul

(1) Comparez Kronecker, Monatsberichte der Berliner Akademie 1869.

terminé, nous pouvons leur donner une valeur quelconque. Dans ce dernier cas, je les nommerai plus particulièrement variables-indéterminées.

Les variables, au contraire, peuvent prendre des valeurs particulières dans le cours d'une démonstration. Elles nous sont, en effet, données par la nature même de nos recherches et nous nous proposons précisément de rechercher les valeurs particulières qu'il faut leur donner, ou encore les restrictions auxquelles elles doivent être soumises pour satisfaire aux conditions d'un problème déterminé.

Nous verrons, dans la suite, que l'emploi de variables *auxiliaires* est parfois fort utile. Il permet d'effectuer des transformations qui affranchissent les expressions considérées de certains cas particuliers dont l'étude spéciale ne serait d'aucun profit pour les résultats à obtenir.

On pourrait objecter à ce que j'ai dit des nombres et fonctions algébriques que ce sont tout aussi bien des auxiliaires légitimes que les quantités indéterminées. Cela n'est point douteux quant à la rigueur des démonstrations. Dans l'état actuel de la science, il peut même être souvent plus avantageux, pour obtenir ou énoncer rapidement des résultats nouveaux, d'employer comme auxiliaires les fonctions algébriques que de faire usage des quantités indéterminées. Mais lorsqu'il s'agit de voir clairement le rôle que joue chaque élément dans l'exposé des principes et des méthodes de l'Algèbre, il ne saurait y avoir de doute sur l'avantage de l'emploi des quantités indéterminées sur celui des nombres et fonctions algébriques.

En effet, l'existence même approximative de ces derniers est une idée très-complexe dans le domaine que nous nous sommes fixés. On peut presque dire qu'elle joue le même rôle en Algèbre que l'intégrale de Cauchy en Analyse. C'est parce qu'ils supposent et renferment plusieurs hypothèses essentielles que ces deux merveilleux instruments permettent d'obtenir rapidement un grand nombre de transformations, l'un d'expressions algébriques, l'autre d'expressions transcendantes. Avant d'avoir cherché à s'en passer, on ne se rend que très-difficilement compte de toute la simplification qu'ils introduisent l'un en Algèbre, l'autre en Analyse. Loin de les critiquer je crois, au contraire, qu'il convient, actuellement, de les placer, dans ces deux sciences, au début de toute recherche nouvelle. Mais je crois aussi que, précisément parce qu'ils renferment tous deux tant d'hypothèses essentielles, ils n'éclairent pas suffisamment les principes de la science, et c'est pourquoi, en me bornant à l'Algèbre, je disais plus haut que lorsqu'on se propose d'en approfondir les principes, il est préférable de chercher à se passer de leur aide.

Les indéterminées, au contraire, ne nous font point quitter le domaine des quantités rationnelles. Elle n'exigent point d'autres symboles que ceux que nous connaissons déjà, les symboles qui correspondent aux quatre opérations. Elles ont de plus un grand avantage, celui d'unir en quelque sorte l'Arithmétique à l'Algèbre, la théorie des nombres à celle des fonctions entières d'une et de plusieurs variables, comme nous le verrons dans la suite.

Je rappelle qu'une *forme* est une fonction entière dans laquelle les variables sont remplacées par des indéterminées.

L'*association* (1) des quantités indéterminées au domaine de l'Algèbre amène naturellement à joindre à l'étude des nombres entiers et des fonctions entières, celle des *formes* dont les coefficients sont soit des nombres entiers, soit des fonctions entières.

Il me reste à parler des nombres transcendants et imaginaires.

Les nombres transcendants, comme le rapport d'une circonférence à son diamètre, ne joueront pour nous que le rôle d'indéterminées. Si, en effet, nous démontrons un théorème en les supposant indéterminées et que nous remplacions ensuite ces indéterminées par les nombres transcendants donnés, rien ne saurait être changé dans notre domaine algébrique.

Les nombres imaginaires, de même que les nombres algébriques ne joueront aussi pour nous que le rôle d'indéterminées; mais, comme ils sont définis par des égalités ayant une existence réelle dans le domaine que nous considérons, il nous faudra tenir compte, dans nos calculs, de ces égalités, ce qui revient à remplacer les équations par des congruences.

Ainsi, par exemple, $\sqrt{2}$ n'est qu'un symbole; ce qu'il y a de réel, pour nous, c'est l'égalité $x^2 = 2$ qui définit $\sqrt{2}$. Si nous joignons au symbole l'égalité correspondante rien n'empêche d'en faire usage; chaque fois que dans le courant d'un calcul paraîtra $\sqrt{2}.\sqrt{2}$, l'égalité adjointe nous montre que nous devons remplacer ce produit par le nombre 2; en d'autres termes, que toute équation

$$F(\sqrt{2}) = 0$$

(1) Comparez KRONECKER: Festschrift, § 22.

où F désigne une fonction entière à coefficients rationnels, est équivalente à la congruence

$$F(u) \equiv 0 \pmod{x^2 - 2}$$

dans laquelle u désigne une indéterminée.

La même chose a lieu pour les nombres imaginaires que l'on emploie ordinairement en Analyse, le module de la congruence étant alors $(x^2 + 1)$. Dans des recherches spéciales d'Arithmétique il peut être convenable d'employer d'autres imaginaires que $\sqrt{-1}$; cela revient à remplacer le module $(x^2 + 1)$ par un autre module qui simplifie d'avantage la recherche particulière que l'on effectue.

3. Ce que j'ai dit du domaine particulier à l'Arithmétique et à l'Algèbre indique la marche à suivre dans tout exposé des résultats principaux obtenus dans ces deux sciences.

Les définitions devront être algébriques et non pas logiques seulement.

Il ne suffit pas de dire: »Une chose est ou elle n'est pas». Il faut montrer ce que veut dire être et ne pas être, dans le domaine particulier dans lequel nous nous mouvons. Alors seulement nous faisons un pas en avant. Si nous définissons, par exemple, une fonction irréductible comme une fonction qui n'est pas réductible, c'est à dire qui n'est pas décomposable en d'autres fonctions d'une nature déterminée, nous ne donnons point de définition algébrique, nous n'énonçons qu'une simple vérité logique. Pour qu'*en Algèbre,* nous soyons en droit de donner cette définition, il faut qu'elle soit précédée de l'exposé d'une méthode nous permettant d'obtenir à l'aide d'un nombre fini d'opérations rationnelles, les facteurs d'une fonction réductible. Seule cette méthode donne aux mots *réductible* et *irréductible* un sens algébrique.

Un raisonnement comme celui-ci: »Si des quantités données, en nombre infini, sont comprises entre des limites finies, il existe nécessairement une limite inférieure de ces quantités», est parfaitement logique. Il n'est point algébrique. Ce qu'il faut c'est donner une méthode pour déterminer, à l'aide d'un nombre fini d'opérations rationnelles, cette limite inférieure. Alors seulement nous faisons de l'Algèbre.

Il convient enfin d'éviter particulièrement toute incursion dans le domaine de la Géométrie. L'idée de continuité géométrique doit nous être d'autant plus étrangère que nous grouperons les nombres, non d'après leur grandeur, mais d'après leurs propriétés algébriques. Pour éviter tout malentendu, je m'efforcerai d'introduire une terminologie aussi peu géométrique que possible, comme l'a d'ailleurs fait M. KRONECKER dans sa Festschrift, en suivant ainsi l'exemple de GAUSS qui empruntait généralement sa nomenclature aux sciences biologiques.

4. En résumé: Quelle que soit la science naturelle dont on se propose d'aborder l'étude, on a soin de définir les éléments dont le groupement suivant des propriétés déterminées constitue en quelque sorte cette science. Les uns ont une existence réelle, ce sont eux que l'on a tout particulièrement en vue. Les autres sont des éléments auxiliaires; leur réduction à un nombre aussi petit que possible constitue un grand progrès; car elle permet d'apercevoir sans intermédiaires et, par suite, plus clairement les liens cachés qui semblent unir les différents phénomènes.

Autre chose est d'élargir les horizons d'une science ou d'en approfondir les principes. Dans les premiers cas toutes les méthodes peuvent être utiles et ce serait méconnaître l'unité de notre esprit que de le contester. Dans le second cas, au contraire, il faut chercher à se maintenir rigoureusement dans le domaine particulier à la science que l'on a en vue. Car ce n'est pas approfondir les principes d'une science dont le domaine est bien défini que d'en développer les éléments à l'aide de principes étrangers à ce domaine.

La méthode que je viens d'indiquer n'aurait-elle d'ailleurs que l'avantage de faire voir clairement où et comment les principes étrangers à notre domaine simplifient les recherches, qu'il conviendrait encore de l'employer dans la mesure du possible.

L'Algèbre est la première des sciences naturelles. Je viens de définir son domaine, les éléments qui le composent, les éléments auxiliaires dont l'introduction n'offre aucune espèce de difficulté, et ces autres éléments auxiliaires dont malgré tous nos efforts nous ne pouvons encore nous passer entièrement dans nos recherches.

CHAPITRE II.

Diviseurs des fonctions entières.

§ 1.

Divisibilité des fonctions entières dans un domaine naturel de rationalité. (¹)

1. Une propriété fondamentale des nombres entiers est leur *divisibilité.* Comme un nombre contenu dans un nombre n doit être nécessairement plus petit que n, il suffit, pour trouver les diviseurs de n, de voir si les nombres $2, 3, \ldots, (n-1)$, sont contenus dans n. Un nombre fini d'opérations nous permet donc de montrer qu'un entier positif n est ou bien un produit de nombres premiers et de *trouver* alors ces nombres premiers, ou bien que n est lui-même nombre premier, c'est à dire sans autres diviseurs que lui-même et l'unité. Dans le premier cas on dit que n est un nombre composé, et l'on montre à l'aide de l'algorithme du plus grand commun diviseur que sa décomposition en facteurs premiers est univoque.

Il en est de même des fonctions entières à coefficients entiers.

Considérons d'abord *une* fonction d'une variable. Ses coefficients peuvent avoir un diviseur commun que nous savons trouver par un nombre fini d'opérations, comme je viens de le rappeler. Nous pouvons ainsi mettre toute fonction entière à coefficients entiers sous la forme d'un produit dont l'un des facteurs est un nombre entier et l'autre une fonction entière dont les coefficients sont des entiers sans diviseur commun. Dans des recherches sur la divisibilité des fonctions entières il est donc permis de supposer les coefficients de chacune de ces fonctions, sans diviseur commun.

Considérons ensuite *deux* fonctions d'une variable, $F(x)$ et $G(x)$. Lorsque le quotient de $F(x)$ par $G(x)$ est une fonction entière à coefficients entiers, $H(x)$, nous dirons que $F(x)$ contient $G(x)$, est divisible par $G(x)$

(¹) Comparez KRONECKER, Journal de CRELLE T. 94 et Festschrift § 4.

et que $G(x)$ est contenue dans $F(x)$, est un diviseur de $F(x)$. Nous écrirons, soit $F(x) = H(x)G(x)$, soit $F(x) \equiv 0 \pmod{G(x)}$, suivant qu'il convient de mettre en évidence la fonction $H(x)$, ou non.

Je vais montrer comment l'on peut, ou bien trouver tous les diviseurs d'une fonction donnée $F(x)$, ou bien montrer que cette fonction $F(x)$ n'a pas de diviseur. Si le degré de $F(x)$ est $2n$ ou $(2n+1)$ il suffit évidemment de donner une méthode permettant de trouver, à l'aide d'un nombre fini d'opérations, ses diviseurs de degré au plus égal à n. Mais d'après la formule d'interpolation de LAGRANGE toute fonction entière $\Phi(x)$ de degré au plus égal à n, peut être mise sous la forme

$$\Phi(x) = \sum_{k=0}^{n} \Phi(r_k) \frac{\mathfrak{F}(x)}{x - r_k} \frac{1}{\mathfrak{F}'(r_k)}$$

où $r_0, r_1, \ldots, r_n$ désignent $(n+1)$ nombres arbitrairement choisis et $\mathfrak{F}(x)$ le produit

$$\prod_{k=0}^{n} (x - r_k).$$

En posant

$$g_k(x) = \frac{\mathfrak{F}(x)}{x - r_k} \frac{1}{\mathfrak{F}'(r_k)}$$

et

$$\Phi(r_k) = c_k$$

nous ordonnons $\Phi(x)$ suivant les fonctions $g_k(x)$, de degré n. Nous avons ainsi

$$\Phi(x) = \sum_{k=0}^{n} c_k g_k(x)$$

où $g_k(r_h) = 0$ pour $h \gtrless k$; et $g_k(r_k) = 1$.

Pour que $\Phi(x)$ soit contenue dans $F(x)$, il faut que $\Phi(r_h) = c_h$ soit contenue dans $F(r_h)$, pour $h = 0, 1, 2, \ldots, n$. Cherchons donc tous les diviseurs positifs et négatifs du nombre $F(r_h)$; ils seront en nombre fini; désignons-les par $c_h, c'_h, c''_h, \ldots, c_h^{(m_h)}$. Répétons cette opération pour $h = 0, 1, 2, \ldots, n$; nous aurons certainement un nombre fini

de combinaisons $\sum\limits_{k=0}^{n} c_k g_k(x)$. Chacune de ces combinaisons *peut* être un diviseur de $F(x)$ et il ne saurait y avoir d'autre diviseur de $F(x)$. Un nombre fini de divisions de deux polynômes nous permet donc de voir si $F(x)$ contient un facteur à coefficients entiers ou s'il n'en contient pas.

Nous pouvons maintenant, les nombres entiers étant considérés comme des fonctions entières de degré zéro, partager en deux classes les fonctions entières à coefficients entiers: Celles qui en contiennent d'autres; nous les nommerons *réductibles*. Et celles qui n'en contiennent pas d'autres; nous les nommerons *irréductibles*.

Dans la pratique les calculs se simplifient; mais ici l'important était de montrer que la réductibilité et l'irréductibilité des fonctions ont un sens algébrique, et que nous avons, par suite, le droit d'introduire ces notions dans la science qui fait l'objet de nos recherches.

Si $F_1(x)$ est contenue dans $F(x)$ nous répéterons sur $F_1(x)$ les mêmes raisonnements que nous venons de faire sur $F(x)$, et comme le degré de chaque diviseur est plus petit que celui de la fonction dans laquelle il est contenu, un nombre fini d'opérations nous permettra de décomposer $F(x)$ en un produit de puissances de fonctions entières *irréductibles*.

2. *Cette décomposition est univoque.* En effet, si le produit $\Phi(x) . \Psi(x)$ de deux fonctions entières à coefficients entiers, est divisible par une fonction irréductible $F(x)$, l'une des deux fonctions $\Phi(x)$, $\Psi(x)$, est elle-même divisible par $F(x)$. Lorsque $F(x)$ se réduit à un nombre premier, la démonstration se déduit immédiatement du théorème qu'un produit de deux nombres ne peut être divisible par un nombre premier p que si l'un des deux nombres est divisible par p, et ce théorème est un corollaire de *l'algorithme* d'EUCLIDE. Lorsque le degré de $F(x)$ est plus grand que zéro, si $\Phi(x)$ n'est pas divisible par $F(x)$, comme $F(x)$ est irréductible, $\Phi(x)$ et $F(x)$ n'ont point de diviseur commun. Mais alors, à l'aide de *l'algorithme* d'EUCLIDE étendu aux fonctions d'une variable, nous pouvons toujours trouver deux fonctions entières $\varphi(x)$ et $f(x)$ vérifiant l'égalité

$$\varphi(x)\Phi(x) + f(x)F(x) = 1$$

ou

$$\varphi(x)\Phi(x)\Psi(x) + f(x)F(x)\Psi(x) = \Psi(x).$$

Comme, par hypothèse, le produit $\Phi(x)\Psi(x)$ est divisible par $F(x)$, cette égalité nous montre que $F(x)$ est contenu dans $\Psi(x)$, en ce sens, du moins, que

$$m \, . \, \Psi(x) = F(x) \, . \, G(x)$$

$G(x)$ étant une fonction entière à coefficients entiers, et m un nombre entier.

Gauss a le premier démontré[1] que si une fonction entière à coefficients entiers est le produit de deux fonctions entières à coefficients rationnels, elle est aussi le produit de deux fonctions entières à coefficients entiers. La démonstration est élémentaire et se déduit du théorème cité, que si le produit de deux fonctions entières à coefficients entiers est divisible par un nombre premier p, l'une de ces deux fonctions est elle-même divisible par p.

Comme les coefficients de $\Psi(x)$ sont entiers, et que $F(x)$ est irréductible, nous voyons donc ici que m divise tous les coefficients de $G(x)$.

Supposons maintenant que, par le procédé indiqué plus haut, nous obtenions deux décompositions d'une même fonction entière à coefficients entiers, et, par suite, l'égalité

$$\prod_{(h)} p_h^{i_h} \cdot \prod_{(k)} P_k^{\mu_k}(x) = \prod_{(r)} q_r^{s_r} \cdot \prod_{(\rho)} Q_\rho^{\sigma_\rho}(x) \qquad \begin{pmatrix} h = 1, 2, \ldots, a \\ k = 1, 2, \ldots, \alpha \\ r = 1, 2, \ldots, b \\ \rho = 1, 2, \ldots, \beta \end{pmatrix}$$

dans laquelle p, q, i, s, μ, σ sont des nombres, p et q, en particulier, des nombres irréductibles, et $P(x)$, $Q(x)$ des fonctions irréductibles.

Le nombre p_1, par exemple, est alors manifestement contenu dans le terme de droite de cette égalité; chacune des fonctions $Q(x)$ étant irréductible, il faut que p_1 soit contenu dans le produit

$$\prod_{(r)} q_r^{s_r} \qquad (r = 1, 2, \ldots, b)$$

donc qu'il soit égal à l'un des nombres $q_1, q_2, \ldots, q_b$. En divisant par ce nombre les deux termes de l'égalité, et en répétant le même raisonnement pour chacun des entiers p et pour chacun des entiers q, aussi longtemps qu'il en reste, nous voyons que l'égalité précédente se réduit à

$$\prod_{(k)} P_k^{\mu_k}(x) = \prod_{(\rho)} Q_\rho^{\sigma_\rho}(x). \qquad \begin{pmatrix} k = 1, 2, \ldots, \alpha \\ \rho = 1, 2, \ldots, \beta \end{pmatrix}$$

---

[1] *Disquisitiones arithmeticæ*, p. 42.

Mais alors, à cause du théorème précédent, la fonction *irréductible* $P_1(x)$ est égale à l'une des fonctions *irréductibles* $Q(x)$. Divisant, de part et d'autre, par cette fonction, et répétant le même raisonnement sur chacune des fonctions $P(x)$ et $Q(x)$ autant de fois que cela est nécessaire, nous voyons que les deux décompositions de la fonction donnée en facteurs irréductibles, sont identiques.

3. Considérons maintenant une fonction de plusieurs variables indépendantes

$$F(x', x'', \ldots, x^{(n)}).$$

En posant

$$x' = x^{g^0}, \quad x'' = x^{g^1}, \quad x''' = x^{g^2}, \quad \ldots, \quad x^{(n)} = x^{g^{n-1}}$$

et en choisissant g assez grand pour que tous les termes du polynôme

$$F(x', x'', \ldots, x^{(n)})$$

soient de degré différent en x, nous transformerons ce polynôme en une fonction d'une seule variable, $\Phi(x)$, dont tous les termes sont linéairement indépendants. Il est commode de considérer tous les exposants de x comme des nombres écrits dans le système dont la base est g. On voit alors immédiatement qu'il est impossible que $F(x', x'', \ldots, x^{(n)})$ ait un facteur quelconque lorsque $\Phi(x)$ n'en a pas; car à toute égalité

$$F(x', x'', \ldots, x^{(n)}) = F_1(x', x'', \ldots, x^{(n)}) F_2(x', x'', \ldots, x^{(n)})$$

en correspond une autre

$$\Phi(x) = \Phi_1(x) \Phi_2(x)$$

Φ_1 et Φ_2 désignant les transformées respectives de F_1 et F_2, par les substitutions indiquées. Pour reconnaître si $F(x', x'', \ldots, x^{(n)})$ a des diviseurs ou non, il suffit donc de rechercher tous les diviseurs possibles de $\Phi(x)$, ce que nous savons faire à l'aide d'un nombre fini d'opérations, puis de voir si les fonctions de plusieurs variables qui correspondent à ces diviseurs sont vraiment facteurs de $F(x', x'', \ldots, x^{(n)})$ ou non, ce qui n'exige qu'un nombre fini de divisions.

Il est donc légitime d'étendre l'idée d'irréductibilité aux fonctions de plusieurs variables indépendantes. Nous allons en donner une seconde