XLVIII.

Sur la Théorie des Nombres entiers algébriques.

[Paris, Gauthier-Villars, 1877, S. 1—121. Bulletin des Sciences mathématiques et astronomiques, 1re série, t. XI, 2e série, t. I, 1876, 1877.]

Table des Matières.

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

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

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 immé-

*) Éléments, VII, 32.

**) Theoria residuorum biquadraticorum, II; 1832.

diatement 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 $\varepsilon\alpha$; 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,

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

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

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

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 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 o.

Le système 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 o spéciaux se reproduisent encore dans tout domaine 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 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

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

dont les facteurs sont les nombres conjugués

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

θ, θ_1, θ_2, ..., θ_{n-1} désignant toutes les racines de la même équation irréductible du $n^{\text{ième}}$ degré, $N(\mu)$ sera toujours, comme on sait, un nombre rationnel, et ne deviendra $= 0$ que si $\mu = 0$; en même temps, on a toujours

$$N(\alpha\,\beta) = N(\alpha)\,N(\beta),$$

α et β étant deux nombres quelconques du corps Ω. Si maintenant μ est un nombre entier et par suite un nombre compris dans o, les autres nombres conjugués μ_1, μ_2, ..., μ_{n-1} seront pareillement des nombres entiers, et par suite $N(\mu)$ sera un nombre entier rationnel. Cette norme joue un rôle extrêmement important dans la théorie des nombres du domaine 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 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 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*), plus

*) 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.»

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*) 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 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.

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 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

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

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 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 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*).

*) 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'éléments 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 différentes), 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 fondamentales de l'Arithmétique 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 déterminé du même domaine; il est impossible de classer encore de nouveaux nombres dans ce domaine $\mathfrak{R}$.

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 o par un nombre idéal, on est conduit naturellement à considérer l'ensemble a de tous ces nombres α du domaine o qui sont divisibles par un nombre idéal déterminé; j'appellerai dès maintenant, pour abréger, un tel système a un idéal, de sorte que, à tout nombre idéal déterminé, correspond un idéal déterminé 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 a, on pourra, au lieu des propriétés A, B, C, ..., par lesquelles a été définie l'introduction des nombres idéaux, considérer les idéaux correspondants a, b, 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 o à une complète conformité avec la théorie des nombres rationnels, il est évidemment nécessaire que les nombres réellement existants dans 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 o, le système a de tous les nombres $\alpha = \mu\omega$ du domaine 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 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 $\alpha - \alpha' = \mu(\omega - \omega')$ 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 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, 1^0 et 2^0, 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, entiè-

rement délivrée de toute obscurité et de l'admission des nombres idéaux*):

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**).

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 $\mathfrak{a}\mathfrak{b}$***).

Or on voit immédiatement, il est vrai, que le produit $\mathfrak{a}\mathfrak{b}$ est divisible 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 diffi-

*) 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.

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

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

cultés caractéristiques, profondément attachées à la nature du sujet; cette liaison s'exprime essentiellement par les deux théorèmes suivants:

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

Tout idéal différent de 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.

I.

Théorèmes auxiliaires de la théorie des modules.

Ainsi qu'il ressort de l'Introduction, nous aurons dans la suite à considérer très-souvent des systèmes de nombres qui se repro-

duisent par addition et soustraction; le développement des propriétés générales de pareils systèmes forme l'objet d'une théorie assez étendue, qui peut aussi être utilisée pour d'autres recherches, tandis que, pour notre but, les premiers éléments de cette théorie sont suffisants. Pour ne pas interrompre plus tard le cours de notre exposition, et en même temps pour faire apercevoir plus clairement la portée des divers concepts sur lesquels s'appuie notre théorie suivante des nombres algébriques entiers, il nous semble à propos d'établir préalablement un petit nombre de théorèmes très-simples, bien qu'ils ne puissent offrir un véritable intérêt que par leurs applications. ...

... Les recherches dans cette première Section ont été exposées sous la forme spéciale qui répond à notre but; mais il est clair qu'elles ne cessent en rien d'être vraies, quand les lettres grecques désignent, non plus des nombres, mais des éléments quelconques, objets de l'étude que l'on poursuit, dont deux quelconques α, β, par une opération commutative et uniformément inversible (composition), tenant la place de l'addition, produiront un élément déterminé $\gamma = \alpha + \beta$ de la même espèce; les modules a se changent en groupes d'éléments, dont les résultats (les composés) appartiennent toujours au même groupe; les coefficients rationnels entiers indiquent combien de fois un élément contribue à la génération d'un autre.

II.

Le germe de la théorie des idéaux.

Dans cette Section, je me propose, comme je l'ai déjà indiqué dans l'Introduction, d'expliquer sur un exemple déterminé la nature du phénomène qui a conduit Kummer à la création des nombres idéaux, et j'utiliserai le même exemple pour éclaircir le concept d'idéal introduit par moi, et celui de la multiplication des idéaux.

§ 5. — Les nombres rationnels entiers.

La théorie des nombres s'occupe d'abord exclusivement du système des nombres rationnels entiers $0, \pm 1, \pm 2, \pm 3, \ldots$, et il sera bon de remémorer ici en peu de mots les lois importantes qui régissent ce domaine. Avant tout, il faut rappeler que ces nombres se reproduisent par addition, soustraction et multiplication, c'est-à-

dire que les sommes, les différences et les produits de deux nombres quelconques de ce domaine appartiennent au même domaine. La théorie de la divisibilité considère de préférence la combinaison des nombres par multiplication; le nombre a est dit divisible par le nombre b, lorsque $a = bc$, c étant également un nombre rationnel entier. Le nombre 0 est divisible par un nombre quelconque; les deux unités ± 1 divisent tous les nombres, et elles sont les seuls nombres qui jouissent de cette propriété. Si a est divisible par b, $\pm a$ sera aussi divisible par $\pm b$, et nous pourrons, par conséquent, nous restreindre à la considération des nombres positifs. Tout nombre positif, différent de l'unité, est ou un nombre premier, c'est-à-dire un nombre divisible seulement par lui-même et par l'unité, ou un nombre composé; dans ce dernier cas, on pourra toujours le mettre sous la forme d'un produit de nombres premiers, et, ce qui est le plus important, on ne le pourra que d'une seule manière, c'est-à-dire que le système de tous les nombres premiers qui entrent comme facteurs dans ce produit est complétement déterminé, ainsi que le nombre de fois qu'un nombre premier désigné entre comme facteur. Cette propriété repose essentiellement sur ce théorème, qu'un produit de deux facteurs n'est divisible par un nombre premier que lorsque celui-ci divise au moins un des deux facteurs.

La manière la plus simple de démontrer ces propositions fondamentales de la théorie des nombres est fondée sur la considération du procédé enseigné déjà par Euclide, et qui sert à trouver le plus grand commun diviseur de deux nombres*). Cette opération a, comme on sait, pour base l'application répétée de ce théorème, que, si m désigne un nombre positif, un nombre quelconque z pourra toujours être mis sous la forme $qm + r$, q et r désignant aussi des nombres entiers, dont le second est moindre que m; car il résulte de là que l'opération devra s'arrêter après un nombre fini de divisions.

La notion de la congruence des nombres a été introduite par Gauss**); deux nombres z, z' sont dits congrus par rapport au module m, ce qu'on exprime par la notation

$$z \equiv z' \pmod{m},$$

lorsque la différence $z - z'$ est divisible par m; dans le cas contraire, z et z' sont dits incongrus par rapport à m. Si l'on range

*) Voir, par exemple, les Vorlesungen über Zahlentheorie de Dirichlet.
**) Disquisitiones arithmeticæ, art. 1.

les nombres, pris deux à deux dans la même classe*) de nombres ou dans deux classes différentes suivant qu'ils sont congrus ou incongrus par rapport à m, on conclut aisément du théorème rappelé plus haut que le nombre de ces classes est fini, et qu'il est égal à la valeur absolue du module m. C'est ce qui résulte évidemment aussi des études de la Section précédente; car la définition de la congruence établie dans la Section I contient celle de Gauss comme cas particulier. Le système $\mathfrak{o}$ de tous les nombres entiers rationnels est identique avec le module fini $[1]$, et de même le système $\mathfrak{m}$ de tous les nombres divisibles par m est identique avec $[m]$; la congruence de deux nombres par rapport au nombre m coïncide avec leur congruence par rapport au système $\mathfrak{m}$; donc (d'après § 3, 2^0, ou § 4, 4^0), le nombre des classes est $= (\mathfrak{o}, \mathfrak{m}) = \pm m$.

§ 6. — Les nombres complexes entiers de Gauss.

Le premier et le plus grand pas vers la généralisation de ces notions a été fait par Gauss, dans son second Mémoire sur les résidus biquadratiques, lorsqu'il les a transportées au domaine des nombres complexes entiers $x + yi$, x et y désignant des nombres rationnels entiers quelconques, et i étant $= \sqrt{-1}$, c'est-à-dire une racine de l'équation quadratique irréductible $i^2 + 1 = 0$. Les nombres de ce domaine se reproduisent encore par addition, soustraction et multiplication, et l'on peut par conséquent définir pour ces nombres la notion de divisibilité de la même manière que pour les nombres rationnels. On peut établir très-simplement, comme Dirichlet l'a montré d'une manière très-élégante**), que les propositions générales sur la composition des nombres au moyen de nombres premiers subsisteront encore dans ce nouveau domaine, en s'appuyant sur la remarque suivante. Si l'on entend par la norme $N(w)$ d'un nombre $w = u + vi$, u et v désignant des nombres rationnels quelconques, le produit $u^2 + v^2$ des deux nombres conjugués $u + vi$ et $u - vi$, la norme d'un produit sera égale au produit des normes des facteurs, et en outre il est clair que, w étant donné, on pourra toujours

*) Le mot classe semble avoir été employé par Gauss pour la première fois dans ce sens à propos des nombres complexes. (Theoria residuorum biquadraticorum, II, art. 42.)

**) Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. (Journal de Crelle, t. 24.)

choisir un nombre complexe entier q, de telle sorte que l'on ait $N(w-q) \leqq \frac{1}{2}$; en désignant maintenant par z et m deux nombres complexes entiers quelconques, dont le second soit différent de zéro, il en résulte, si l'on prend $w = \frac{z}{m}$, que l'on pourra toujours poser $z = qm + r$, q et r étant des nombres complexes entiers, et cela de telle manière que l'on ait $N(r) < N(m)$. On pourra donc, absolument comme pour les nombres rationnels, trouver par un nombre fini de divisions le plus grand commun diviseur de deux nombres complexes entiers quelconques, et les démonstrations des lois générales de la divisibilité des nombres rationnels entiers pourront s'appliquer presque mot pour mot au domaine des nombres complexes entiers. Il y a quatre unités, ± 1, $\pm i$, c'est-à-dire quatre nombres qui divisent tous les nombres, et dont la norme est, par suite, $= 1$. Tout autre nombre différent de zéro est dit un nombre composé, lorsqu'il peut être représenté par le produit de deux facteurs dont aucun n'est une unité; dans le cas contraire, le nombre est dit un nombre premier, et un tel nombre ne peut diviser un produit s'il ne divise au moins l'un des facteurs. Tout nombre composé peut toujours, et d'une seule manière, être mis sous la forme d'un produit de nombres premiers, les quatre nombres premiers associés $\pm q$, $\pm qi$ ne comptant naturellement que comme les représentants d'un seul et même nombre premier q. L'ensemble de tous les nombres premiers q du domaine des nombres complexes entiers se compose:

1° De tous les nombres premiers rationnels qui (pris positivement) sont de la forme $4n + 3$;

2° Du nombre $1 + i$, qui divise le nombre premier rationnel $2 = (1 + i)(1 - i) = -i(1 + i)^2$;

3° Des couples de deux facteurs $a + bi$ et $a - bi$, contenus dans tout nombre premier rationnel p de la forme $4n + 1$, et dont la norme $a^2 + b^2 = p$.

L'existence des nombres premiers $a \pm bi$, cités en dernier lieu, laquelle résulte immédiatement du célèbre théorème de Fermat contenu dans l'équation $p = a^2 + b^2$, et entraîne réciproquement ce théorème comme conséquence, se déduit ici sans le secours de ce théorème, avec une merveilleuse facilité, et ce n'est là qu'un premier exemple de la puissance extraordinaire des principes auxquels nous

parviendrons par la plus grande généralisation de l'idée de nombre entier.

La congruence des nombres complexes entiers par rapport à un nombre donné de même nature m peut aussi se définir absolument de la même manière que dans la théorie de nombres rationnels; les nombres z, z' sont dits congrus par rapport à m, et l'on pose $z \equiv z' \pmod{m}$ lorsque la différence $z - z'$ est divisible par m. Si l'on range les nombres, pris deux à deux, dans la même classe ou dans deux classes différentes, suivant qu'ils sont congrus ou incongrus par rapport à m, le nombre total des classes différentes sera fini, et $= N(m)$. C'est ce qui résulte très-facilement des recherches de la première Section; car le système $\mathfrak{o}$ de tous les nombres complexes entiers $x + yi$ forme un module fini $[1, i]$, et pareillement le système $\mathfrak{m}$ de tous les nombres $m(x + yi)$ divisibles par m forme le module $[m, mi]$, dont la base est liée avec celle de $\mathfrak{o}$ par deux équations de la forme

$$m = a.1 + b.i, \quad mi = -b.1 + a.i;$$

par suite, on a (§ 4, 4°)

$$(\mathfrak{o}, \mathfrak{m}) = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = N(m).$$

§ 7. — Le domaine $\mathfrak{o}$ des nombres $x + y\sqrt{-5}$.

Il y a encore d'autres domaines numériques qui peuvent se traiter absolument de la même manière. Désignons, par exemple, par θ une racine de l'une des cinq équations

$$\theta^2 + \theta + 1 = 0, \quad \theta^2 + \theta + 2 = 0,$$
$$\theta^2 + 2 = 0, \quad \theta^2 - 2 = 0, \quad \theta^2 - 3 = 0,$$

et faisons prendre à x, y toutes les valeurs rationnelles et entières; les nombres $x + y\theta$ formeront un domaine numérique correspondant. Dans chacun de ces domaines, comme il est aisé de s'en assurer, on peut trouver le plus grand commun diviseur de deux nombres par un nombre fini de divisions, et il s'ensuit de là immédiatement que les lois générales de la divisibilité coïncident avec celles qui ont lieu pour les nombres rationnels, bien que, dans les deux derniers exemples, apparaisse cette circonstance, que le nombre des unités est infini.

Cette méthode, au contraire, n'est plus applicable au domaine o des nombres entiers

$$\omega = x + y\theta,$$

où θ est une racine de l'équation

$$\theta^2 + 5 = 0,$$

x, y prenant encore toutes les valeurs rationnelles et entières. Ici l'on rencontre déjà le phénomène qui a suggéré à Kummer la création des nombres idéaux, et que nous allons maintenant décrire en détail sur quelques exemples.

Les nombres ω du domaine o, dont il sera exclusivement question dans ce qui va suivre, se reproduisent encore par addition, soustraction et multiplication, et nous définirons, par suite, exactement comme dans ce qui précède, les notions de divisibilité et de congruence des nombres. Si l'on appelle, de plus, norme $N(\omega)$ d'un nombre $\omega = x + y\theta$ le produit $x^2 + 5y^2$ des deux nombres conjugués $x \pm y\theta$, la norme d'un produit sera égale au produit des normes de tous les facteurs; et si μ est un nombre déterminé, différent de zéro, on en conclut, absolument comme ci-dessus, que $N(\mu)$ exprime combien il y a de nombres non congrus par rapport à μ. Si μ est une unité, et partant divise tous les nombres, il faut que l'on ait $N(\mu) = 1$, d'où $\mu = \pm 1$.

Nous appellerons décomposable un nombre (différent de zéro et de ± 1), lorsqu'il sera le produit de deux facteurs dont aucun ne sera une unité; dans le cas contraire, le nombre sera dit indécomposable. Alors il résulte bien du théorème sur la norme d'un produit que tout nombre décomposable peut être mis sous la forme d'un nombre fini de facteurs indécomposables; mais dans une infinité de cas il se présente ici un phénomène tout nouveau, savoir, qu'un seul et même nombre est susceptible de plusieurs représentations de cette sorte, essentiellement différentes entre elles. Les exemples les plus simples de ces cas sont les suivants. Il est aisé de se convaincre que chacun des quinze nombres suivants:

$$a = 2, \quad b = 3, \quad c = 7;$$

$$b_1 = -2 + \theta, \quad b_2 = -2 - \theta; \quad c_1 = 2 + 3\theta, \quad c_2 = 2 - 3\theta;$$

$$d_1 = 1 + \theta, \quad d_2 = 1 - \theta; \quad e_1 = 3 + \theta, \quad e_2 = 3 - \theta;$$

$$f_1 = -1 + 2\theta, \quad f_2 = -1 - 2\theta; \quad g_1 = 4 + \theta, \quad g_2 = 4 - \theta$$

est indécomposable. En effet, pour qu'un nombre premier rationnel p soit décomposable et, par suite, de la forme $\omega\omega'$, il faut que $N(p) = p^2 = N(\omega)N(\omega')$, et comme ω, ω' ne sont pas des unités, on devra avoir $p = N(\omega) = N(\omega')$, c'est-à-dire que p devra pouvoir se représenter par la forme quadratique binaire $x^2 + 5y^2$. Or les trois nombres premiers 2, 3, 7, comme on le voit par la théorie de ces formes*), ou encore par un petit nombre d'essais directs, ne peuvent pas se représenter de cette manière; ils sont donc indécomposables. Il est aisé de démontrer la même chose, et d'une manière semblable, pour les douze autres nombres, dont les normes sont les produits de deux de ces trois nombres premiers. Mais, malgré l'indécomposabilité de ces quinze nombres, il existe entre leurs produits de nombreuses relations, qui toutes peuvent se déduire des suivantes:

$$(1) \qquad ab = d_1 d_2, \quad b^2 = b_1 b_2, \quad ab_1 = d_1^2,$$

$$(2) \qquad ac = e_1 e_2, \quad c^2 = c_1 c_2, \quad ac_1 = e_1^2,$$

$$(3) \qquad bc = f_1 f_2 = g_1 g_2, \quad af_1 = d_1 e_1, \quad ag_1 = d_1 e_2.$$

Dans chacune de ces dix relations, un même nombre est représenté de deux ou trois manières différentes sous la forme d'un produit de deux nombres indécomposables; on voit donc qu'un nombre indécomposable peut très-bien diviser un produit, sans toutefois diviser l'un ou l'autre des facteurs; un tel nombre indécomposable ne possède donc pas la propriété qui, dans la théorie des nombres rationnels, est tout à fait caractéristique pour un nombre premier.

Imaginons pour un instant que les quinze nombres précédents soient des nombres rationnels entiers; alors, d'après les lois générales de la divisibilité, on déduirait aisément des relations (1) une décomposition de la forme

$$a = \mu\alpha^2, \quad d_1 = \mu\alpha\beta_1, \quad d_2 = \mu\alpha\beta_2,$$
$$b = \mu\beta_1\beta_2, \quad b_1 = \mu\beta_1^2, \quad b_2 = \mu\beta_2^2,$$

et de même, des relations (2) une décomposition de la forme

$$a = \mu'\alpha'^2, \quad e_1 = \mu'\alpha'\gamma_1, \quad e_2 = \mu'\alpha'\gamma_2,$$
$$c = \mu'\gamma_1\gamma_2, \quad c_1 = \mu'\gamma_1^2, \quad c_2 = \mu'\gamma_2^2,$$

où toutes les lettres grecques désignent des nombres rationnels entiers, et il en résulterait immédiatement, en vertu de l'équation

*) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 71.

$\mu\alpha^2 = \mu'\alpha'^2$, que les quatre nombres f_1, f_2, g_1, g_2, qui entrent dans les relations (3), seraient également des nombres entiers. Ces décompositions se simplifient si l'on introduit, en outre, l'hypothèse que a est un nombre premier avec b et avec c; car on tire de là $\mu = \mu' = 1$, $\alpha = \alpha'$, et l'on obtient les quinze nombres, exprimés comme il suit, au moyen des cinq nombres α, β_1, β_2, γ_1, γ_2,

$$(4)\quad \begin{cases} a = \alpha^2, \quad b = \beta_1\beta_2, \quad c = \gamma_1\gamma_2; \\ b_1 = \beta_1^2, \quad b_2 = \beta_2^2; \quad c_1 = \gamma_1^2, \quad c_2 = \gamma_2^2; \\ d_1 = \alpha\beta_1, \quad d_2 = \alpha\beta_2; \quad e_1 = \alpha\gamma_1, \quad e_2 = \alpha\gamma_2; \\ f_1 = \beta_1\gamma_1, \quad f_2 = \beta_2\gamma_2; \quad g_1 = \beta_1\gamma_2, \quad g_2 = \beta_2\gamma_1. \end{cases}$$

Quoique maintenant nos quinze nombres soient en réalité indécomposables, ils se comportent cependant, chose remarquable, dans toutes les questions de divisibilité relatives au domaine o, absolument comme s'ils étaient composés, de la manière indiquée ci-dessus, au moyen de cinq nombres premiers α, β_1, β_2, γ_1, γ_2, différents les uns des autres. Je vais exposer tout à l'heure en détail ce qu'il faut entendre par cette relation des nombres.

§ 8. — Rôle du nombre 2 dans le domaine o.

Dans ce dessein, je remarque avant tout que, dans la théorie des nombres rationnels entiers, on peut reconnaître complétement la constitution essentielle d'un nombre, sans en effectuer la décomposition en facteurs premiers, en observant seulement la manière dont il se comporte comme diviseur. Si l'on sait, par exemple, qu'un nombre positif a ne divise un produit de deux carrés que si l'un au moins de ces carrés est divisible par a, on en conclut avec certitude que a est égal à 1, ou qu'il est un nombre premier ou le carré d'un nombre premier. Il est pareillement certain qu'un nombre a doit contenir au moins un facteur carré, outre l'unité, lorsqu'on peut démontrer l'existence d'un nombre non divisible par a, et dont le carré est divisible par a. Si l'on peut donc constater, pour un nombre a, l'un et l'autre de ces deux caractères, on en conclut d'une manière sûre que a est le carré d'un nombre premier.

Nous allons maintenant examiner, dans ce sens, comment se comporte le nombre 2 dans notre domaine o des nombres $\omega = x + y\theta$. Comme deux nombres conjugués quelconques sont congrus par rapport au module 2, on aura

$$\omega^2 \equiv N(\omega) \pmod 2,$$

et par suite aussi $\omega^2 \omega'^2 \equiv N(\omega) N(\omega') \pmod 2$; maintenant, pour que le nombre 2 divise le produit $\omega^2 \omega'^2$, et par suite aussi le produit des deux nombres rationnels $N(\omega)$, $N(\omega')$, il faut que l'une au moins de ces normes, et par suite aussi que l'un au moins des deux carrés ω^2, ω'^2 soient divisibles par 2. Si de plus on choisit pour x, y deux nombres impairs quelconques, on obtient un nombre $\omega = x + y\theta$ non divisible par 2, et dont le carré est divisible par 2. En ayant égard aux remarques précédentes sur les nombres rationnels, nous dirons donc que le nombre 2 se comporte dans notre domaine o comme s'il était le carré d'un nombre premier α.

Bien qu'un tel nombre premier α n'existe nullement dans le domaine o, nous n'en introduirons pas moins, comme l'a fait Kummer avec grand succès dans des circonstances semblables, un pareil nombre α sous le nom de nombre idéal, et nous nous laisserons d'abord conduire par l'analogie avec la théorie des nombres rationnels, pour définir avec précision la présence du nombre α dans les nombres existants quelconques ω du domaine o. Or, quand un nombre rationnel a est déjà reconnu comme étant le carré d'un nombre premier rationnel α, on peut aisément, sans même avoir à faire intervenir α, juger si α est contenu et combien de fois il est contenu comme facteur dans un nombre rationnel entier quelconque z; car il est clair que z est divisible par a^n toutes les fois, et alors seulement, que z^2 est divisible par a^n. Nous étendrons donc ce critérium au cas qui nous occupe, et nous dirons qu'un nombre ω du domaine o est divisible par la $n^{\text{ième}}$ puissance α^n du nombre premier idéal α, lorsque ω^2 sera divisible par 2^n. Le succès fera voir que cette définition est très-heureusement*) choisie, parce qu'elle conduit à un mode d'expression en harmonie parfaite avec les lois de la théorie des nombres rationnels.

Il s'ensuit d'abord, pour $n = 1$, qu'un nombre $\omega = x + y\theta$ est divisible par α dans le cas, et seulement dans ce cas, où $N(\omega)$ est un nombre pair, et où l'on a, par suite,

$$(\alpha) \qquad x \equiv y \pmod 2.$$

*) Heureusement, car, par exemple, la tentative de déterminer d'une manière analogue le rôle du nombre 2 dans le domaine des nombres $x + y\sqrt{-3}$ aurait complétement échoué; plus tard nous découvrirons clairement la raison de ce phénomène.

Le nombre ω n'est pas divisible par α, quand $N(\omega)$ est un nombre impair, et que l'on a par suite $x \equiv 1 + y \pmod 2$; et de là résulte évidemment le théorème dans lequel on reconnaîtra le caractère du nombre idéal α comme nombre premier: «Tout produit de deux nombres non divisibles par α est aussi non divisible par α».

Relativement aux puissances supérieures de α, on conclut d'abord de la définition qu'un nombre ω divisible par α^n l'est aussi par toutes les puissances inférieures de α, puisqu'un nombre ω^2 divisible par 2^n l'est aussi par toutes les puissances inférieures de 2. Nous allons maintenant, si ω est différent de zéro, chercher l'exposant m de la plus haute puissance de α qui divise ω, c'est-à-dire l'exposant de la plus haute puissance de 2 qui divise ω^2. Soit s l'exposant de la plus haute puissance de 2 qui divise ω lui-même; on aura

$$\omega = 2^s \omega_1 = 2^s (x_1 + y_1 \theta),$$

et l'un au moins des deux nombres rationnels entiers x_1, y_1 sera impair; si les deux sont impairs, ω_1 sera divisible par α, et l'on aura

$$\omega_1^2 = x_1^2 - 5 y_1^2 + 2 x_1 y_1 \theta = 2 \omega_2,$$

$\omega_2 = x_2 + y_2 \theta$ n'étant pas divisible par α, puisque x_2 est pair et y_2 impair; mais si l'un des deux nombres x_1, y_1 est pair, et partant l'autre impair, ω_1 et par suite aussi ω_1^2 ne seront pas divisibles par α. Donc, dans le premier cas, $m = 2s + 1$; dans le second cas, $m = 2s$; mais dans les deux cas $\omega^2 = 2^m \omega'$, ω' désignant un nombre non divisible par α. On voit en même temps que m est aussi l'exposant de la plus haute puissance de 2 qui divise la norme $N(\omega)$; on a donc ce théorème: «L'exposant de la plus haute puissance de α qui divise un produit est égal à la somme des exposants des plus hautes puissances de α qui divisent les facteurs.» Il est pareillement évident que tout nombre ω divisible par α^{2n} est aussi divisible par 2^n; car, si l'exposant désigné plus haut par s était $< n$, les nombres $2s$, $2s + 1$, et par suite aussi m seraient $< 2n$, ce qui est contre l'hypothèse. Il suit immédiatement de la définition que, réciproquement, tout nombre divisible par 2^n l'est aussi par α^{2n}.

Le nombre $1 + \theta$ étant divisible par α, mais ne l'étant pas par α^2, on reconnaît aisément, à l'aide du théorème précédent, que la congruence $\omega^2 \equiv 0 \pmod{2^n}$, qui a servi de définition pour la di-

visibilité du nombre ω par α^n, peut être complétement remplacée par la congruence

$$(\alpha^n) \qquad \omega(1+\theta)^n \equiv 0 \pmod{2^n},$$

qui a l'avantage de ne contenir le nombre ω qu'à la première puissance.

§ 9. — Rôle des nombres 3 et 7 dans le domaine o.

Quand toutes les quantités qui entrent dans les équations (4) du § 7 sont des nombres rationnels entiers, et qu'en même temps a est premier avec b et avec c, il est évident qu'un nombre rationnel entier quelconque z sera ou ne sera pas divisible par β_1, β_2, γ_1, γ_2, selon qu'il satisfera ou ne satisfera pas à la congruence correspondante

$$z d_2 \equiv 0, \quad z d_1 \equiv 0 \pmod{b},$$
$$z e_2 \equiv 0, \quad z e_1 \equiv 0 \pmod{c}.$$

Ces congruences ont maintenant ceci de particulier, que les nombres β_1, β_2, γ_1, γ_2 n'y entrent aucunement par eux-mêmes, et c'est précisément pour cela que, dans le cas que nous traitons effectivement, et où il s'agit de nombres du domaine o, elles sont appropriées pour servir à l'introduction de quatre nombres idéaux β_1, β_2, γ_1, γ_2. Nous dirons qu'un nombre quelconque $\omega = x + y\theta$ est divisible par l'un de ces quatre nombres, si ω est une racine de la congruence correspondante

$$(1-\theta)\omega \equiv 0, \quad (1+\theta)\omega \equiv 0 \pmod{3},$$
$$(3-\theta)\omega \equiv 0, \quad (3+\theta)\omega \equiv 0 \pmod{7}.$$

En effectuant la multiplication, ces congruences se changent dans les suivantes:

$$(\beta_1) \qquad x \equiv y \pmod{3},$$
$$(\beta_2) \qquad x \equiv -y \pmod{3},$$
$$(\gamma_1) \qquad x \equiv 3y \pmod{7},$$
$$(\gamma_2) \qquad x \equiv -3y \pmod{7}.$$

A cela nous rattacherons les remarques suivantes.

Chacune de ces conditions peut être satisfaite par l'un des nombres $\omega = 1+\theta$, $1-\theta$, $3+\theta$, $3-\theta$, ce nombre ne satisfaisant à aucune des trois autres, et il s'ensuit de là qu'il est légitime d'appeler ces quatre nombres idéaux différents entre eux. Comme, en outre, tout nombre ω divisible par β_1 et par β_2 est aussi divisible

par 3, puisque l'on doit avoir $x \equiv y \equiv -y \equiv 0 \pmod 3$, et que réciproquement tout nombre divisible par 3 est aussi divisible par chacun des nombres β_1, β_2, on devrait, par analogie avec la théorie des nombres rationnels, considérer le nombre 3 comme le plus petit commun multiple des deux nombres idéaux β_1, β_2. Mais chacun de ces deux nombres idéaux possède aussi le caractère d'un nombre premier, c'est-à-dire qu'il ne divise un produit $\omega\omega'$ que lorsqu'il divise un au moins des facteurs ω, ω'; si l'on pose, en effet,

$$\omega = x + y\theta, \quad \omega' = x' + y'\theta, \quad \omega'' = \omega\omega' = x'' + y''\theta,$$

on aura

$$x'' = xx' - 5yy', \quad y'' = xy' + yx',$$

et par suite

$$x'' \pm y'' \equiv (x \pm y)(x' \pm y') \pmod 3,$$

ce qui vérifie immédiatement notre assertion, en ayant égard aux congruences ci-dessus (β_1), (β_2). D'après cela, le nombre 3 devra être considéré, à un certain point de vue, comme le produit des deux nombres premiers idéaux différents β_1, β_2.

Comme, de plus, chacun de ces deux nombres premiers idéaux β_1, β_2 est différent (dans le sens indiqué ci-dessus) du nombre premier idéal α introduit plus haut, dès lors, en observant que 2 se comporte comme le carré de α, et que $1 + \theta$ est divisible par α et par β_1, de même que $1 - \theta$ est divisible par α et par β_2, on devra conclure, de l'équation $2.3 = (1 + \theta)(1 - \theta)$, que $1 + \theta$ se comporte comme le produit de α et de β_1, et $1 - \theta$ comme le produit de α et de β_2. Cette présomption se confirme en effet pleinement: tout nombre $\omega = x + y\theta$ divisible par $1 + \theta$ est, en effet, divisible par α et par β_1, puisque

$$x + y\theta = (1 + \theta)(x' + y'\theta),$$

d'où

$$x = x' - 5y', \quad y = x' + y',$$

et par suite

$$x \equiv y \pmod 2, \quad x \equiv y \pmod 3;$$

et réciproquement, tout nombre $\omega = x + y\theta$, divisible par α et par β_1, c'est-à-dire satisfaisant aux deux congruences précédentes, est aussi divisible par $1 + \theta$, puisque l'on a $y = x + 6y'$, et par suite

$$x + y\theta = (1 + \theta)(x + 5y' + y'\theta).$$

On peut maintenant introduire aussi les puissances des nombres premiers idéaux β_1, β_2, comme on l'a fait plus haut pour les puissances du nombre idéal α; par analogie avec la théorie des nombres

rationnels, nous définirons la divisibilité d'un nombre quelconque ω par β_1^n ou par β_2^n respectivement par les congruences

(β_1^n) $\qquad \omega(1-\theta)^n \equiv 0 \pmod{3^n}$,

(β_2^n) $\qquad \omega(1+\theta)^n \equiv 0 \pmod{3^n}$,

et il en résulterait une suite de théorèmes qui coïncideraient parfaitement avec ceux de la théorie des nombres rationnels. On traiterait de la même façon les nombres premiers idéaux γ_1, γ_2.

§ 10. — Lois de la divisibilité dans le domaine o.

En étudiant d'une manière semblable tout le domaine o des nombres $\omega = x + y\theta$, on trouve les résultats suivants:

1° Tous les nombres premiers rationnels positifs qui sont $\equiv$ 11, 13, 17, 19 (mod 20) se comportent aussi, dans le cas actuel, comme des nombres premiers.

2° Le nombre θ, dont le carré $= -5$, possède le caractère d'un nombre premier; le nombre 2 se comporte comme le carré d'un nombre premier idéal α.

3° Tout nombre premier rationnel positif qui est $\equiv$ 1, 9 (mod 20) peut se décomposer en deux facteurs différents, réellement existants, dont chacun a le caractère d'un nombre premier.

4° Tout nombre premier rationnel positif qui est $\equiv$ 3, 7 (mod 20) se comporte comme un produit de deux nombres premiers idéaux différents entre eux.

5° Tout nombre existant ω, différent de zéro et de ± 1, est ou un des nombres désignés ci-dessus qui ont le caractère de nombres premiers, ou bien il se comporte, dans toutes les questions de divisibilité, comme s'il était un produit composé d'une manière complétement déterminée de facteurs premiers existants et idéaux.

Mais, pour parvenir à ce résultat et acquérir une certitude complète sur la question de savoir si, en réalité, toutes les lois générales de la divisibilité qui régissent le domaine des nombres rationnels peuvent s'étendre à notre domaine o à l'aide des nombres idéaux que nous avons introduits*), il faut encore, comme on s'en

*) Il semblera peut-être à quelques personnes évident a priori que le rétablissement de cette harmonie avec la théorie des nombres rationnels doit pouvoir s'imposer, quoi qu'il arrive, par l'introduction des nombres idéaux; mais l'exemple, déjà donné plus haut, du rôle irrégulier du nombre 2 dans le domaine des nombres $x + y\sqrt{-3}$, suffit bien pour dissiper cette illusion.

apercevra bientôt quand on essayera une déduction rigoureuse, se livrer à une étude très-approfondie, lors même qu'on voudrait supposer connue ici la théorie des résidus quadratiques et celle des formes quadratiques binaires (théorie qui, réciproquement, se tire avec la plus grande facilité de la théorie générale des nombres algébriques entiers). On peut bien atteindre en toute rigueur le but proposé, en suivant la voie indiquée; mais, comme nous l'avons remarqué dans l'Introduction, la plus grande circonspection est nécessaire pour ne pas se laisser entraîner à des conclusions prématurées, et, en particulier, la notion de produit de facteurs quelconques, existants ou idéaux, ne peut être exactement définie qu'à l'aide de détails assez minutieux. A cause de ces difficultés, il semblera toujours désirable de remplacer le nombre idéal de Kummer, qui n'est jamais défini en lui-même, mais seulement comme diviseur des nombres existants ω du domaine o, par un substantif réellement existant, et c'est ce qui peut se faire de plusieurs manières.

On pourrait, par exemple (et, si je ne me trompe, ce serait la voie que Kronecker aurait choisie dans ses recherches), introduire, au lieu des nombres idéaux, des nombres algébriques existants, mais non compris dans le domaine o, et les adjoindre à ce domaine dans le sens que Galois a donné à ce mot. En effet, si l'on pose

$$\beta_1 = \sqrt{-2+\theta}, \quad \beta_2 = \sqrt{-2-\theta},$$

et que l'on choisisse ces radicaux carrés de manière que l'on ait $\beta_1 \beta_2 = 3$, on aura

$$\theta^2 = -5, \quad \beta_1^2 = -2+\theta, \quad \beta_2^2 = -2-\theta,$$

$$\beta_1 \beta_2 = 3, \quad \theta\beta_1 = -2\beta_1 - 3\beta_2, \quad \theta\beta_2 = 3\beta_1 + 2\beta_2,$$

d'où il s'ensuit que les nombres quadrinômes

$$x + y\theta + z_1\beta_1 + z_2\beta_2,$$

où x, y, z_1, z_2 désignent des nombres rationnels entiers quelconques, se reproduiront par addition, soustraction et multiplication; le domaine o' de ces nombres embrasse le domaine o, et tous les nombres idéaux qu'il fallait introduire dans ce dernier pourront être remplacés par des nombres existants du nouveau domaine o'. En posant, par exemple,

$$\alpha = \beta_1 + \beta_2, \quad \gamma_1 = 2\beta_1 + \beta_2, \quad \gamma_2 = \beta_1 + 2\beta_2,$$

toutes les équations (4) du § 7 seront satisfaites; pareillement, les deux facteurs premiers idéaux du nombre 23 dans le domaine $\mathfrak{o}$ seront remplacés par les deux nombres existants $2\beta_1 - \beta_2$ et $-\beta_1 + 2\beta_2$ du domaine $\mathfrak{o}'$, et il en sera de même de tous les nombres idéaux du domaine $\mathfrak{o}$.

Cependant cette voie, bien qu'elle puisse aussi conduire au but, ne me semble pas présenter toute la simplicité désirable, parce que l'on est forcé de passer du domaine donné $\mathfrak{o}$ à un domaine plus compliqué $\mathfrak{o}'$; et il est facile aussi de reconnaître que dans le choix de ce nouveau domaine $\mathfrak{o}'$ il règne un grand arbitraire. Dans l'Introduction, j'ai exposé avec tant de détails le courant d'idées qui m'a conduit à fonder cette théorie sur une tout autre base, savoir, sur la notion de l'idéal, qu'il serait superflu d'y revenir ici, et je me bornerai, en conséquence, à éclaircir cette notion par un exemple.

§ 11. — Idéaux dans le domaine $\mathfrak{o}$.

La condition pour qu'un nombre $\omega = x + y\theta$ soit divisible par le nombre premier idéal α consiste, d'après le § 8, dans la congruence $x \equiv y \pmod 2$; donc, pour obtenir le système $\mathfrak{a}$ de tous les nombres ω divisibles par α, on posera $x = y + 2z$, y et z désignant des nombres rationnels entiers quelconques; ce système $\mathfrak{a}$ se compose donc de tous les nombres de la forme $2z + (1 + \theta)y$, c'est-à-dire que $\mathfrak{a}$ est un module fini, dont la base se compose des deux nombres indépendants 2 et $1 + \theta$, et par suite

$$\mathfrak{a} = [2,\ 1 + \theta].$$

En désignant de même par $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ les systèmes de tous les nombres ω divisibles respectivement par les nombres premiers idéaux β_1, β_2, γ_1, γ_2, on tirera, des congruences correspondantes du § 9,

$$\mathfrak{b}_1 = [3,\ 1 + \theta], \quad \mathfrak{b}_2 = [3,\ 1 - \theta],$$
$$\mathfrak{c}_1 = [7,\ 3 + \theta], \quad \mathfrak{c}_2 = [7,\ 3 - \theta].$$

Si l'on désigne maintenant par $\mathfrak{m}$ un quelconque de ces cinq systèmes, $\mathfrak{m}$ jouira des propriétés suivantes:

I. Les sommes et les différences de deux nombres quelconques du système $\mathfrak{m}$ seront toujours des nombres de ce même système $\mathfrak{m}$.

II. Tout produit d'un nombre du système $\mathfrak{m}$ et d'un nombre du système $\mathfrak{o}$ est un nombre du système $\mathfrak{m}$.

La première propriété, caractéristique de chaque module, est évidente. Pour constater la seconde propriété relativement au système $\mathfrak{m}$, dont la base se compose des deux nombres μ, μ', il suffit évidemment de démontrer que les deux produits $\theta\mu$, $\theta\mu'$ appartiennent au même système; pour le système $\mathfrak{a}$, cela résulte des deux égalités

$$2\theta = -1.2 + 2(1+\theta), \quad (1+\theta)\theta = -3.2 + (1+\theta),$$

et il en est exactement de même pour les autres systèmes. Mais ces deux propriétés peuvent aussi s'établir sans ces vérifications, en s'appuyant sur ce que chacun des cinq systèmes $\mathfrak{m}$ est l'ensemble de tous les nombres ω du domaine $\mathfrak{o}$ qui satisfont à une congruence de la forme

$$\nu\omega \equiv 0 \pmod{\mu},$$

μ, ν étant deux nombres donnés du domaine $\mathfrak{o}$.

Nous appellerons maintenant tout système $\mathfrak{m}$, composé de nombres du domaine $\mathfrak{o}$ et jouissant des deux propriétés I et II, un idéal, et nous nous poserons d'abord le problème de trouver la forme générale de tous les idéaux. En excluant le cas singulier où $\mathfrak{m}$ se compose du seul nombre zéro, et choisissant arbitrairement un nombre μ (différent de zéro), de l'idéal $\mathfrak{m}$, alors, si l'on désigne par μ' le nombre conjugué, la norme $N(\mu) = \mu\mu'$, ainsi que le produit $\theta N(\mu)$, appartiendra aussi, en vertu de II, à l'idéal $\mathfrak{m}$; donc tous les nombres du module $\mathfrak{o} = [1, \theta]$, en les multipliant par le nombre rationnel $N(\mu)$ différent de zéro, se changeront en nombres du module $\mathfrak{m}$, lequel est en même temps un multiple de $\mathfrak{o}$; or il s'ensuit de là (§ 3, 2°) que $\mathfrak{m}$ est un module fini, de la forme $[k, l + m\theta]$, k, l, m étant des nombres rationnels entiers, parmi lesquels k et m pourront être choisis positifs. Puisque $\mathfrak{m}$ possède déjà, comme module, la propriété I, il ne s'agit plus maintenant que de l'assujettir à la propriété II, qui consiste en ce que les deux produits $k\theta$ et $(l + m\theta)\theta$ appartiennent au même système $\mathfrak{m}$. Les conditions nécessaires et suffisantes pour cela consistent, comme on le voit sans peine, en ce que k et l soient divisibles par m et que les nombres rationnels entiers a, b, qui entrent dans l'expression

$$\mathfrak{m} = [ma, m(b+\theta)],$$

satisfassent, en outre, à la congruence

$$b^2 \equiv -5 \pmod{a};$$

si l'on remplace b par un nombre quelconque qui soit $\equiv b \pmod{a}$, l'idéal $\mathfrak{m}$ ne sera pas changé. Les cinq idéaux ci-dessus $\mathfrak{a}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{c}_1$, $\mathfrak{c}_2$ sont évidemment contenus dans cette forme, puisque $(b + \theta)$ peut aussi être remplacé par $-(b + \theta)$.

L'ensemble de tous les nombres conjugués avec les nombres de l'idéal $\mathfrak{m}$ est évidemment aussi un idéal

$$\mathfrak{m}_1 = [m a,\ m(-b + \theta)];$$

deux idéaux de cette sorte $\mathfrak{m}$, $\mathfrak{m}_1$ peuvent être appelés des idéaux conjugués.

Soit μ un nombre quelconque du domaine $\mathfrak{o}$; le système $[\mu, \mu\theta]$ de tous les nombres divisibles par μ formera un idéal, que nous appellerons un idéal principal*), et que nous désignerons par $\mathfrak{o}(\mu)$ ou encore par $\mathfrak{o}\mu$; il est facile de lui donner la forme ci-dessus $[m a,\ m(b + \theta)]$; m est le plus grand nombre rationnel entier qui divise $\mu = m(u + v\theta)$, et l'on a, de plus

$$a = \frac{N(\mu)}{m^2}, \quad v b \equiv u \pmod{a}.$$

On trouve ainsi, par exemple,

$$\mathfrak{o}(\pm 1) = \mathfrak{o} = [1, \theta],$$

et

$$\mathfrak{o}(2) = [2, 2\theta], \quad \mathfrak{o}(3) = [3, 3\theta], \quad \mathfrak{o}(7) = [7, 7\theta],$$

$$\mathfrak{o}(1 \pm \theta) = [6, \pm 1 + \theta], \quad \mathfrak{o}(3 \pm \theta) = [14, \pm 3 + \theta],$$

$$\mathfrak{o}(-2 \pm \theta) = [9, \mp 2 + \theta], \quad \mathfrak{o}(2 \pm 3\theta) = [49, \pm 17 + \theta],$$

$$\mathfrak{o}(-1 \pm 2\theta) = [21, \pm 10 + \theta], \quad \mathfrak{o}(4 \pm \theta) = [21, \pm 4 + \theta].$$

Comme tous les idéaux sont en même temps des modules, nous dirons (d'après le § 2, 1°) que deux nombres ω, ω' sont congrus par rapport à l'idéal $\mathfrak{m}$, et nous poserons $\omega \equiv \omega' \pmod{\mathfrak{m}}$, lorsque la différence $\omega - \omega'$ sera un nombre contenu dans $\mathfrak{m}$; la norme $N(\mathfrak{m})$ de l'idéal $\mathfrak{m} = [m a,\ m(b + \theta)]$ sera le nombre

$$(\mathfrak{o}, \mathfrak{m}) = m^2 a$$

*) Si l'on étend la définition de l'idéal au domaine $\mathfrak{o}$ des nombres rationnels entiers, ou à celui des nombres complexes entiers de Gauss, ou à l'un des cinq domaines $\mathfrak{o}$ dont il a été question dans le § 7, on voit aisément que tout idéal est un idéal principal; il est évident aussi que, dans le domaine des nombres rationnels entiers, la propriété II est déjà contenue dans la propriété I.

des classes dans lesquelles se décompose le domaine $\mathfrak{o}$ par rapport au module $\mathfrak{m}$ (§ 4, 4°). Si $\mathfrak{m}$ est un idéal principal $\mathfrak{o}\mu$, la congruence précédente sera identique avec $\omega \equiv \omega' \pmod{\mu}$, et l'on aura

$$N(\mathfrak{m}) = N(\mu).$$

La norme d'un nombre quelconque $m\{ax + (b+\theta)y\}$ contenu dans l'idéal $\mathfrak{m} = [m\,a,\ m(b+\theta)]$ est égale au produit de $N(\mathfrak{m}) = m^2 a$ par la forme quadratique binaire $a x^2 + 2bxy + cy^2$, dont le déterminant, suivant la définition de Gauss, est $b^2 - ac = -5$*).

§ 12. — Divisibilité et multiplication des idéaux dans le domaine $\mathfrak{o}$.

Je vais maintenant montrer de quelle manière la théorie des nombres $\omega = x + y\theta$ du domaine $\mathfrak{o}$ peut se fonder sur la notion de l'idéal; toutefois, je serai obligé, pour abréger, de laisser au lecteur le soin de développer quelques calculs faciles.

Nous dirons, absolument comme dans la théorie des modules (§ 1, 2°), qu'un idéal $\mathfrak{m}''$ est divisible par un idéal $\mathfrak{m}$, quand tous les nombres du premier seront contenus aussi dans le second. D'après cela, un idéal principal $\mathfrak{o}\mu''$ sera toujours divisible par un idéal principal $\mathfrak{o}\mu$ dans le cas, et seulement dans ce cas, où le nombre μ'' sera divisible par le nombre μ; de là résulte que la théorie de la divisibilité des nombres est contenue dans celle des idéaux. Les conditions nécessaires et suffisantes pour que l'idéal

$$\mathfrak{m}'' = [m''a'',\ m''(b''+\theta)]$$

soit divisible par l'idéal $\mathfrak{m} = [m\,a,\ m(b+\theta)]$ consiste, comme on l'aperçoit immédiatement, dans les trois congruences

$$m''a \equiv m''a'' \equiv m''(b''-b) \equiv 0 \pmod{m\,a}.$$

La définition de la multiplication des idéaux est celle-ci: Si μ parcourt tous les nombres de l'idéal $\mathfrak{m}$, et de même μ' tous les nombres de l'idéal $\mathfrak{m}'$, tous les produits $\mu\mu'$ et leurs sommes formeront un idéal $\mathfrak{m}''$, qui sera dit le produit**) des facteurs $\mathfrak{m}$, $\mathfrak{m}'$, et que l'on désignera par $\mathfrak{m}\mathfrak{m}'$. On aura évidemment $\mathfrak{o}\mathfrak{m} = \mathfrak{m}$, $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}'\mathfrak{m}$,

*) La théorie générale des formes se simplifie cependant un peu si l'on admet aussi les formes $Ax^2 + Bxy + Cy^2$, où B est impair, et si l'on entend toujours par déterminant de la forme le nombre $B^2 - 4AC$.

**) La même définition s'applique aussi à la multiplication de deux modules quelconques.

$(\mathfrak{m}\mathfrak{m}')\mathfrak{n} = \mathfrak{m}(\mathfrak{m}'\mathfrak{n})$, et de là s'ensuivent, pour les produits d'un nombre quelconque d'idéaux, les mêmes théorèmes que pour les produits de nombres*); de plus, il est clair que le produit des deux idéaux principaux $\mathfrak{o}\mu$ et $\mathfrak{o}\mu'$ est l'idéal principal $\mathfrak{o}(\mu\mu')$.

Soient donnés maintenant deux idéaux,

$$\mathfrak{m} = [m\,a,\ m(b+\theta)],\quad \mathfrak{m}' = [m'\,a',\ m'(b'+\theta)];$$

on déduira de là leur produit

$$\mathfrak{m}'' = \mathfrak{m}\,\mathfrak{m}' = [m''\,a'',\ m''(b''+\theta)],$$

à l'aide des méthodes indiquées dans la première Section (§ 4, 5° et 6°); car il est clair d'abord, en vertu de la définition, que le produit $\mathfrak{m}\,\mathfrak{m}'$ est un module fini, dont la base se compose des quatre produits

$$m\,m'\,a\,a',\quad m\,m'\,a(b'+\theta),\quad m\,m'\,a'(b+\theta),$$
$$m\,m'(b+\theta)(b'+\theta) = m\,m'[b\,b' - 5 + (b+b')\,\theta],$$

dont deux seulement sont indépendants entre eux. On trouve ainsi, par exemple, pour les idéaux considérés plus haut,

$$\mathfrak{b}_1 = [3,\ 1+\theta],\quad \mathfrak{c}_2 = [7,\ 3-\theta],$$

le produit

$$\mathfrak{b}_1\mathfrak{c}_2 = [21,\ 9-3\,\theta,\quad 7+7\,\theta,\quad 8+2\,\theta];$$

ce module se déduit de celui qui a été considéré à la fin de la première Section (§ 4, 6°), en y faisant $\omega_1 = 1$, $\omega_2 = \theta$, et l'on en tire

$$\mathfrak{b}_1\mathfrak{c}_2 = [21,\ -17+\theta] = [21,\ 4+\theta] = \mathfrak{o}(4+\theta);$$

on obtiendrait absolument de la même manière les résultats suivants, entièrement analogues aux équations hypothétiques (4) du § 7:

$$\begin{aligned}
\mathfrak{o}(2) &= \mathfrak{a}^2,\quad \mathfrak{o}(3) = \mathfrak{b}_1\mathfrak{b}_2,\quad \mathfrak{o}(7) = \mathfrak{c}_1\mathfrak{c}_2;\\
\mathfrak{o}(-2+\theta) &= \mathfrak{b}_1^2,\quad \mathfrak{o}(-2-\theta) = \mathfrak{b}_2^2;\\
\mathfrak{o}(2+3\,\theta) &= \mathfrak{c}_1^2,\quad \mathfrak{o}(2-3\,\theta) = \mathfrak{c}_2^2;\\
\mathfrak{o}(1+\theta) &= \mathfrak{a}\mathfrak{b}_1,\quad \mathfrak{o}(1-\theta) = \mathfrak{a}\mathfrak{b}_2;\\
\mathfrak{o}(3+\theta) &= \mathfrak{a}\mathfrak{c}_1,\quad \mathfrak{o}(3-\theta) = \mathfrak{a}\mathfrak{c}_2;\\
\mathfrak{o}(-1+2\,\theta) &= \mathfrak{b}_1\mathfrak{c}_1,\quad \mathfrak{o}(-1-2\,\theta) = \mathfrak{b}_2\mathfrak{c}_2;\\
\mathfrak{o}(4+\theta) &= \mathfrak{b}_1\mathfrak{c}_2,\quad \mathfrak{o}(4-\theta) = \mathfrak{b}_2\mathfrak{c}_1.
\end{aligned}$$

Pour effectuer en général la multiplication de deux idéaux quelconques $\mathfrak{m}$, $\mathfrak{m}'$, il faut transformer la base composée des quatre

*) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 2.

nombres ci-dessus en une autre composée seulement des deux nombres $m''a''$, $m''(b''+\theta)$. On y parvient (en vertu du § 4), au moyen de quatre équations de la forme

$$\begin{aligned} mm'aa' &= p\ m''a'' + q\ m''(b''+\theta), \\ mm'a(b'+\theta) &= p'\ m''a'' + q'\ m''(b''+\theta), \\ mm'a'(b+\theta) &= p''m''a'' + q''m''(b''+\theta), \\ mm'[bb'-5+(b+b')\theta] &= b'''m''a'' + q'''m''(b''+\theta), \end{aligned}$$

où p, p', ..., q''' désignent huit nombres rationnels entiers tellement choisis que les six déterminants, formés avec ces nombres,

$$P = p\,q' - q\,p', \quad Q = p\,q'' - q\,p'', \quad R = p\,q''' - q\,p''',$$
$$U = p''q''' - q''p''', \quad T = p'q''' - q'p''', \quad S = p'q'' - q'p'',$$

n'admettent aucun diviseur commun. Des quatre équations précédentes, dont chacune se décompose en deux autres, on conclura maintenant sans peine que ces six déterminants sont respectivement proportionnels aux six nombres

$$\begin{aligned} &a, \quad a', \quad b'+b, \\ &c, \quad c', \quad b'-b, \end{aligned}$$

c et c' étant déterminés par les équations

$$bb - ac = b'b' - a'c' = -5;$$

or, comme ces six nombres n'admettent non plus aucun diviseur commun*), ils devront coïncider précisément avec ces six déterminants. Il s'ensuit de là, puisque l'on a $q = 0$, et que q', q'', q''' ne peuvent avoir aucun diviseur commun, que l'on déterminera comme il suit le produit $\mathfrak{m}'' = \mathfrak{m}\mathfrak{m}'$ des deux facteurs donnés $\mathfrak{m}$, $\mathfrak{m}'$. Soit p le plus grand commun diviseur (positif) des trois nombres donnés

$$a = pq', \quad a' = pq'', \quad b+b' = pq''';$$

on aura

$$m'' = pmm', \quad a'' = \frac{aa'}{p^2} = q'q'',$$

et b'' sera déterminé par les congruences

$$q'b'' \equiv q'b', \quad q''b'' \equiv q''b, \quad q'''b'' \equiv \frac{bb'-5}{p} \pmod{a''};$$

puis on aura en même temps $b''b'' \equiv -5 \pmod{a''}$, c'est-à-dire

$$b''b'' - a''c'' = -5,$$

*) Il n'en serait pas toujours ainsi dans le domaine des nombres $x + y\sqrt{-3}$.

c'' désignant un nombre rationnel entier, et, d'après la dénomination employée par Gauss*), la forme quadratique binaire (a'', b'', c'') sera composée des deux formes (a, b, c) et (a', b', c').

Des valeurs de m'', a'' on tire $m''^2 a'' = m^2 a . m'^2 a'$, d'où ce théorème

$$N(\mathfrak{m}\mathfrak{m}') = N(\mathfrak{m})\, N(\mathfrak{m}');$$

en outre, il faut remarquer le cas particulier où $\mathfrak{m}'$ est l'idéal $\mathfrak{m}_1$ conjugué avec $\mathfrak{m}$; des formules précédentes on déduit immédiatement ce résultat

$$\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}\, N(\mathfrak{m}).$$

Les deux notions de la divisibilité et de la multiplication des idéaux sont maintenant liées entre elles de la manière suivante. Le produit $\mathfrak{m}\mathfrak{m}'$ est divisible à la fois par $\mathfrak{m}$ et par $\mathfrak{m}'$, puisque, en vertu de la propriété II des idéaux, tous les produits $\mu\mu'$, dont les facteurs sont contenus respectivement dans $\mathfrak{m}$, $\mathfrak{m}'$, appartiennent également à ces idéaux; on tirerait la même conclusion de la forme de l'idéal-produit trouvée plus haut. Réciproquement, si l'idéal $\mathfrak{m}'' = [m''a'', m''(b'' + \theta)]$ est divisible par l'idéal $\mathfrak{m} = [ma, m(b + \theta)]$, il existera un idéal $\mathfrak{m}'$, et un seul, tel que l'on aura $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$; si l'on désigne, en effet, par $\mathfrak{m}_1$ l'idéal conjugué de $\mathfrak{m}$, et que l'on forme, d'après les règles précédentes, le produit

$$\mathfrak{m}_1\mathfrak{m}'' = [m'''a', m'''(b' + \theta)],$$

il résulte, des trois congruences établies au commencement de ce paragraphe, que m''' est divisible par $N(\mathfrak{m}) = m^2 a$, et par suite que $m''' = m^2 a m'$, m' désignant un nombre entier; en joignant à cela le théorème précédent, que $\mathfrak{m}\mathfrak{m}_1 = \mathfrak{o}(m^2 a)$, on en conclut aisément que l'idéal $\mathfrak{m}' = [m'a', m'(b' + \theta)]$, et lui seul, remplit la condition $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}''$. Il en résulte en même temps que l'égalité $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}\mathfrak{m}'''$ entraîne toujours l'égalité $\mathfrak{m}' = \mathfrak{m}'''$.

Pour arriver maintenant à la conclusion de cette théorie, il ne nous reste plus qu'à introduire encore la notion suivante: un idéal $\mathfrak{p}$, différent de $\mathfrak{o}$ et n'ayant pour diviseur aucun autre idéal que $\mathfrak{o}$ et $\mathfrak{p}$, sera dit un idéal premier. η étant un nombre déterminé, le système $\mathfrak{r}$ de toutes les racines ϱ de la congruence $\eta\varrho \equiv 0 \pmod{\mathfrak{p}}$ formera un idéal, parce qu'il possède les propriétés I et II;

*) Disquisitiones arithmeticæ, art. 235, 242.

cet idéal $\mathfrak{r}$ est un diviseur de $\mathfrak{p}$, puisque tous les nombres contenus dans $\mathfrak{p}$ sont aussi des racines de cette congruence; donc, si $\mathfrak{p}$ est un idéal premier, $\mathfrak{r}$ devra être ou $= \mathfrak{o}$ ou $= \mathfrak{p}$. Si le nombre donné η n'est pas contenu dans $\mathfrak{p}$, le nombre 1, contenu dans $\mathfrak{o}$, ne sera pas une racine de la congruence, et partant dans ce cas $\mathfrak{r}$ ne sera pas $= \mathfrak{o}$, mais $= \mathfrak{p}$, c'est-à-dire que toutes les racines ϱ devront être contenues dans $\mathfrak{p}$. Ainsi se trouve évidemment établi le théorème suivant*): «Un produit $\eta\varrho$ de deux nombres η, ϱ n'est contenu dans un idéal premier $\mathfrak{p}$ que si l'un au moins des deux facteurs est contenu dans $\mathfrak{p}$.» Et de là résulte immédiatement cet autre théorème: «Si aucun des deux idéaux $\mathfrak{m}$, $\mathfrak{m}'$ n'est divisible par l'idéal premier $\mathfrak{p}$, leur produit $\mathfrak{m}\mathfrak{m}'$ ne sera pas non plus divisible par $\mathfrak{p}$»; car, puisqu'il y a dans $\mathfrak{m}$, $\mathfrak{m}'$ respectivement des nombres μ, μ' qui ne sont pas contenus dans $\mathfrak{p}$, il existera aussi dans $\mathfrak{m}\mathfrak{m}'$ un nombre $\mu\mu'$ qui ne sera pas non plus contenu dans $\mathfrak{p}$.

En combinant le théorème que nous venons de démontrer avec les théorèmes précédents relatifs à la dépendance entre les notions de divisibilité et de multiplication des idéaux, et ayant égard à ce que, en dehors de $\mathfrak{o}$, il n'existe aucun autre idéal dont la norme soit $= 1$, on arrive, par les mêmes raisonnements**) que dans la théorie des nombres rationnels, au théorème suivant: «Tout idéal différent de $\mathfrak{o}$ ou est un idéal premier, ou peut se mettre, et cela d'une seule manière, sous la forme d'un produit d'un nombre fini d'idéaux premiers.» De ce théorème il résulte immédiatement qu'un idéal $\mathfrak{m}''$ est toujours divisible par un idéal $\mathfrak{m}$ dans le cas, et seulement dans ce cas, où toutes les puissances d'idéaux premiers qui divisent $\mathfrak{m}$ divisent aussi $\mathfrak{m}''$. Si $\mathfrak{m} = \mathfrak{o}\mu$ et $\mathfrak{m}'' = \mathfrak{o}\mu''$ sont des idéaux principaux, le même critérium décide aussi de la divisibilité du nombre μ'' par le nombre μ. Et ainsi la théorie de la divisibilité des nombres dans le domaine $\mathfrak{o}$ se trouve ramenée à des lois fixes et simples.

Toute cette théorie peut s'appliquer presque mot pour mot à un domaine $\mathfrak{o}$ quelconque composé de tous les nombres entiers d'un corps quelconque Ω du second degré, quand la notion de nombre

*) Ce théorème conduit aisément à la détermination de tous les idéaux premiers contenus dans $\mathfrak{o}$, et ceux-ci correspondent exactement aux nombres premiers, existants et idéaux, énumérés dans le § 10.

**) Voir Dirichlet, Vorlesungen über Zahlentheorie, § 8.

entier est définie comme elle l'a été dans l'Introduction*). Mais cette base de la théorie, bien qu'elle ne laisse rien à désirer du côté de la rigueur, n'est nullement celle que je me propose d'établir. On peut remarquer, en effet, que les démonstrations des propositions les plus importantes se sont appuyées sur la représentation des idéaux par l'expression $[m\,a,\ m(b+\theta)]$ et sur la réalisation effective de la multiplication, c'est-à-dire sur un calcul qui coïncide avec la composition des formes quadratiques binaires, enseignée par Gauss. Si l'on voulait traiter de la même manière tous les corps Ω de degré quelconque, on se heurterait à de grandes difficultés, peut-être insurmontables. Mais, lors même qu'il n'en serait pas ainsi, une telle théorie, fondée sur le calcul, n'offrirait pas encore, ce me semble, le plus haut degré de perfection; il est préférable, comme dans la théorie moderne des fonctions, de chercher à tirer les démonstrations, non plus du calcul, mais immédiatement des concepts fondamentaux caractéristiques, et d'édifier la théorie de manière qu'elle soit, au contraire, en état de prédire les résultats du calcul (par exemple, la composition des formes décomposables de tous les degrés). Tel est le but que je vais poursuivre dans les Sections suivantes de ce Mémoire. ...

---

*) Le domaine, mentionné plus haut, des nombres $x+y\sqrt{-3}$, où x, y prennent toutes les valeurs rationnelles et entières, n'est pas un domaine de cette nature; mais il constitue seulement une partie du domaine $\mathfrak{o}$ de tous les nombres $x+y\varrho$, ϱ étant une racine de l'équation $\varrho^2+\varrho+1=0$.

[Erläuterungen gemeinsam mit denen zu XLVI, XLVII, XLIX am Schluß von XLIX.]