BULLETIN DES SCIENCES
MATHÉMATIQUES ET ASTRONOMIQUES

R. DEDEKIND

Sur la théorie des nombres entiers algébriques

Bulletin des sciences mathématiques et astronomiques, tome 11 (1876), p. 278-288

<http://www.numdam.org/item?id=BSMA_1876__11__278_0>

MÉLANGES.

SUR LA THÉORIE DES NOMBRES ENTIERS ALGÉBRIQUES;

PAR M. R. DEDEKIND.

INTRODUCTION.

En réponse à l'invitation que l'on m'a fait l'honneur de m'adresser, je me propose, dans le présent Mémoire, de développer les *principes fondamentaux* de la théorie générale, échappant à toute exception des nombres entiers algébriques, principes que j'ai publiés dans la seconde édition des *Leçons sur la Théorie des nombres* de Dirichlet. Mais, à cause de l'étendue extraordinaire de ce champ de recherches mathématiques, je me bornerai ici à poursuivre un but unique, que je vais essayer de définir clairement par les remarques suivantes.

La théorie de la divisibilité des nombres, qui sert de fondement à l'arithmologie, a déjà été établie par Euclide dans ce qu'elle a d'essentiel; du moins, le théorème capital que tout nombre entier composé peut toujours se mettre, et cela d'une seule manière, sous la forme d'un produit de nombres tous premiers, est une conséquence immédiate de ce théorème démontré par Euclide (1), qu'un produit de deux nombres ne peut être divisible par un nombre premier que si celui-ci divise au moins l'un des facteurs.

Deux mille ans plus tard, Gauss donna, pour la première fois, une extension à la notion du nombre entier; tandis que, jusqu'à lui, on ne désignait sous ce nom que les nombres $0, \pm 1, \pm 2, \ldots$, que j'appellerai dans tout ce qui va suivre nombres *entiers rationnels*, Gauss introduisit (2) les nombres *entiers complexes*, de la forme $a + b\sqrt{-1}$, a et b désignant des nombres entiers rationnels quelconques, et il démontra que les lois générales de la divisibilité de ces nombres sont identiques avec celles qui régissent le domaine des nombres entiers rationnels.

La plus haute généralisation de la notion du nombre entier con-

(1) *Éléments*, VII, 32

(2) *Theoria residuorum biquadraticorum*, II; 1832.

siste dans ce qui suit. Un nombre θ est dit un nombre *algébrique*, lorsqu'il satisfait à une équation

$$\theta^n + a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_{n-1}\theta + a_n = 0,$$

de degré fini n et à coefficients rationnels $a_1, a_2, \ldots, a_{n-1}, a_n$; il est dit un nombre *entier algébrique*, ou plus brièvement un nombre *entier*, lorsqu'il satisfait à une équation de la forme ci-dessus, dans laquelle les coefficients $a_1, a_2, \ldots, a_{n-1}, a_n$ sont tous des nombres entiers rationnels. De cette définition il résulte immédiatement que les sommes, les différences et les produits de nombres entiers sont tous aussi des nombres entiers; par suite, un nombre entier α sera dit *divisible* par un nombre entier β, si l'on a $\alpha = \beta\gamma$, γ étant également un nombre entier. Un nombre entier ε s'appellera une *unité*, lorsque tout nombre entier quelconque sera divisible par ε. Par analogie, on devrait entendre par nombre *premier* un nombre entier α qui ne serait pas une unité, et qui n'aurait pour diviseurs que les unités ε et les produits de la forme εx; mais il est facile de reconnaître que, dans le domaine de tous les nombres entiers que nous considérons ici, il n'existe pas de tels nombres premiers, puisque tout nombre entier qui n'est pas une unité peut toujours être mis sous la forme d'un produit de deux facteurs ou plutôt d'un nombre quelconque de facteurs, qui sont tous des nombres entiers, mais non des unités.

Toutefois, l'existence des nombres premiers et l'analogie avec les domaines des nombres entiers rationnels ou complexes commence à se montrer de nouveau, lorsque du domaine de tous les nombres entiers on sépare une partie infiniment petite, de la manière suivante. Si θ est un nombre algébrique déterminé, parmi les équations à coefficients rationnels, en nombre infini dont θ est racine, il y en a une et une seule,

$$\theta^n + a_1\theta^{n-1} + \ldots + a_{n-1}\theta + a_n = 0,$$

qui est de degré moins élevé que toutes les autres, et que l'on nomme à cause de cela *irréductible*. Si $x_0, x_1, x_2, \ldots, x_{n-1}$ désignent des nombres rationnels pris à volonté, tous les nombres de la forme

$$\varphi(\theta) = x_0 + x_1\theta + x_2\theta^2 + \ldots + x_{n-1}\theta^{n-1},$$

dont nous représenterons le complexe par Ω, seront aussi des nombres algébriques, et ils jouiront de la propriété fondamentale

que leurs sommes, leurs différences, leurs produits et leurs quotients appartiendront tous aussi au même complexe Ω; j'appellerai un tel complexe Ω *un corps fini du degré n*. Tous les nombres $\varphi(\theta)$ appartenant au corps Ω se partagent maintenant, conformément à la définition ci-dessus, en deux grandes classes, savoir, en nombres entiers dont nous désignerons le complexe par $\mathfrak{o}$, et en nombres non entiers ou nombres fractionnaires. *Le problème que nous nous proposons consiste à établir les lois générales de la divisibilité qui régissent un tel système* $\mathfrak{o}$.

Le système $\mathfrak{o}$ est évidemment identique avec le système de tous les nombres entiers rationnels, lorsqu'on a $n = 1$, ou avec celui des nombres entiers complexes, lorsqu'on a $n = 2$ et $\theta = \sqrt{-1}$. Certains phénomènes qui se présentent dans ces deux domaines $\mathfrak{o}$ spéciaux se reproduisent encore dans tout domaine $\mathfrak{o}$ de cette nature; il faut observer avant tout que la décomposition illimitée dont il a été question plus haut, et qui règne dans le domaine qui comprend tous les nombres algébriques entiers, ne se rencontre jamais dans un domaine $\mathfrak{o}$ de l'espèce indiquée, comme on peut aisément s'en assurer par la considération des normes. Si l'on entend, en effet, par *norme* d'un nombre quelconque $\mu = \varphi(\theta)$, appartenant au corps Ω, le produit

$$\mathrm{N}(\mu) = \mu\mu_1\mu_2 \ldots \mu_{n-1},$$

dont les facteurs sont les nombres conjugués

$$\mu = \varphi(\theta), \quad \mu_1 = \varphi(\theta_1), \quad \mu_2 = \varphi(\theta_2), \quad \ldots, \quad \mu_{n-1} = \varphi(\theta_{n-1}),$$

$\theta, \theta_1, \theta_2, \ldots, \theta_{n-1}$ désignant toutes les racines de la même équation irréductible du $n^{\text{ième}}$ degré, $\mathrm{N}(\mu)$ sera toujours, comme on sait, un nombre rationnel, et ne deviendra $= 0$ que si $\mu = 0$; en même temps, on a toujours

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta),$$

α et β étant deux nombres quelconques du corps Ω. Si maintenant μ est un nombre entier et par suite un nombre compris dans $\mathfrak{o}$, les autres nombres conjugués $\mu_1, \mu_2, \ldots, \mu_{n-1}$ seront pareillement des nombres entiers, et par suite $\mathrm{N}(\mu)$ sera un nombre entier rationnel. Cette norme joue un rôle extrêmement important dans la théorie des nombres du domaine $\mathfrak{o}$; en effet, si deux nombres quelconques α, β de ce domaine sont dits *congrus* ou *incongrus* par rapport

à un troisième μ, pris pour *module,* selon que leur différence $\pm(\alpha-\beta)$ est ou n'est pas divisible par μ, on pourra, exactement comme dans la théorie des nombres entiers rationnels ou complexes, partager tous les nombres du système $\mathfrak{o}$ en *classes de nombres,* de sorte que chaque classe comprenne l'ensemble de tous les nombres qui sont congrus à un nombre déterminé, lequel sera le représentant de cette classe, et une étude plus approfondie nous apprend que le nombre de ces classes (à l'exception du seul cas de $\mu = 0$) est toujours fini, et de plus égal à la valeur absolue de $N(\mu)$. Une conséquence immédiate de ce résultat, c'est que $N(\mu)$ sera toujours $= \pm 1$ dans le cas, et seulement dans ce cas, où μ sera une unité. Si maintenant un nombre du système $\mathfrak{o}$ est dit *décomposable,* lorsqu'il est le produit de deux nombres de ce système, dont aucun ne soit une unité, il suit évidemment de ce qui précède que tout nombre décomposable peut toujours être représenté comme le produit d'un nombre fini de facteurs *indécomposables*.

Ce résultat correspond encore complétement à la loi qui a lieu dans la théorie des nombres entiers rationnels ou complexes, savoir que tout nombre composé peut être représenté par le produit d'un nombre fini de facteurs premiers; mais en même temps c'est ici le point où l'analogie, observée jusqu'ici, avec l'ancienne théorie menace de se rompre pour toujours. Dans ses recherches sur le domaine des nombres qui appartiennent à la théorie de la division du cercle, et qui correspondent par suite aux équations de la forme $\theta^m = 1$, Kummer a remarqué l'existence d'un phénomène par lequel les nombres de ce domaine se distinguent en général de ceux qu'on a considérés auparavant, d'une manière si complète et si essentielle, qu'il restait à peine un espoir quelconque de conserver les lois simples qui régissent l'ancienne théorie des nombres. En effet, tandis que, dans le domaine des nombres entiers, tant rationnels que complexes, tout nombre composé ne peut se mettre *que d'une seule manière* sous la forme d'un produit de nombres premiers, on reconnaît que, dans les domaines numériques considérés par Kummer, un nombre décomposable peut souvent se représenter *de plusieurs manières, entièrement différentes entre elles,* sous la forme d'un produit de nombres indécomposables, ou, ce qui dans le fond revient au même, on reconnaît que les nombres *indécomposables* ne possèdent pas tous le caractère d'un nombre *premier* proprement dit, lequel consiste en ce qu'un nombre premier ne peut

diviser un produit de deux ou de plusieurs facteurs, s'il ne divise au moins un de ces facteurs. Mais plus le succès des recherches ultérieures sur de tels domaines numériques devait sembler désespéré (1), plus on doit de reconnaissance aux efforts persévérants de Kummer, qui ont été enfin récompensés par une découverte vraiment grande et féconde. Ce géomètre est parvenu (2) à ramener toutes les irrégularités apparentes à des lois rigoureuses, et en considérant les nombres indécomposables, mais dépourvus du caractère de véritables nombres premiers, comme des produits de facteurs premiers *idéaux,* qui n'apparaissent et ne manifestent leur effet que combinés ensemble, et non pas isolés, il a obtenu ce résultat surprenant, que les lois de la divisibilité dans les domaines de nombres étudiés par lui coïncident maintenant complétement avec celles qui régissent le domaine des nombres entiers rationnels. Tout nombre qui n'est pas une unité se comporte, dans toutes les questions de divisibilité, tant dans un rôle actif que dans un rôle passif, ou comme un nombre premier, ou comme un nombre formé par la multiplication de facteurs premiers, existants ou idéaux, complétement déterminés. Deux nombres idéaux, soit premiers, soit composés, qui se changent en deux nombres existants par la combinaison avec un seul et même nombre idéal, sont dits *équivalents,* et tous les nombres idéaux équivalents à un même nombre idéal déterminé forment une *classe de nombres idéaux;* l'ensemble de tous les nombres existants, qui sont considérés comme un cas spécial des nombres idéaux, forme la *classe principale;* à chaque classe principale correspond un système d'une infinité de *formes* homogènes équivalentes, à n variables et du degré n, qui sont décomposables en n facteurs linéaires à coefficients algébriques; le nombre de ces classes est fini, et Kummer est parvenu à étendre à la détermination de ce nombre les principes par lesquels Dirichlet a déterminé le nombre des classes des formes quadratiques binaires.

---

(1) Dans le Mémoire : *De numeris complexis qui radicibus unitatis et numeris integri realibus constant* (*Vrastislaviæ*, 1844, § 8), Kummer dit: « Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in factores primos dissolvi possint qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset. »

(2) *Zur Theorie der complexen Zahlen* (*Journal de Crelle*, t. 35).

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 conduisit 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 fondee, 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 definition, 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 où 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* $\mathfrak{a}$ *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.*

sible aussi bien par $\mathfrak{a}$ que par $\mathfrak{b}$; mais l'établissement complet de la liaison entre les deux notions de la divisibilité et de la multiplication des idéaux réussit seulement après que l'on a vaincu des difficultés caractéristiques, profondément attachées à la nature du sujet; cette liaison s'exprime essentiellement par les deux théorèmes suivants :

Si l'idéal $\mathfrak{c}$ *est divisible par l'idéal* $\mathfrak{a}$, *il existera toujours un idéal* $\mathfrak{b}$, *et un seul, tel que le produit* $\mathfrak{ab}$ *soit identique avec* $\mathfrak{c}$.

Tout idéal différent de $\mathfrak{o}$ *ou est un idéal premier, ou peut être représenté, et cela d'une seule manière, sous forme d'un produit d'idéaux tous premiers.*

Dans le présent Mémoire, je me borne à démontrer ces résultats avec une entière rigueur et par voie synthétique. En cela consiste le *fondement* propre de la théorie complète des idéaux et des formes décomposables, laquelle offre aux mathématiciens un champ inépuisable de recherches. De tous les développements ultérieurs, pour lesquels je dois renvoyer à l'exposition faite dans les *Vorlesungen über Zahlentheorie* de Dirichlet et à quelques Mémoires qui paraîtront plus tard, je n'ai inséré dans le Mémoire actuel que le partage des idéaux en *classes*, et la démonstration que le nombre de ces *classes d'idéaux* (ou des classes de formes correspondantes) est fini. La première Section contient seulement les propositions indispensables pour le but présent, extraites d'une théorie auxiliaire, importante aussi pour d'autres recherches, et dont je publierai ailleurs l'exposition complète. La seconde Section, qui a pour but d'éclaircir sur des exemples numériques complétement déterminés les notions générales qui devront être introduites plus tard, pourrait être entièrement supprimée; mais je l'ai conservée parce qu'elle peut être utile pour faciliter l'intelligence des Sections suivantes, où l'on trouvera la théorie des nombres entiers d'un corps fini quelconque développée jusqu'au point indiqué ci-dessus. Pour cela, il suffit d'emprunter seulement les premiers éléments à la théorie générale des corps, théorie dont le développement ultérieur conduirait aisément aux principes algébriques inventés par Galois, lesquels servent à leur tour de base aux recherches plus approfondies dans la théorie des idéaux.

(*A suivre.*)