BULLETIN DES SCIENCES
MATHÉMATIQUES ET ASTRONOMIQUES

R. DEDEKIND

Sur la théorie des nombres entiers algébriques

Bulletin des sciences mathématiques et astronomiques 2^e *série*, tome 1, n° 1 (1877), p. 207-248

<http://www.numdam.org/item?id=BSMA_1877_2_1_1_207_1>

MÉLANGES.

SUR LA THÉORIE DES NOMBRES ENTIERS ALGÉBRIQUES (¹);

PAR R. DEDEKIND.

(Suite et fin.)

IV.

ÉLÉMENTS DE LA THÉORIE DES IDÉAUX.

Dans cette Section, nous développerons la théorie des idéaux jusqu'au point indiqué dans l'Introduction, c'est-à-dire que nous démontrerons les lois fondamentales qui s'appliquent également à tous les corps finis sans exception, et qui régissent et expliquent les phénomènes de la divisibilité dans le domaine $\mathfrak{o}$ de tous les nombres entiers d'un tel corps Ω. Il ne sera question, dans ce qui va suivre, que de ces seuls nombres, à moins que nous n'indiquions expressément le contraire. La théorie se fonde sur la notion de l'*idéal,* dont nous avons mentionné l'origine dans l'Introduction, et dont l'importance a été suffisamment mise en lumière par l'exemple de la Section II (§§ 11 et 12). L'exposition suivante de la théorie coïncide pour le fond avec celle que j'ai donnée dans la seconde édition des *Vorlesungen über Zahlentheorie* de Dirichlet (§ 163); mais elle en diffère notablement pour la forme extérieure; par ces change-

(¹) Voir *Bulletin*, t. XI, p. 278, et t. I (2ᵉ Série), p. 17, 69 et 144.

ments la théorie, si elle n'est pas abrégée, est cependant un peu simplifiée, et en particulier la principale difficulté qu'il s'agissait de surmonter est maintenant mise plus clairement en relief.

§ 19. — *Les idéaux et leur divisibilité.*

Soient, comme dans la Section précédente, Ω un corps fini du degré n, et $\mathfrak{o}$ le domaine de tous les nombres entiers ω contenus dans Ω. Nous entendons par un *idéal* de ce domaine $\mathfrak{o}$ tout système $\mathfrak{a}$ de nombres α du domaine $\mathfrak{o}$ qui possède les deux propriétés suivantes :

I. Les sommes et les différences de deux nombres α quelconques du système $\mathfrak{a}$ appartiennent au même système $\mathfrak{a}$, c'est-à-dire que $\mathfrak{a}$ est un module.

II. Tout produit $\alpha\omega$ d'un nombre α du système $\mathfrak{a}$ par un nombre ω du système $\mathfrak{o}$ est un nombre du système $\mathfrak{a}$.

Signalons d'abord un cas particulièrement important de cette conception d'*idéal*. Soit μ un nombre déterminé ; le système $\mathfrak{a}$ de tous les nombres $\alpha = \mu\omega$ divisibles par μ formera un idéal. Nous appellerons un tel idéal un *idéal principal*, et nous le désignerons par $\mathfrak{o}(\mu)$, ou plus simplement par $\mathfrak{o}\mu$ ou $\mu\mathfrak{o}$; il est évident que cet idéal ne sera pas altéré si l'on remplace μ par un nombre associé, c'est-à-dire par un nombre de la forme $\varepsilon\mu$, ε désignant une unité. Si μ est lui-même une unité, on aura $\mathfrak{o}\mu = \mathfrak{o}$, puisque tous les nombres contenus dans $\mathfrak{o}$ sont divisibles par μ. Il est encore facile de reconnaître qu'aucun autre idéal ne peut contenir d'unité ; car si l'unité ε est contenue dans l'idéal $\mathfrak{a}$, alors (d'après II) tous les produits $\varepsilon\omega$, et par suite aussi tous les nombres ω de l'idéal principal $\mathfrak{o}$ sont contenus dans $\mathfrak{a}$, et comme, par définition, tous les nombres de l'idéal $\mathfrak{a}$ sont également contenus dans $\mathfrak{o}$, on aura $\mathfrak{a} = \mathfrak{o}$. Cet idéal $\mathfrak{o}$ joue le même rôle parmi les idéaux que le nombre 1 parmi les nombres rationnels entiers. Dans la notion d'un idéal principal $\mathfrak{o}\mu$ est compris aussi le cas singulier où $\mu = 0$, et où par conséquent l'idéal se compose du seul nombre zéro ; toutefois nous exclurons ce cas dans ce qui va suivre.

Dans le cas de $n = 1$, où notre théorie se change dans l'ancienne théorie des nombres, tout idéal est évidemment un idéal principal,

c'est-à-dire un module de la forme $[m]$, m étant un nombre rationnel entier (§§ 1 et 5); il en est également de même des corps quadratiques spéciaux, qui ont été considérés dans la Section II (§ 6 et commencement du § 7). Dans tous ces cas, où tout idéal du corps Ω est un idéal principal, règnent les mêmes lois de la divisibilité des nombres que dans la théorie des nombres rationnels entiers, puisque tout nombre *indécomposable* possède aussi le caractère d'un *nombre premier* (*voir* l'Introduction et le § 7). C'est de quoi l'on pourra aisément se convaincre dans ce qui doit suivre; mais je présente dès maintenant cette remarque pour recommander au lecteur de faire la comparaison continuelle avec les cas spéciaux mentionnés et principalement avec l'ancienne théorie des nombres rationnels, parce que sans aucun doute cela facilitera beaucoup l'intelligence de notre théorie générale.

Puisque tout idéal (en vertu de I) est un module, nous transporterons immédiatement aux idéaux la notion de la divisibilité des modules (§ 1). On dit qu'un idéal $\mathfrak{m}$ est *divisible* par un idéal $\mathfrak{a}$, ou qu'il est un *multiple* de $\mathfrak{a}$, quand tous les nombres contenus dans $\mathfrak{m}$ sont aussi contenus dans $\mathfrak{a}$; on dit en même temps que $\mathfrak{a}$ est un *diviseur* de $\mathfrak{m}$. D'après cela, tout idéal est divisible par l'idéal $\mathfrak{o}$. Si α est un nombre de l'idéal $\mathfrak{a}$, l'idéal principal $\mathfrak{o}\alpha$ sera (d'après II) divisible par $\mathfrak{a}$; nous dirons, pour cette raison, que le *nombre* α, et par suite tout nombre contenu dans $\mathfrak{a}$, est *divisible* par l'idéal $\mathfrak{a}$.

Nous dirons de même qu'un idéal $\mathfrak{a}$ est *divisible* par le *nombre* η, quand $\mathfrak{a}$ sera divisible par l'idéal principal $\mathfrak{o}\eta$; alors tous les nombres α de l'idéal $\mathfrak{a}$ seront de la forme $\eta\rho$, et il est facile de voir que le système $\mathfrak{r}$ de tous les nombres $\rho = \frac{\alpha}{\eta}$ formera un idéal. Réciproquement, si ρ devient égal successivement à tous les nombres d'un idéal quelconque $\mathfrak{r}$, tandis que η désigne un nombre déterminé, différent de zéro, tous les produits $\eta\rho$ formeront encore un idéal divisible par $\mathfrak{o}\eta$; un tel idéal, formé au moyen de l'idéal $\mathfrak{r}$ et du nombre η, et nous le désignerons, pour abréger, par $\mathfrak{r}\eta$ ou $\eta\mathfrak{r}$; on aura évidemment $(\mathfrak{r}\eta)\eta' = \mathfrak{r}(\eta\eta') = (\mathfrak{r}\eta')\eta$, et $\eta\mathfrak{r}'$ sera toujours divisible par $\eta\mathfrak{r}$ dans le cas, et seulement dans ce cas, où $\mathfrak{r}'$ sera divisible par $\mathfrak{r}$; donc l'équation $\eta\mathfrak{r}' = \eta\mathfrak{r}$ entraîne l'équation $\mathfrak{r}' = \mathfrak{r}$. La notion d'un idéal principal $\mathfrak{o}\mu$ se déduit de celle de $\mathfrak{r}\mu$, lorsqu'on suppose $\mathfrak{r} = \mathfrak{o}$.

Enfin il est à remarquer que la divisibilité de l'idéal principal

$\mathfrak{o}\mu$ par l'idéal principal $\mathfrak{o}\eta$ est complétement identique avec la divisibilité du *nombre* μ par le *nombre* η; les lois de la divisibilité des *nombres* de $\mathfrak{o}$ sont donc entièrement contenues dans les lois de la divisibilité des *idéaux*.

Le plus petit commun multiple $\mathfrak{m}$ et le plus grand commun diviseur $\mathfrak{d}$ de deux idéaux quelconques $\mathfrak{a}$, $\mathfrak{b}$ sont aussi des idéaux; car, en tous cas, $\mathfrak{m}$ et $\mathfrak{d}$ sont des modules (§ 1, 3° et 4°), et des modules divisibles par $\mathfrak{o}$, puisque $\mathfrak{a}$ et $\mathfrak{b}$ sont divisibles par $\mathfrak{o}$; si, de plus, $\mu = \alpha = \beta$ est un nombre contenu dans $\mathfrak{m}$ et partant aussi dans $\mathfrak{a}$ et dans $\mathfrak{b}$, et si $\delta = \alpha' + \beta'$ est un nombre du module $\mathfrak{d}$, le produit $\mu\omega = \alpha\omega = \beta\omega$ sera également contenu dans $\mathfrak{m}$, et le produit $\delta\omega = \alpha'\omega + \beta'\omega$ contenu dans $\mathfrak{d}$, puisque (en vertu de II) les produits $\alpha\omega$, $\alpha'\omega$ sont contenus dans $\mathfrak{a}$ et les produits $\beta\omega$, $\beta'\omega$ dans $\mathfrak{b}$. Donc $\mathfrak{m}$ et $\mathfrak{d}$ jouissent de toutes les propriétés d'un idéal. Il est clair en même temps que $\mathfrak{m}\eta$ sera le plus petit commun multiple, et $\mathfrak{d}\eta$ le plus grand commun diviseur des deux idéaux $\mathfrak{a}\eta$, $\mathfrak{b}\eta$.

Si $\mathfrak{b}$ est un idéal principal $\mathfrak{o}\eta$, le plus petit commun multiple $\mathfrak{m}$ de $\mathfrak{a}$, $\mathfrak{b}$ sera en tous cas de la forme $\eta\mathfrak{r}$, $\mathfrak{r}$ étant encore un idéal et, en outre, un diviseur de $\mathfrak{a}$, puisque $\eta\mathfrak{a}$ est un multiple commun de $\mathfrak{a}$ et de $\mathfrak{o}\eta$, et qu'il est par suite divisible par $\eta\mathfrak{r}$; ce cas se présentera très-fréquemment dans la suite, et pour cette raison nous appellerons, pour abréger, l'idéal $\mathfrak{r}$ le diviseur de l'idéal $\mathfrak{a}$ *correspondant* au nombre η. Maintenant si $\mathfrak{r}'$ est le diviseur de $\mathfrak{r}$ correspondant au nombre η', $\mathfrak{r}'$ sera en même temps le diviseur de $\mathfrak{a}$ correspondant au produit $\eta\eta'$; car $\eta\eta'\mathfrak{r}'$ est le plus petit commun multiple de $\eta\mathfrak{r}$ et de $\mathfrak{o}\eta\eta'$, et par conséquent aussi celui de $\mathfrak{a}$ et de $\mathfrak{o}\eta\eta'$, puisque $\eta\mathfrak{r}$ est le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$, et que $\mathfrak{o}\eta\eta'$ est divisible par $\mathfrak{o}\eta$.

§ 20. — *Normes.*

Comme tout idéal $\mathfrak{a}$ est aussi un module, nous dirons que deux nombres quelconques ω, ω' du domaine $\mathfrak{o}$ sont *congrus* ou *incongrus suivant* $\mathfrak{a}$, selon que leur différence $\omega - \omega'$ sera ou non divisible par $\mathfrak{a}$; nous représenterons la congruence de ω, ω' suivant $\mathfrak{a}$ (§ 2) par la notation

$$\omega \equiv \omega' \pmod{\mathfrak{a}}.$$

En outre des théorèmes établis précédemment, ayant lieu pour les

congruences par rapport à des modules quelconques, il faut encore remarquer que deux de ces congruences,

$$\omega \equiv \omega', \quad \omega'' \equiv \omega''' \pmod{\mathfrak{a}},$$

relatives au même idéal $\mathfrak{a}$, peuvent aussi être multipliées entre elles, et qu'elles entraînent ainsi la congruence

$$\omega\omega'' \equiv \omega'\omega''' \pmod{\mathfrak{a}};$$

car les produits $(\omega - \omega')\,\omega''$ et $(\omega'' - \omega''')\,\omega'$, et par suite aussi leur somme $\omega\omega'' - \omega'\omega'''$, sont des nombres de l'idéal $\mathfrak{a}$. Si, de plus, $\mathfrak{m}$ est un idéal principal $\mathfrak{o}\mu$, alors (en vertu du § 18) la congruence $\omega \equiv \omega' \pmod{\mathfrak{m}}$ sera identique avec la congruence $\omega \equiv \omega' \pmod{\mu}$.

Une considération particulièrement importante est celle du *nombre* des classes de nombres différents par rapport à l'idéal $\mathfrak{a}$, et dont se compose le domaine $\mathfrak{o}$. Si μ est un nombre déterminé de l'idéal $\mathfrak{a}$, et différent de zéro, l'idéal principal $\mathfrak{o}\mu$ sera divisible par $\mathfrak{a}$, et comme $\mathfrak{a}$ est divisible par $\mathfrak{o}$, il en résulte (§ 2, 4°)

$$(\mathfrak{o}, \mathfrak{o}\mu) = (\mathfrak{o}, \mathfrak{a})\,(\mathfrak{a}, \mathfrak{o}\mu);$$

or (§ 18) le nombre $(\mathfrak{o}, \mathfrak{o}\mu) = \pm N(\mu)$, et par suite le domaine $\mathfrak{o}$ ne contient qu'un nombre fini de nombres incongrus par rapport à l'idéal $\mathfrak{a}$ (§ 2, 2°). Ce nombre $(\mathfrak{o}, \mathfrak{a})$ sera dit la *norme de l'idéal* $\mathfrak{a}$, et nous le représenterons par $N(\mathfrak{a})$; la norme de l'idéal principal $\mathfrak{o}\mu$ est égale à $\pm N(\mu)$, et $\mathfrak{o}$ est évidemment le seul idéal dont la norme est égale à 1.

Si ρ parcourt un système complet de $N(\mathfrak{a})$ nombres incongrus (mod. $\mathfrak{a}$), la même chose aura lieu pour $(1 + \rho)$, et des congruences correspondantes $1 + \rho \equiv \rho'$, où ρ' parcourt les mêmes valeurs que ρ, résulte, par addition, $N(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{a}}$, c'est-à-dire que $N(\mathfrak{a})$ est toujours divisible par $\mathfrak{a}$. Comme cas particulier, ce résultat contient ce théorème évident par lui-même, que $N(\mu)$ est divisible par μ (*voir* § 17).

Soit, de plus, $\mathfrak{r}$ un idéal quelconque, et η un nombre différent de zéro; on aura toujours

$$(\mathfrak{o}\eta, \mathfrak{r}\eta) = (\mathfrak{o}, \mathfrak{r}) = N(\mathfrak{r});$$

car deux nombres $\eta\omega'$ et $\eta\omega''$ de l'idéal principal $\eta\mathfrak{o}$ sont congrus ou

incongrus (mod. $\eta\mathfrak{r}$), suivant que les nombres ω', ω'' du domaine $\mathfrak{o}$ seront congrus ou incongrus (mod. $\mathfrak{r}$).

Soient $\mathfrak{a}$, $\mathfrak{b}$ deux idéaux quelconques, $\mathfrak{m}$ leur plus petit commun multiple, $\mathfrak{d}$ leur plus grand commun diviseur; on aura (§ 2, 3° et 4°)

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}),$$

et, $\mathfrak{b}$ étant divisible par $\mathfrak{o}$,

$$(\mathfrak{o}, \mathfrak{a}) = (\mathfrak{o}, \mathfrak{b})(\mathfrak{d}, \mathfrak{a}), \quad (\mathfrak{o}, \mathfrak{m}) = (\mathfrak{o}, \mathfrak{b})(\mathfrak{b}, \mathfrak{m}),$$

partant

$$N(\mathfrak{a}) = (\mathfrak{b}, \mathfrak{a})\, N(\mathfrak{d}), \quad N(\mathfrak{m}) = (\mathfrak{b}, \mathfrak{a})\, N(\mathfrak{b}),$$

et

$$N(\mathfrak{m})\, N(\mathfrak{d}) = N(\mathfrak{a})\, N(\mathfrak{b}).$$

Si l'on applique ces théorèmes au cas où $\mathfrak{b}$ est un idéal principal $\mathfrak{o}\eta$, et où par suite $\mathfrak{m}$ est de la forme $\mathfrak{r}\eta$, l'idéal $\mathfrak{r}$ étant le diviseur de $\mathfrak{a}$ correspondant au nombre η (§ 19), il vient

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{o}\eta, \mathfrak{r}\eta) = N(\mathfrak{r}),$$

et par conséquent

$$N(\mathfrak{a}) = N(\mathfrak{r})\, N(\mathfrak{d}).$$

L'idéal $\mathfrak{r}$ peut maintenant aussi être défini comme le système de toutes les racines ρ de la congruence $\eta\rho \equiv 0 \pmod{\mathfrak{a}}$, comme il est facile de s'en convaincre.

§ 21. — *Idéaux premiers.*

Un idéal $\mathfrak{p}$ est dit un *idéal premier*, quand il est différent de $\mathfrak{o}$, et qu'il n'admet comme diviseur aucun autre idéal que $\mathfrak{o}$ et $\mathfrak{p}$. De cette définition résultent les théorèmes suivants :

1° Tout idéal $\mathfrak{a}$ différent de $\mathfrak{o}$ est divisible au moins par un idéal premier.

Car, parmi tous les idéaux qui sont différents de $\mathfrak{o}$ et diviseurs de l'idéal $\mathfrak{a}$, il en existe un $\mathfrak{p}$ dont la norme est la *plus petite*, et celui-là est certainement un idéal premier; si, en effet, $\mathfrak{d}$ était un idéal divisant $\mathfrak{p}$, mais différent de $\mathfrak{p}$ et de $\mathfrak{o}$, on aurait $(\mathfrak{d}, \mathfrak{p}) > 1$, par

suite $N(\mathfrak{p}) = (\mathfrak{b}, \mathfrak{p})\, N(\mathfrak{b}) > N(\mathfrak{b})$, et $\mathfrak{b}$ serait un diviseur de l'idéal $\mathfrak{a}$, différent de $\mathfrak{o}$ et dont la norme serait $< N(\mathfrak{p})$, contre l'hypothèse ; donc $\mathfrak{p}$ est un idéal premier. C. Q. F. D.

2° Si le nombre η n'est pas divisible par l'idéal premier $\mathfrak{p}$, $\eta\mathfrak{p}$ sera le plus petit commun multiple des deux idéaux $\mathfrak{p}$ et $\mathfrak{o}\eta$.

Car le plus petit commun multiple de $\mathfrak{p}$ et de $\mathfrak{o}\eta$ est en tous cas de la forme $\eta\mathfrak{r}$, l'idéal $\mathfrak{r}$ étant un diviseur de $\mathfrak{p}$, et par suite ou $= \mathfrak{o}$ ou $= \mathfrak{p}$ (§ 19) ; mais $\mathfrak{r}$ ne peut pas être $= \mathfrak{o}$, puisque $\eta\mathfrak{o}$ n'est pas divisible par $\mathfrak{p}$; par conséquent $\mathfrak{r} = \mathfrak{p}$. C. Q. F. D.

3° Si aucun des deux nombres η, ρ n'est divisible par l'idéal premier $\mathfrak{p}$, leur produit $\eta\rho$ ne sera pas non plus divisible par $\mathfrak{p}$.

Car autrement l'idéal $\eta(\mathfrak{o}\rho)$ serait un multiple commun de $\mathfrak{p}$, $\mathfrak{o}\eta$; et partant il serait divisible par le plus petit commun multiple $\eta\mathfrak{p}$ de $\mathfrak{p}$, $\mathfrak{o}\eta$; mais de la divisibilité de $\eta(\mathfrak{o}\rho)$ par $\eta\mathfrak{p}$ il résulterait (§ 19) que $\mathfrak{o}\rho$ serait divisible par $\mathfrak{p}$, ce qui contredirait la supposition ; donc $\eta\rho$ n'est pas divisible par $\mathfrak{p}$. C. Q. F. D.

De là il s'ensuit immédiatement que tous les nombres *rationnels* divisibles par un idéal premier $\mathfrak{p}$, et auxquels appartient aussi $N(\mathfrak{p})$ (§ 20), forment un module $[p]$, p étant un *nombre premier* rationnel positif complétement déterminé ; car le *plus petit* nombre rationnel positif p, divisible par $\mathfrak{p}$, ne peut en aucune façon être un nombre composé ab, puisque alors l'un des deux nombres moindres a, b serait pareillement divisible par $\mathfrak{p}$; et comme p ne peut non plus être $= 1$, puisqu'on aurait alors $\mathfrak{p} = \mathfrak{o}$ (§ 19), p devra être un nombre premier ; et tout nombre rationnel entier m divisible par $\mathfrak{p}$ devra être divisible par p, ce qui devient immédiatement évident, en mettant m sous la forme $pq + r$, puisque le reste $r = m - pq$ est aussi divisible par $\mathfrak{p}$. Maintenant $\mathfrak{o}p$ étant divisible par $\mathfrak{p}$, et par suite $N(\mathfrak{o}p) = p^n$ divisible par $N(\mathfrak{p})$ (§ 20), $N(\mathfrak{p}) = p^f$ sera une puissance de p, et l'exposant f sera dit le *degré de l'idéal premier* $\mathfrak{p}$.

4° Si l'idéal $\mathfrak{a}$ est divisible par l'idéal premier $\mathfrak{p}$, il existera un nombre η tel que $\eta\mathfrak{p}$ soit le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$.

Ce théorème important est évident, si l'on a $\mathfrak{a} = \mathfrak{p}$, puisque tout nombre η non divisible par $\mathfrak{p}$, par exemple, le nombre $\eta = 1$, satisfait à la condition indiquée. Mais si $\mathfrak{a}$ est différent de $\mathfrak{p}$, nous nous bornerons d'abord à démontrer l'existence d'un nombre η tel que le diviseur $\mathfrak{r}$ de l'idéal $\mathfrak{a}$, correspondant à η, soit en même temp

divisible par $\mathfrak{p}$, mais ait une norme *moindre* que celle de $\mathfrak{a}$. Puisque l'on a $N(\mathfrak{a}) = N(\mathfrak{r})\,N(\mathfrak{b})$, $\mathfrak{b}$ étant le plus grand commun diviseur de $\mathfrak{a}$ et de $\mathfrak{o}\eta$ (§ 20), la dernière condition revient à choisir η de manière que $N(\mathfrak{b})$ soit > 1, et par suite $\mathfrak{b}$ différent de $\mathfrak{o}$. Pour atteindre ce but, et faire en même temps que $\mathfrak{r}$ soit divisible par $\mathfrak{p}$, nous distinguerons deux cas :

Premièrement, si tous les idéaux (à l'exception de $\mathfrak{o}$) qui divisent $\mathfrak{a}$ sont divisibles par $\mathfrak{p}$, on choisira pour η un nombre divisible par $\mathfrak{p}$, mais non divisible par $\mathfrak{a}$, ce qui est toujours possible, puisque $\mathfrak{p}$ n'est pas divisible par $\mathfrak{a}$; alors il est clair que $\mathfrak{b}$ sera divisible par $\mathfrak{p}$, et par suite différent de $\mathfrak{o}$; comme, de plus, η n'est pas divisible par $\mathfrak{a}$, mais que $\eta\mathfrak{r}$ est divisible par $\mathfrak{a}$, $\mathfrak{r}$ sera pareillement différent de $\mathfrak{o}$, et par suite divisible par $\mathfrak{p}$.

Deuxièmement, s'il existe un idéal $\mathfrak{e}$ divisant $\mathfrak{a}$, et qui soit différent de $\mathfrak{o}$ et non divisible par $\mathfrak{p}$, choisissons pour η un nombre divisible par $\mathfrak{e}$, mais non divisible par $\mathfrak{p}$; alors $\mathfrak{b}$ sera divisible par $\mathfrak{e}$, et partant encore différent de $\mathfrak{o}$; comme, de plus, $\eta\mathfrak{r}$ est divisible par $\mathfrak{a}$ et par suite aussi par $\mathfrak{p}$, $\mathfrak{r}$ sera aussi divisible par $\mathfrak{p}$, puisque η n'est pas divisible par $\mathfrak{p}$ (d'après 1°).

Après avoir établi ainsi pour les deux cas l'existence au moins d'un nombre η ayant la propriété demandée, on reconnaît sans peine que l'on a certainement $\mathfrak{r} = \mathfrak{p}$, si l'on choisit, en outre, η de manière que $N(\mathfrak{r})$ soit *aussi petit que possible;* car, si l'idéal $\mathfrak{r}$, divisible par $\mathfrak{p}$, n'est pas $= \mathfrak{p}$, on peut procéder avec $\mathfrak{r}$ comme on vient de le faire avec $\mathfrak{a}$, et choisir un nombre η' de manière que le diviseur $\mathfrak{r}'$ de $\mathfrak{r}$, correspondant à ce nombre, ait une norme encore moindre que celle de $\mathfrak{r}$, et soit pareillement divisible par $\mathfrak{p}$; mais comme (§ 19) $\mathfrak{r}'$ est en même temps le diviseur de $\mathfrak{a}$ correspondant au nombre $\eta\eta'$, cela est en contradiction avec la supposition qu'on vient de faire sur η et sur $\mathfrak{r}$. Donc $\mathfrak{r} = \mathfrak{p}$, c'est-à-dire que $\eta\mathfrak{p}$ est le plus petit multiple commun de $\mathfrak{a}$ et de $\mathfrak{o}\eta$. C. Q. F. D.

§ 22. — *Multiplication des idéaux.*

Si α parcourt tous les nombres d'un idéal $\mathfrak{a}$, et de même 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 $\mathfrak{c}$; car tous ces nombres sont contenus dans $\mathfrak{o}$; de plus, ils se reproduisent par addition,

et aussi par soustraction, puisque les nombres $(-\alpha)$ sont également contenus dans $\mathfrak{a}$; et enfin tout produit d'un nombre $\Sigma\alpha\beta$ du système $\mathfrak{c}$ et d'un nombre ω du domaine $\mathfrak{o}$ appartient également au système $\mathfrak{c}$, puisque tout produit $\alpha\omega$ est encore contenu dans $\mathfrak{a}$. Cet idéal $\mathfrak{c}$ sera dit le *produit* des deux *facteurs* $\mathfrak{a}$, $\mathfrak{b}$, et nous le désignerons par $\mathfrak{ab}$.

De cette définition il s'ensuit immédiatement que l'on a $\mathfrak{oa} = \mathfrak{a}$, $\mathfrak{ab} = \mathfrak{ba}$, et, si $\mathfrak{c}$ est un troisième idéal quelconque, $(\mathfrak{ab})\,\mathfrak{c} = \mathfrak{a}\,(\mathfrak{bc})$, et l'on en conclut par le raisonnement connu (1) que, dans la formation d'un produit d'un nombre quelconque d'idéaux $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$, l'ordre des multiplications successives, par lesquelles on réunit chaque fois *deux* idéaux en un seul produit, n'a aucune influence sur le résultat final, lequel peut être désigné, pour abréger, par $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_m$, et se compose évidemment de tous les nombres de la forme $\Sigma\alpha_1\alpha_2 \ldots \alpha_m$, en désignant par $\alpha_1, \alpha_2, \ldots, \alpha_m$ des nombres quelconques des facteurs $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$. Si tous les m facteurs sont $= \mathfrak{a}$, leur produit sera dit la $m^{\text{ième}}$ *puissance* de $\mathfrak{a}$, et on le représentera par $\mathfrak{a}^m$; en posant, de plus, $\mathfrak{a}^0 = \mathfrak{o}$, $\mathfrak{a}^1 = \mathfrak{a}$, on aura en général $\mathfrak{a}^r\mathfrak{a}^s = \mathfrak{a}^{r+s}$, $(\mathfrak{a}^r)^s = \mathfrak{a}^{rs}$. En outre, on aura évidemment $\mathfrak{a}(\mathfrak{o}\eta) = \mathfrak{a}\eta$ et $(\mathfrak{o}\eta)(\mathfrak{o}\eta') = \mathfrak{o}\eta\eta'$. Enfin nous établirons encore les théorèmes suivants :

1° Le produit $\mathfrak{ab}$ est divisible par les facteurs $\mathfrak{a}$ et $\mathfrak{b}$; car (en vertu de la propriété II) tout produit $\alpha\omega$, par suite aussi tout produit $\alpha\beta$, et conséquemment (d'après 1) toute somme de semblables produits sont contenus dans $\mathfrak{a}$, c'est-à-dire que $\mathfrak{ab}$ est divisible par $\mathfrak{a}$.

2° Si $\mathfrak{a}$ est divisible par $\mathfrak{a}'$, et $\mathfrak{b}$ divisible par $\mathfrak{b}'$, $\mathfrak{ab}$ sera divisible par $\mathfrak{a}'\mathfrak{b}'$. Car tous les nombres $\Sigma\alpha\beta$ contenus dans $\mathfrak{ab}$ sont contenus dans $\mathfrak{a}'\mathfrak{b}'$, puisque α est contenu dans $\mathfrak{a}$ et par suite dans $\mathfrak{a}'$, et que β est contenu dans $\mathfrak{b}$ et par suite dans $\mathfrak{b}'$.

3° Si aucun des idéaux $\mathfrak{a}$, $\mathfrak{b}$ n'est divisible par l'idéal premier $\mathfrak{p}$, le produit $\mathfrak{ab}$ ne sera pas non plus divisible par $\mathfrak{p}$; car il existe dans $\mathfrak{a}$, $\mathfrak{b}$ respectivement des nombres α, β qui ne sont pas divisibles par $\mathfrak{p}$, et par suite le nombre $\alpha\beta$ contenu dans $\mathfrak{ab}$ n'est pas non plus divisible par $\mathfrak{p}$ (§ 21, 3°).

---

(1) Voir le § 2 des *Vorlesungen über Zahlentheorie* de Dirichlet.

§ 23. — *La difficulté de la théorie.*

Il serait aisé d'augmenter considérablement le nombre de ces théorèmes, qui se rapportent à la dépendance entre les deux notions de la *divisibilité* et de la *multiplication* des idéaux, et nous énoncerons encore sans démonstration les propositions suivantes, uniquement pour faire ressortir la ressemblance avec les propositions correspondantes de la théorie des nombres rationnels :

Si $\mathfrak{a}$, $\mathfrak{b}$ sont des idéaux *premiers entre eux,* c'est-à-dire tels que leur plus grand commun diviseur soit $= \mathfrak{o}$, leur plus petit commun multiple sera $= \mathfrak{ab}$, et l'on aura en même temps

$$N(\mathfrak{ab}) = N(\mathfrak{a})\,N(\mathfrak{b}).$$

Si $\mathfrak{p}$ est un idéal premier, $\mathfrak{a}$ un idéal quelconque, alors ou $\mathfrak{a}$ sera divisible par $\mathfrak{p}$, ou $\mathfrak{a}$ et $\mathfrak{p}$ seront des idéaux premiers entre eux.

Si $\mathfrak{a}$ est un idéal premier avec $\mathfrak{b}$ et avec $\mathfrak{c}$, $\mathfrak{a}$ sera aussi premier avec $\mathfrak{bc}$.

Si $\mathfrak{ab}$ est divisible par $\mathfrak{c}$, et que $\mathfrak{a}$ soit premier avec $\mathfrak{c}$, $\mathfrak{b}$ sera divisible par $\mathfrak{c}$.

Mais toutes ces propositions ne suffisent pas pour rendre complète l'analogie avec la théorie des nombres rationnels. Il ne faut pas oublier que la divisibilité d'un idéal $\mathfrak{c}$ par un idéal $\mathfrak{a}$, suivant notre définition (§ 19), consiste seulement en ce que tous les nombres de l'idéal $\mathfrak{c}$ sont contenus aussi dans $\mathfrak{a}$; or on a vu très-facilement (§ 22, 1°) que tout produit de $\mathfrak{a}$ par un idéal quelconque $\mathfrak{b}$ est divisible par $\mathfrak{a}$, mais il n'est nullement aisé de démontrer la réciproque, savoir, que tout idéal divisible par $\mathfrak{a}$ est aussi un produit de $\mathfrak{a}$ par un idéal $\mathfrak{b}$. Cette difficulté, la plus grande et, à proprement parler, la seule que présente la théorie, ne peut en aucune manière être surmontée à l'aide des seuls moyens de démonstration que nous avons employés jusqu'ici, et il faut que nous examinions ici d'un peu plus près la raison de ce phénomène, parce que celui-ci se rattache à une généralisation très-importante de la théorie. En considérant avec attention la théorie développée jusqu'à présent, on reconnaîtra que toutes les définitions conservent un sens déterminé, et que les démonstrations de tous les théorèmes ont encore toute leur force,

lors même que l'on ne *suppose plus* que le domaine désigné par $\mathfrak{o}$ comprenne *tous* les nombres entiers du corps Ω. Les propriétés du système $\mathfrak{o}$ sur lesquelles on s'est appuyé se réduisent en réalité aux suivantes :

(a) Le système $\mathfrak{o}$ est un module fini $[\omega_1, \omega_2, \ldots, \omega_n]$, dont la base forme en même temps une base du corps Ω.

(b) Le nombre 1, et par suite aussi tous les nombres rationnels entiers sont contenus dans $\mathfrak{o}$.

(c) Tout produit de deux nombres du système $\mathfrak{o}$ appartient au même système $\mathfrak{o}$.

Quand un domaine $\mathfrak{o}$ jouira de ces trois propriétés, nous l'appellerons un *ordre*. De l'ensemble de (a) et de (c) il résulte immédiatement qu'un ordre se compose seulement de nombres *entiers* du corps Ω, mais ne contient pas nécessairement *tous* ces nombres entiers (excepté dans le cas $n = 1$). Si maintenant un nombre α de l'ordre $\mathfrak{o}$ est appelé *divisible* par un second nombre semblable μ dans le cas seulement où l'on a $\alpha = \mu\omega$, ω désignant également un nombre contenu dans $\mathfrak{o}$, et si l'on modifie de la même manière la notion de la *congruence* des nombres dans l'étendue du domaine $\mathfrak{o}$, on voit immédiatement que le nombre $(\mathfrak{o}, \mathfrak{o}\mu)$ des nombres du domaine $\mathfrak{o}$ incongrus par rapport à μ est encore maintenant $= \pm N(\mu)$ (§ 18), et il est tout aussi facile de reconnaître que toutes les définitions et tous les théorèmes de la présente Section conserveront leur signification et leur vérité, si l'on entend toujours par *nombre* un nombre de cet ordre $\mathfrak{o}$. Dans tout ordre $\mathfrak{o}$ du corps Ω il existe donc une théorie particulière des idéaux, et cette théorie est la même pour tous les ordres (qui sont en nombre infini), jusqu'au point où elle a été développée dans ce qui précède. Mais, tandis que la théorie des idéaux, dans l'ordre $\mathfrak{o}$ qui comprend *tous* les nombres entiers du corps Ω, conduit finalement à des lois générales qui ne souffrent aucune exception et qui coïncident complétement avec les lois de la divisibilité des nombres rationnels, la théorie des idéaux de chacun des autres ordres est sujette à certaines exceptions, ou plutôt elle exige une certaine restriction de la notion d'idéal. Mais cette théorie générale des idéaux d'un ordre quelconque, dont le développement est également indispensable pour les besoins de la théorie des nombres, et qui, dans le cas $n = 2$, coïncide avec la

théorie des divers *ordres* des *formes* quadratiques binaires (¹), nous la laisserons entièrement de côté dans ce qui va suivre (²), et je me contenterai ici de donner un exemple pour appeler l'attention sur le caractère des exceptions dont nous venons de parler. Dans le corps quadratique, résultant d'une racine

$$\theta = \frac{-1+\sqrt{-3}}{2}$$

de l'équation $\theta^2 + \theta + 1 = 0$, le module $[1, \sqrt{-3}]$ forme un ordre $\mathfrak{o}$ qui ne comprend pas tous les nombres entiers de ce corps. Les modules $[2, 1+\sqrt{-3}] = \mathfrak{p}$ et $[2, 2\sqrt{-3}] = \mathfrak{o}(2)$ devraient être considérés comme des idéaux de cet ordre $\mathfrak{o}$, en tant qu'ils jouissent des propriétés I et II (§ 19); mais, quoique $\mathfrak{o}(2)$ soit divisible par $\mathfrak{p}$, il n'existe toutefois dans $\mathfrak{o}$ aucun idéal $\mathfrak{q}$ tel que l'on ait $\mathfrak{p}\mathfrak{q} = \mathfrak{o}(2)$.

§ 21. — *Propositions auxiliaires.*

Pour achever maintenant complétement la théorie des idéaux de celui des ordres $\mathfrak{o}$ qui comprend *tous* les nombres entiers du corps Ω, nous avons besoin des lemmes suivants, qui ne sont vrais sans restriction que pour un tel domaine $\mathfrak{o}$.

1° Soient ω, μ, ν trois nombres de $\mathfrak{o}$, différents de zéro, et tels que ν ne soit pas divisible par μ; les termes de la progression géométrique

$$\omega, \quad \omega\frac{\nu}{\mu}, \quad \omega\left(\frac{\nu}{\mu}\right)^2, \quad \omega\left(\frac{\nu}{\mu}\right)^3, \quad \ldots,$$

jusqu'à un terme

$$\omega\left(\frac{\nu}{\mu}\right)^e,$$

situé à une distance finie, seront tous contenus dans $\mathfrak{o}$, et aucun des termes suivants ne sera un nombre entier.

En effet, si le nombre des termes qui sont des nombres entiers

---

(¹) *Disquisitiones arithmeticæ*, art. 226.

(²) Je traite cette theorie en détail dans le Mémoire récemment publié : « *Ueber die Anzahl der Ideal-Classen in den verschiedenen Ordnungen eines endlichen Körpers.* » (*Festschrift zur Säcularfeier des Geburtstages von C.-F. Gauss.* Braunschweig, 30. April 1877).

était plus grand que la valeur absolue k de $N(\omega)$, il faudrait (§ 18) que, sur $k+1$ de ces termes, il y en eût au moins deux différents qui correspondissent à des exposants s et $r > s$, et qui fussent congrus entre eux suivant le module ω; or d'une telle congruence

$$\omega\left(\frac{\nu}{\mu}\right)^r \equiv \omega\left(\frac{\nu}{\mu}\right)^s \pmod{\omega}$$

il résulterait que le nombre

$$\eta = \frac{\nu}{\mu},$$

appartenant au corps Ω, satisferait à une équation du $r^{\text{ième}}$ degré de la forme

$$\eta^r = \eta^s + \omega',$$

ω' étant un nombre entier, et par suite (§ 13, 2°) serait lui-même un nombre entier, ce qui est contraire à notre hypothèse, que ν n'est pas divisible par μ. Donc k termes au plus de la série précédente peuvent être des nombres entiers, et par suite être contenus dans $\mathfrak{o}$. Si, de plus, le terme

$$\rho = \omega\left(\frac{\nu}{\mu}\right)^r,$$

r étant $\geqq 1$, est un nombre entier, et que s soit un quelconque des r exposants $0, 1, 2, \ldots, r-1$, le terme

$$\sigma = \omega\left(\frac{\nu}{\mu}\right)$$

sera aussi un nombre entier, puisque

$$\sigma^r = \omega^{r-s}\,\rho^s$$

est un nombre entier (§ 13, 2°). Ainsi la proposition se trouve complétement démontrée.

2° Soient μ, ν deux nombres de $\mathfrak{o}$, différents de zéro, ν n'étant pas divisible par μ; il existe toujours dans $\mathfrak{o}$ deux nombres $\varkappa$, λ, différents de zéro, et tels que l'on ait

$$\frac{\varkappa}{\lambda} = \frac{\nu}{\mu},$$

et que $\varkappa^2$ ne soit pas divisible par λ.

Car si

$$\lambda = \mu \left(\frac{\nu}{\mu}\right)^{e-1}, \quad \varkappa = \mu \left(\frac{\nu}{\mu}\right)^{e}$$

sont les deux derniers termes de la série

$$\mu, \quad \mu \left(\frac{\nu}{\mu}\right), \quad \mu \left(\frac{\nu}{\mu}\right)^{2}, \quad \mu \left(\frac{\nu}{\mu}\right)^{3}, \quad \ldots$$

qui soient des nombres entiers et par suite contenus dans $\mathfrak{o}$, on aura évidemment $e \geqq 1$, et

$$\frac{\varkappa}{\lambda} = \frac{\nu}{\mu}, \quad \frac{\varkappa^2}{\lambda} = \mu \left(\frac{\nu}{\mu}\right)^{e+1};$$

donc $\varkappa^2$ n'est pas divisible par λ. C. Q. F. D.

§ 25. — *Lois de la divisibilité.*

A l'aide de ces lemmes, il est facile d'apporter à la théorie des idéaux du domaine $\mathfrak{o}$ le complément désiré, qui se trouve contenu dans les lois suivantes:

1° Si $\mathfrak{p}$ est un idéal premier, il existe un nombre λ divisible par $\mathfrak{p}$, et un nombre $\varkappa$ non divisible par $\mathfrak{p}$, tels que $\varkappa\mathfrak{p}$ soit le plus petit commun multiple de $\mathfrak{o}\lambda$ et $\mathfrak{o}\varkappa$.

Démonstration. — Soit μ un nombre quelconque, mais autre que zéro, de l'idéal premier $\mathfrak{p}$; $\mathfrak{o}\mu$ étant divisible par $\mathfrak{p}$, il existera un nombre ν tel que $\nu\mathfrak{p}$ soit le plus petit commun multiple de $\mathfrak{o}$ et $\mathfrak{o}\nu$ (§ 21, 4°). Ce nombre ν ne peut pas être divisible par μ; car autrement le plus petit commun multiple de $\mathfrak{o}\mu$ et de $\mathfrak{o}\nu$ serait $= \mathfrak{o}\nu$, et non $= \mathfrak{p}\nu$. Si l'on choisit maintenant (§ 24, 2°) les deux nombres $\varkappa$, λ de telle manière que l'on ait $\varkappa\mu = \lambda\nu$, et que $\varkappa^2$ ne soit pas divisible par λ, alors (§ 19) l'idéal $\varkappa\nu\mathfrak{p}$ sera le plus petit commun multiple de $\varkappa(\mathfrak{o}\mu) = \mathfrak{o}\lambda\nu$ et de $\mathfrak{o}\varkappa\nu$, d'où il s'ensuit (§ 19) que $\varkappa\mathfrak{p}$ est le plus petit commun multiple de $\mathfrak{o}\lambda$ et $\mathfrak{o}\varkappa$; donc $\mathfrak{p}$ est le diviseur correspondant au nombre $\varkappa$ de l'idéal principal $\mathfrak{o}\lambda$; mais $\varkappa$ n'est pas divisible par $\mathfrak{p}$, puisque, s'il l'était, $\varkappa^2$ serait divisible par $\varkappa\mathfrak{p}$ et par suite aussi par λ.

2° Tout idéal premier $\mathfrak{p}$ peut, au moyen de la multiplication par un idéal $\mathfrak{b}$, être changé en un idéal principal.

Démonstration. — Conservons à $\varkappa$ et λ la même signification que plus haut, et soit $\mathfrak{b}$ le plus grand commun diviseur de $\mathfrak{o}\lambda$ et $\mathfrak{o}\varkappa$; nous allons démontrer que l'on a $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$. En effet, tous les nombres de l'idéal $\mathfrak{b}$ étant de la forme $\delta = \varkappa\omega + \lambda\omega'$, où ω, ω' sont deux nombres de $\mathfrak{o}$, alors, si ϖ est un nombre quelconque de $\mathfrak{p}$, on aura $\varpi\delta = \varkappa\varpi\omega + \lambda\varpi\omega' \equiv 0 \pmod{\lambda}$, puisque $\varkappa\mathfrak{p}$ et par suite aussi $\varkappa\varpi$ sont divisibles par $\mathfrak{o}\lambda$; donc $\mathfrak{p}\mathfrak{b}$ est divisible par $\mathfrak{o}\lambda$. Réciproquement, $\varkappa$ n'étant pas divisible par $\mathfrak{p}$, et partant $\mathfrak{o}$ étant le plus grand commun diviseur de $\mathfrak{o}\varkappa$ et $\mathfrak{p}$, on peut poser le nombre 1, contenu dans $\mathfrak{o}$, $= \varkappa\omega + \varpi$, ω étant contenu dans $\mathfrak{o}$ et ϖ dans $\mathfrak{p}$; on aura donc $\lambda = \lambda.\varkappa\omega + \varpi.\lambda \equiv 0 \pmod{\mathfrak{p}\mathfrak{b}}$, puisque les premiers facteurs λ, ϖ sont contenus dans $\mathfrak{p}$, et les seconds facteurs $\varkappa\omega$, λ contenus dans $\mathfrak{b}$. Ainsi chacun des deux idéaux $\mathfrak{p}\mathfrak{b}$ et $\mathfrak{o}\lambda$ est divisible par l'autre, et par suite $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$. C. Q. F. D.

3° Si l'idéal $\mathfrak{a}$ est divisible par l'idéal premier $\mathfrak{p}$, il existera un idéal $\mathfrak{a}'$, et un seul, tel que l'on aura $\mathfrak{p}\mathfrak{a}' = \mathfrak{a}$, et en même temps on aura $N(\mathfrak{a}') < N(\mathfrak{a})$.

Démonstration. — Soit, comme tout à l'heure, $\mathfrak{p}\mathfrak{b} = \mathfrak{o}\lambda$; $\mathfrak{a}$ étant divisible par $\mathfrak{p}$, et par suite $\mathfrak{a}\mathfrak{b}$ par $\mathfrak{p}\mathfrak{b}$ (§ 22, 2°), on aura $\mathfrak{a}\mathfrak{b} = \lambda\mathfrak{a}'$, $\mathfrak{a}'$ représentant un idéal (§ 19); en multipliant par $\mathfrak{p}$, on tire de là $\lambda\mathfrak{a} = \lambda\mathfrak{p}\mathfrak{a}'$, et par conséquent aussi $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$. Soit maintenant $\mathfrak{b}$ un idéal, satisfaisant également à la condition $\mathfrak{p}\mathfrak{b} = \mathfrak{a}$; de l'égalité $\mathfrak{p}\mathfrak{b} = \mathfrak{p}\mathfrak{a}'$ il résulte, en multipliant par $\mathfrak{b}$, que l'on devra avoir $\lambda\mathfrak{b} = \lambda\mathfrak{a}'$, d'où $\mathfrak{b} = \mathfrak{a}'$. Il existe en outre (§ 21, 4°) un nombre η tel que $\eta\mathfrak{p}$ est le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$; or, $\eta\mathfrak{p}$ étant divisible par $\mathfrak{a} = \mathfrak{a}'\mathfrak{p}$, il s'ensuit, en multipliant par $\mathfrak{b}$, que $\mathfrak{o}\eta\lambda$ est divisible par $\lambda\mathfrak{a}'$, et par suite η par $\mathfrak{a}'$; mais η n'est certainement pas divisible par $\mathfrak{a}$, car autrement ce serait $\mathfrak{o}\eta$, et non $\eta\mathfrak{p}$, qui serait le plus petit commun multiple de $\mathfrak{a}$ et $\mathfrak{o}\eta$. Donc, η étant divisible par $\mathfrak{a}'$, mais non divisible par $\mathfrak{a}$, il faut que $\mathfrak{a}'$ soit *différent* de $\mathfrak{a}$, et par suite que l'on ait $N(\mathfrak{a}') < N(\mathfrak{a})$, puisque $\mathfrak{a}'$ est un diviseur de $\mathfrak{a}$.

C. Q. F. D.

4° Tout idéal $\mathfrak{a}$ différent de $\mathfrak{o}$ est lui-même un idéal premier, ou bien il peut se mettre sous la forme d'un produit d'idéaux tous premiers, et cela d'une seule manière.

Démonstration. — Puisque $\mathfrak{a}$ est différent de $\mathfrak{o}$, il existe (§ 21, 1°) un idéal premier $\mathfrak{p}_1$ divisant $\mathfrak{a}$, et par suite on peut poser (d'après 3°) $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, où $N(\mathfrak{a}_1) < N(\mathfrak{a})$. Si l'on a $\mathfrak{a}_1 = \mathfrak{o}$, alors $\mathfrak{a} = \mathfrak{p}_1$ sera un idéal premier; mais si $N(\mathfrak{a}_1)$ est > 1, et partant $\mathfrak{a}_1$ différent de $\mathfrak{o}$, on pourra de même poser $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$, $\mathfrak{p}_2$ étant un idéal premier, et $N(\mathfrak{a}_2) < N(\mathfrak{a}_1)$. Si $N(\mathfrak{a}_2)$ est > 1, on pourra continuer de la même manière, jusqu'à ce que, parmi les idéaux $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$, dont les normes sont de plus en plus petites, se présente l'idéal $\mathfrak{o} = \mathfrak{a}_m$, ce qui doit arriver après un nombre fini de décompositions. On aura alors

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_m,$$

mis sous la forme d'un produit de m idéaux premiers. Si maintenant on a en même temps

$$\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_r,$$

$\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ désignant également des idéaux premiers, $\mathfrak{q}_1$ sera un diviseur du produit $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_m$, et par suite (§ 22, 3°) l'un au moins des facteurs, $\mathfrak{p}_1$ par exemple, devra être divisible par $\mathfrak{q}_1$, et comme $\mathfrak{p}_1$ n'est divisible que par les deux idéaux $\mathfrak{o}$ et $\mathfrak{p}_1$, il faudra que l'on ait $\mathfrak{q}_1 = \mathfrak{p}_1$, puisque $\mathfrak{q}_1$ est différent de $\mathfrak{o}$. On aura donc

$$\mathfrak{p}_1(\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_m) = \mathfrak{p}_1(\mathfrak{q}_2\mathfrak{q}_3 \ldots \mathfrak{q}_r),$$

d'où (d'après 3°)

$$\mathfrak{p}_2\mathfrak{p}_3 \ldots \mathfrak{p}_m = \mathfrak{q}_2\mathfrak{q}_3 \ldots \mathfrak{q}_r.$$

On pourra continuer de la même manière, absolument comme dans la théorie des nombres rationnels (1), et l'on arrivera ainsi à ce résultat, que tout idéal premier entrant comme facteur dans l'un des produits entrera exactement le même nombre de fois comme facteur dans l'autre produit. C. Q. F. D.

5° Tout idéal $\mathfrak{a}$ peut, au moyen de la multiplication par un idéal $\mathfrak{m}$, être changé en un idéal principal.

Démonstration. — Soit, en effet, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_m$; on pourra (d'après 2°), en multipliant les idéaux premiers $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m$ par

(1) Voir les *Vorlesungen über Zahlentheorie* de Dirichlet, § 8.

les idéaux correspondants $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_m$, les changer en idéaux principaux $\mathfrak{p}_1\mathfrak{b}_1, \mathfrak{p}_2\mathfrak{b}_2, \ldots, \mathfrak{p}_m\mathfrak{b}_m$. Si l'on pose maintenant

$$\mathfrak{m} = \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_m,$$

alors $\mathfrak{a}\mathfrak{m} = (\mathfrak{p}_1\mathfrak{b}_1)(\mathfrak{p}_2\mathfrak{b}_2)\ldots(\mathfrak{p}_m\mathfrak{b}_m)$ sera un produit uniquement d'idéaux principaux, et par suite sera lui-même un idéal principal.

C. Q. F. D.

6° Si l'idéal $\mathfrak{c}$ est divisible par l'idéal $\mathfrak{a}$, il existera un idéal $\mathfrak{b}$, et un seul, satisfaisant à la condition $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. — Si le produit $\mathfrak{a}\mathfrak{b}$ est divisible par le produit $\mathfrak{a}\mathfrak{b}'$, $\mathfrak{b}$ sera divisible par $\mathfrak{b}'$; et de $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ il s'ensuivra $\mathfrak{b} = \mathfrak{b}'$.

Démonstration. — Choisissons l'idéal $\mathfrak{m}$ de telle sorte que $\mathfrak{a}\mathfrak{m}$ soit un idéal principal $\mathfrak{o}\mu$; si maintenant $\mathfrak{c}$ est divisible par $\mathfrak{a}$, et par suite $\mathfrak{c}\mathfrak{m}$ divisible par $\mathfrak{a}\mathfrak{m}$ (§ 22, 2°), on pourra (§ 19) poser $\mathfrak{c}\mathfrak{m} = \mu\mathfrak{b}$, $\mathfrak{b}$ étant un idéal. En multipliant par $\mathfrak{a}$, il vient $\mu\mathfrak{c} = \mu\mathfrak{a}\mathfrak{b}$, d'où $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. — Soient ensuite $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{b}'$ des idéaux quelconques, et supposons $\mathfrak{a}\mathfrak{b}$ divisible par $\mathfrak{a}\mathfrak{b}'$; il en résultera encore, en multipliant par $\mathfrak{m}$ (§ 22, 2°), que $\mu\mathfrak{b}$ est divisible par $\mu\mathfrak{b}'$, et partant (§ 19) $\mathfrak{b}$ divisible par $\mathfrak{b}'$. Si, de plus, on a $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$, chacun des deux idéaux $\mathfrak{b}$, $\mathfrak{b}'$ devra être divisible par l'autre, c'est-à-dire qu'on aura $\mathfrak{b} = \mathfrak{b}'$. C. Q. F. D.

7° La norme d'un produit d'idéaux est égale au produit des normes des facteurs; $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$.

Démonstration. — Considérons d'abord le cas d'un produit $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$, dont un facteur $\mathfrak{p}$ est un idéal premier. Comme $\mathfrak{a}$ est divisible par $\mathfrak{p}$, il existera (d'après 3°) un nombre η divisible par $\mathfrak{a}'$, mais non par $\mathfrak{a}$, et $\eta\mathfrak{p}$ sera le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$; donc on aura (§ 20) $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{p})\,\mathrm{N}(\mathfrak{d})$, $\mathfrak{d}$ étant le plus grand commun diviseur des mêmes idéaux $\mathfrak{a}$ et $\mathfrak{o}\eta$. Comme $\mathfrak{a}$ et $\mathfrak{o}\eta$ sont divisibles par $\mathfrak{a}'$, $\mathfrak{d}$ devra être aussi divisible par $\mathfrak{a}'$ (§ 1, 4°) et par suite il existe (d'après 6°) un idéal $\mathfrak{n}$ satisfaisant à la condition $\mathfrak{n}\mathfrak{a}' = \mathfrak{d}$. De plus, $\mathfrak{a}$ étant divisible par $\mathfrak{d}$, et conséquemment $\mathfrak{p}\mathfrak{a}'$ par $\mathfrak{n}\mathfrak{a}'$, l'idéal premier $\mathfrak{p}$ devra (d'après 6°) être divisible par $\mathfrak{n}$, et l'on devra, par suite, avoir $\mathfrak{n} = \mathfrak{p}$ ou $= \mathfrak{o}$. La première égalité est impossible, sans quoi l'on aurait $\mathfrak{d} = \mathfrak{p}\mathfrak{a}' = \mathfrak{a}$, et par suite η serait divisible par $\mathfrak{a}$, ce qui n'a pas lieu; on aura donc $\mathfrak{n} = \mathfrak{o}$, d'où $\mathfrak{d} = \mathfrak{a}'$, et aussi $\mathrm{N}(\mathfrak{p}\mathfrak{a}') = \mathrm{N}(\mathfrak{p})\,\mathrm{N}(\mathfrak{a}')$, ce qui démontre le théorème pour le

cas considéré. Mais on en conclut immédiatement le théorème général. Car tout idéal (autre que 0) étant (d'après 4°) de la forme

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m,$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ sont des idéaux premiers, il en résulte

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)\, N(\mathfrak{p}_2 \mathfrak{p}_3 \dots \mathfrak{p}_m) = N(\mathfrak{p}_1)\, N(\mathfrak{p}_2)\, N(\mathfrak{p}_3 \dots \mathfrak{p}_m) = \dots,$$

et par suite aussi

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)\, N(\mathfrak{p}_2) \dots N(\mathfrak{p}_m);$$

si l'on a de plus

$$\mathfrak{b} = \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_r,$$

$\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r$ désignant encore des idéaux premiers, il viendra

$$\mathfrak{a}\mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_r,$$

et par conséquent

$$N(\mathfrak{b}) = N(\mathfrak{q}_1)\, N(\mathfrak{q}_2) \dots N(\mathfrak{q}_r),$$
$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{p}_1) \dots N(\mathfrak{p}_m)\, N(\mathfrak{q}_1) \dots N(\mathfrak{q}_r);$$

on a donc bien

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\, N(\mathfrak{b}). \qquad \text{C. Q. F. D.}$$

8° Un idéal $\mathfrak{a}$ (ou un nombre α) est toujours, et seulement alors, divisible par un idéal $\mathfrak{b}$ (ou un nombre δ), quand toutes les puissances d'idéaux premiers qui divisent $\mathfrak{b}$ (ou δ) divisent aussi $\mathfrak{a}$ (ou α).

Démonstration. — Si $\mathfrak{p}$ est un idéal premier, et $\mathfrak{p}^m$ un diviseur d'un idéal $\mathfrak{b}$, on a (d'après 6°) $\mathfrak{b} = \mathfrak{b}_1 \mathfrak{p}^m$, $\mathfrak{b}_1$ désignant un idéal ; si l'on suppose ce dernier décomposé en ses facteurs tous premiers, $\mathfrak{b}$ se trouvera aussi sous la forme d'un produit d'idéaux tous premiers, et parmi ceux-ci le facteur $\mathfrak{p}$ entre au moins m fois ; réciproquement, si, dans la décomposition de $\mathfrak{b}$ en facteurs premiers, l'idéal premier $\mathfrak{p}$ entre au moins m fois comme facteur, $\mathfrak{b}$ sera évidemment divisible par $\mathfrak{p}^m$. Si donc on suppose que toute puissance d'idéal premier qui divise $\mathfrak{b}$ divise aussi un idéal $\mathfrak{a}$, cela revient à dire que tous les facteurs premiers qui entrent dans la décomposition de $\mathfrak{b}$

entrent tous aussi, au moins autant de fois, comme facteurs dans la décomposition de $\mathfrak{a}$; parmi les facteurs de $\mathfrak{a}$ se trouvent donc d'abord tous les facteurs de $\mathfrak{b}$, et, si l'on désigne le produit des autres facteurs de $\mathfrak{a}$ par $\mathfrak{b}'$, on aura $\mathfrak{a} = \mathfrak{b}\mathfrak{b}'$, et par suite $\mathfrak{a}$ est divisible par $\mathfrak{b}$. La proposition réciproque, que, si $\mathfrak{b}$ est un diviseur de $\mathfrak{a}$, toute puissance d'idéal premier qui divise $\mathfrak{b}$ divise aussi $\mathfrak{a}$, se vérifie d'elle-même. C. Q. F D.

Si l'on réunit sous forme de puissance tous les facteurs premiers d'un idéal $\mathfrak{a}$ qui sont égaux entre eux, on trouve

$$\mathfrak{a} = \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c \ldots,$$

$\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, ... étant tous des idéaux premiers différents entre eux, et en vertu des théorèmes que nous venons de démontrer, tous les diviseurs $\mathfrak{b}$ de $\mathfrak{a}$ sont compris dans la formule

$$\mathfrak{b} = \mathfrak{p}^{a'} \mathfrak{q}^{b'} \mathfrak{r}^{c'} \ldots,$$

où les exposants a', b', c', ... satisfont aux conditions

$$0 \leqq a' \leqq a, \quad 0 \leqq b' \leqq b, \quad 0 \leqq c' \leqq c, \quad \ldots;$$

comme à deux combinaisons différentes quelconques des exposants a', b', c', ... correspondent (d'après 4°) deux idéaux $\mathfrak{b}$ différents, le nombre total des diviseurs différents sera $= (a+1)(b+1)(c+1)\ldots$.

9° Si $\mathfrak{b}$ est le plus grand commun diviseur des deux idéaux $\mathfrak{a}$, $\mathfrak{b}$, on aura

$$\mathfrak{a} = \mathfrak{b}\mathfrak{a}', \quad \mathfrak{b} = \mathfrak{b}\mathfrak{b}',$$

$\mathfrak{a}'$, $\mathfrak{b}'$ désignant deux idéaux premiers entre eux, et le plus petit commun multiple $\mathfrak{m}$ de $\mathfrak{a}$, $\mathfrak{b}$ sera $= \mathfrak{b}\mathfrak{a}'\mathfrak{b}' = \mathfrak{a}\mathfrak{b}' = \mathfrak{b}\mathfrak{a}'$. De plus, si $\mathfrak{a}\mathfrak{e}$ est divisible par $\mathfrak{b}$, $\mathfrak{e}$ sera divisible par $\mathfrak{b}'$.

Nous laisserons au lecteur le soin de chercher la démonstration de cette proposition et les règles qui servent à déduire les idéaux $\mathfrak{m}$, $\mathfrak{b}$ des décompositions de $\mathfrak{a}$, $\mathfrak{b}$ en facteurs premiers.

§ 26. — *Congruences.*

Après avoir établi les lois de la divisibilité des idéaux et, par suite, aussi des *nombres* contenus dans $\mathfrak{o}$, nous allons ajouter encore quelques considérations sur les congruences, importantes

pour la théorie des idéaux; nous nous contenterons toutefois, pour le moment, de donner de simples indications sur les démonstrations.

1° $\mathfrak{o}$ étant le plus grand commun diviseur de deux idéaux quelconques $\mathfrak{a}$, $\mathfrak{b}$, *premiers entre eux*, et $\mathfrak{ab}$ étant leur plus petit commun multiple, alors (§ 2, 5°) le système des deux congruences

$$\omega \equiv \rho \pmod{\mathfrak{a}}, \quad \omega \equiv \sigma \pmod{\mathfrak{b}},$$

ρ, σ étant deux nombres donnés contenus dans $\mathfrak{o}$, aura toujours des racines ω, et toutes ces racines seront comprises dans la forme

$$\omega \equiv \tau \pmod{\mathfrak{ab}},$$

τ étant le représentant d'une classe de nombres par rapport à $\mathfrak{ab}$, laquelle est complétement déterminée par les deux nombres ρ et σ, ou par les classes qui leur correspondent par rapport à $\mathfrak{a}$, $\mathfrak{b}$. Réciproquement, toute classe $\tau \pmod{\mathfrak{ab}}$ se déterminera de cette manière au moyen d'une combinaison, et d'une seule, $\rho \pmod{\mathfrak{a}}$, $\sigma \pmod{\mathfrak{b}}$.

Nous dirons maintenant que le nombre ρ est *premier avec* l'idéal $\mathfrak{a}$, lorsque $\mathfrak{o}\rho$ et $\mathfrak{a}$ seront des idéaux premiers entre eux, et nous désignerons par $\psi(\mathfrak{a})$ le nombre de tous les nombres incongrus suivant $\mathfrak{a}$ qui sont des nombres premiers avec $\mathfrak{a}$. On tire aisément de là, pour deux idéaux premiers entre eux, $\mathfrak{a}$, $\mathfrak{b}$, le théorème

$$\psi(\mathfrak{ab}) = \psi(\mathfrak{a})\psi(\mathfrak{b}) :$$

car τ est toujours, et seulement alors, un nombre premier avec $\mathfrak{ab}$, lorsque ρ est un nombre premier avec $\mathfrak{a}$, et σ un nombre premier avec $\mathfrak{b}$. On n'a donc besoin de déterminer la fonction $\psi(\mathfrak{a})$ que pour le cas où $\mathfrak{a}$ est une puissance $\mathfrak{p}^m$ de l'idéal premier $\mathfrak{p}$. Le nombre de tous les nombres incongrus suivant $\mathfrak{p}^m$ est, dans le cas de $m > 0$, égal à

$$\mathrm{N}(\mathfrak{p}^m) = [\mathrm{N}(\mathfrak{p})]^m = (\mathfrak{o}, \mathfrak{p}^m) = (\mathfrak{o}, \mathfrak{p})(\mathfrak{p}, \mathfrak{p}^m) = (\mathfrak{p}, \mathfrak{p}^m)\mathrm{N}(\mathfrak{p});$$

il faut en soustraire le nombre de tous les nombres qui ne sont pas premiers avec $\mathfrak{p}^m$ et, par suite, qui sont divisibles par $\mathfrak{p}$; ce

nombre étant égal à

$$(\mathfrak{p}, \mathfrak{p}^m) = [N(\mathfrak{p})]^{m-1},$$

il vient

$$\psi(\mathfrak{p}^m) = [N(\mathfrak{p})]^m - [N(\mathfrak{p})]^{m-1} = N(\mathfrak{p}^m)\left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

d'où l'on tire immédiatement, en vertu du théorème précédent,

$$\psi(\mathfrak{a}) = N(\mathfrak{a}) \prod \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

le signe de multiplication Π se rapportant à tous les idéaux premiers $\mathfrak{p}$, différents entre eux, qui divisent l'idéal $\mathfrak{a}$. Comme on a, de plus,

$$\psi(\mathfrak{o}) = 1,$$

on en conclut encore, absolument comme dans la théorie des nombres rationnels (¹), le théorème

$$\Sigma\psi(\mathfrak{a}') = N(\mathfrak{a}),$$

le signe sommatoire étant relatif à tous les idéaux $\mathfrak{a}'$ diviseurs de $\mathfrak{a}$.

2° Si $\mathfrak{b}$ est le plus grand commun diviseur des idéaux $\mathfrak{a}$ et $\mathfrak{o}\eta$, on aura $\mathfrak{a} = \mathfrak{b}\mathfrak{a}'$, et $\eta\mathfrak{a}'$ sera (§ 25, 9°) le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$, c'est-à-dire que $\mathfrak{a}'$ sera le diviseur de $\mathfrak{a}$ correspondant au nombre η (§ 19); réciproquement, si $\eta\mathfrak{a}'$ est le plus petit commun multiple de $\mathfrak{a}$ et de $\mathfrak{o}\eta$, on aura $\mathfrak{a} = \mathfrak{b}\mathfrak{a}'$, $\mathfrak{b}$ étant le plus grand commun diviseur de $\mathfrak{a}$ et de $\mathfrak{o}\eta$. Il est clair aussi que les facteurs complémentaires $\mathfrak{b}$ et $\mathfrak{a}'$ de l'idéal $\mathfrak{a}$ restent les mêmes pour tous les nombres η congrus entre eux suivant $\mathfrak{a}$; il en sera encore de même, évidemment, si l'on remplace η par un nombre $\eta' \equiv \eta\omega \pmod{\mathfrak{a}}$, ω désignant un nombre premier avec $\mathfrak{a}'$; et réciproquement, si le plus grand commun diviseur $\mathfrak{b}$ de $\mathfrak{a}$, $\mathfrak{o}\eta$ est en même temps celui de $\mathfrak{a}$, $\mathfrak{o}\eta'$; il en résulte

$$\eta' \equiv \eta\omega, \quad \eta = \eta'\omega' \pmod{\mathfrak{a}},$$

d'où l'on tire

$$\eta\omega\omega' \equiv \eta \pmod{\mathfrak{a}}, \quad \omega\omega' \equiv 1 \pmod{\mathfrak{a}'},$$

(¹) *Voir* DIRICHLET, *Vorlesungen über Zahlentheorie*, § 14.

et par conséquent ω est un nombre premier avec $\mathfrak{a}'$. Donc le nombre de tous les nombres η incongrus suivant $\mathfrak{a}$, auxquels correspond le même diviseur $\mathfrak{a}'$ de $\mathfrak{a}$, est $= \psi(\mathfrak{a}')$. Mais il faut bien faire attention à ce qu'ici l'on a supposé l'existence au moins d'un tel nombre η; donc, étant donné un diviseur quelconque $\mathfrak{a}'$ de l'idéal $\mathfrak{a}$, tout ce que nous pouvons affirmer jusqu'ici, c'est que le nombre $\chi(\mathfrak{a}')$ de tous les nombres η incongrus suivant $\mathfrak{a}$, auxquels correspond le même diviseur $\mathfrak{a}'$, sera égal à $\psi(\mathfrak{a}')$ ou à zéro. Pour décider cette alternative, considérons *tous* les nombres incongrus suivant $\mathfrak{a}$, qui sont au nombre de $N(\mathfrak{a})$, et ordonnons-les, suivant les diviseurs $\mathfrak{a}'$ qui leur correspondent, en groupes respectifs de $\chi(\mathfrak{a}')$ nombres; on devra avoir

$$\Sigma\chi(\mathfrak{a}') = N(\mathfrak{a}),$$

la sommation s'étendant à tous les diviseurs $\mathfrak{a}'$ de $\mathfrak{a}$; or, comme on a aussi (1°)

$$\Sigma\psi(\mathfrak{a}') = N(\mathfrak{a}),$$

il s'ensuit immédiatement que $\chi(\mathfrak{a}')$ n'est jamais $= 0$, mais toujours $= \psi(\mathfrak{a}')$. Ainsi se trouve démontré ce théorème très-important :

« Si $\mathfrak{b}$ et $\mathfrak{a}'$ sont deux idéaux quelconques, on pourra toujours, en multipliant $\mathfrak{b}$ par un idéal $\mathfrak{b}'$, premier avec $\mathfrak{a}'$, le changer en un idéal principal $\mathfrak{b}\mathfrak{b}' = (\eta)$. »

Car, en posant $\mathfrak{b}\mathfrak{a}' = \mathfrak{a}$, il existera toujours, puisque $\psi(\mathfrak{a}')$ est différent de zéro, un nombre η, auquel correspondra le diviseur $\mathfrak{a}$ de $\mathfrak{a}$, de telle sorte que $\mathfrak{b}$ sera le plus grand commun diviseur de $\mathfrak{a}$ et de (η); si l'on pose donc $(\eta) = \mathfrak{b}\mathfrak{b}'$, $\mathfrak{b}'$ sera un idéal premier avec $\mathfrak{a}'$.

C. Q. F. D.

3° Comme tout produit $\rho\rho'$ de nombres ρ, ρ' premiers avec un idéal $\mathfrak{a}$ est également un nombre premier avec $\mathfrak{a}$, et que, ρ restant constant et ρ' variant, $\rho\rho'$ parcourt un système de $\psi(\mathfrak{a})$ nombres incongrus (mod. $\mathfrak{a}$), on en déduit par la méthode connue (1), pour chaque valeur du nombre ρ, la congruence

$$\rho^{\psi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}},$$

(1) *Voir* Dirichlet, *Vorlesungen über Zahlentheorie*, § 19.

qui renferme la plus haute généralisation d'un célèbre théorème de Fermat. Pour un idéal premier $\mathfrak{p}$, on en conclut aisément que *tout* nombre ω du domaine $\mathfrak{o}$ satisfait à la congruence

$$\omega^{N(\mathfrak{p})} \equiv \omega \pmod{\mathfrak{p}},$$

c'est-à-dire à la congruence

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}},$$

p étant le nombre premier rationnel positif divisible par $\mathfrak{p}$, et f le degré de l'idéal premier $\mathfrak{p}$ (§ 21, 3°). Ce théorème est de la même importance pour la théorie du domaine $\mathfrak{o}$ que le théorème de Fermat pour la théorie des nombres rationnels, et c'est ce que nous allons du moins essayer de faire voir par les remarques suivantes, l'espace ne nous permettant pas de poursuivre plus avant la théorie générale.

Si les coefficients de la fonction rationnelle entière $F(x)$, du degré m, sont compris dans $\mathfrak{o}$, et que le coefficient du terme le plus élevé ne soit pas divisible par l'idéal premier $\mathfrak{p}$, on en déduit, par le raisonnement connu (1), que la congruence $F(\omega) \equiv 0 \pmod{\mathfrak{p}}$ ne peut avoir plus de m racines incongrues entre elles, et cette proposition, combinée avec le théorème précédent, conduit à une théorie complète des congruences binômes suivant le module $\mathfrak{p}$; on en déduit, entre autres, l'existence des *racines primitives* de l'idéal premier $\mathfrak{p}$, en entendant par là des nombres γ tels que leurs puissances

$$1, \gamma, \gamma^2, \ldots, \gamma^{N(\mathfrak{p})-2}$$

soient toutes incongrues entre elles. Généralement, la théorie des congruences de degré supérieur à coefficients rationnels peut s'appliquer complétement aux fonctions $F(x)$ dont les coefficients sont des nombres du domaine $\mathfrak{o}$.

Mais on peut déjà constater aussi une dépendance intime entre la théorie des idéaux et la théorie des congruences de degré supérieur, restreinte au cas des coefficients *rationnels*, dont on doit

(1) *Voir* DIRICHLET, *Vorlesungen über Zahlentheorie*, § 26.

l'établissement aux travaux de Gauss, de Galois, de Schönemann, de Serret (1). Tous les idéaux étant composés d'idéaux premiers, et chaque idéal premier $\mathfrak{p}$ divisant un nombre rationnel premier déterminé p, on obtiendra un aperçu complet sur tous les idéaux du domaine $\mathfrak{o}$, en décomposant tous les idéaux de la forme $\mathfrak{o}p$ dans leurs facteurs premiers. La théorie des congruences fournit pour cela un procédé suffisant dans un grand nombre de cas. Soit, en effet, θ un nombre entier du corps Ω, et

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{n-1}) = k^2\Delta(\Omega);$$

si p n'est pas diviseur de k, on reconnaîtra de la manière suivante la décomposition de $\mathfrak{o}p$ en idéaux premiers. Si $f(t)$ est la fonction entière du $n^{\text{ième}}$ degré de la variable t qui s'annule pour $t = \theta$, on pourra poser

$$f(t) \equiv \mathrm{P}_1(t)^{a_1}\mathrm{P}_2(t)^{a_2}\ldots\mathrm{P}_e(t)^{a_e} \pmod{p},$$

$\mathrm{P}_1(t), \mathrm{P}_2(t), \ldots, \mathrm{P}_e(t)$ étant des fonctions premières, différentes entre elles, des degrés respectifs $f_1, f_2, \ldots, f_e$, et alors on a certainement

$$\mathfrak{o}p = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_e^{a_e},$$

$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ étant des idéaux premiers, différents entre eux, des degrés respectifs $f_1, f_2, \ldots, f_e$. On tire de là facilement ce théorème extrêmement important :

« Le nombre premier rationnel p divise toujours, et seulement alors, le nombre fondamental $\Delta(\Omega)$ du corps Ω, lorsque p est divisible par le carré d'un idéal premier. »

Ce théorème est encore vrai, quoique bien plus difficile à démontrer, lorsque les nombres k, qui correspondent à tous les nombres θ possibles, sont tous divisibles par p; de tels cas se rencontrent en réalité (2), et c'est là une des raisons qui m'ont déterminé à fonder la théorie des idéaux non sur celle des congruences de degré supérieur, mais sur des principes entièrement nouveaux qui sont en

(1) *Voir* mon Mémoire : *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus.* (*Journal de Crelle*, t. 54.)

(2) Voir les *Göttingische gelehrte Anzeigen* du 20 septembre 1871, p. 1490.

même temps beaucoup plus simples, et qui répondent mieux à la véritable nature du sujet.

§ 27. — *Exemples empruntés à la division du cercle.*

Par la théorie générale des idéaux, dont j'ai développé les bases dans ce qui précède, les phénomènes de la divisibilité des nombres pour tout domaine $\mathfrak{o}$, composé de tous les nombres entiers d'un corps fini Ω, ont été ramenés aux mêmes lois fixes qui règnent dans l'ancienne théorie des nombres rationnels. Si l'on pense à la variété infinie de ces corps Ω, dont chacun possède sa théorie des nombres spéciale, l'esprit du géomètre aura lieu, sans nul doute, d'être satisfait en constatant l'unité ou l'identité des lois générales auxquelles ces théories diverses obéissent sans exception. Mais ce n'est pas seulement un intérêt esthétique ou purement théorique, mais aussi un intérêt on ne peut plus pratique qui se rattache à cette constatation ; car la certitude que ces lois générales existent réellement facilite au plus haut degré la démonstration et la découverte des phénomènes spéciaux qui se présentent dans un corps déterminé Ω. L'établissement de cette vérité dans toute son étendue exigerait, il est vrai, que l'on poussât beaucoup plus loin le développement de la théorie générale des idéaux que nous ne pouvions le faire ici, et qu'on la combinât en particulier avec les principes algébriques de Galois; mais j'essayerai du moins de montrer, sur l'exemple simple à l'occasion duquel Kummer a introduit pour la première fois ses nombres idéaux, que déjà les premiers éléments de la théorie générale, exposés dans ce qui précède, conduisent au but avec la plus grande facilité.

Soit m un *nombre premier* rationnel positif, et Ω le corps du $n^{\text{ième}}$ degré, qui résulte, de la manière indiquée plus haut (§ 15), d'une racine primitive θ de l'équation $\theta^m = 1$, c'est-à-dire d'une racine de l'équation

$$f(\theta) = \theta^{m-1} + \theta^{m-2} + \ldots + \theta^2 + \theta + 1 = 0;$$

les coefficients étant rationnels, on aura toujours $n \leqq m-1$. Comme, de plus, $\theta, \theta^2, \ldots, \theta^{m-1}$ sont toutes les racines de cette équation, on aura, en désignant par t une variable,

$$f(t) = \frac{t^m - 1}{t - 1} = (t-\theta)(t-\theta^2)\ldots(t-\theta^{m-1}),$$

et, par suite,

$$m = (1 - \theta)(1 - \theta^2)\dots(1 - \theta^{m-1}).$$

Les m facteurs du second membre sont des nombres entiers et associés entre eux; car, si r désigne un des nombres $1, 2, \dots, m-1$, alors

$$\frac{1-\theta^r}{1-\theta} = 1 + \theta + \theta^2 + \dots + \theta^{r-1}$$

sera un nombre entier, et si s est positif et choisi de façon que l'on ait $rs \equiv 1 \pmod{m}$,

$$\frac{1-\theta}{1-\theta^r} = \frac{1-\theta^{rs}}{1-\theta^r} = 1 + \theta^r + \theta^{2r} + \dots + \theta^{(s-1)r}$$

sera aussi un nombre entier. En faisant donc, pour abréger,

$$1 - \theta = \mu,$$

il vient

$$m = \varepsilon \mu^{m-1},$$

ε désignant une unité du corps Ω, et par suite, en formant la norme,

$$m^n = [\mathrm{N}(\mu)]^{m-1}.$$

Or, m étant un nombre premier, $\mathrm{N}(\mu)$ devra être une puissance de m; si l'on pose $\mathrm{N}(\mu) = m^e$, il en résulte $n = e(m-1)$, et comme, ainsi qu'on l'a remarqué plus haut, n est toujours $\leq m - 1$, on en conclut $e = 1$, et $n = m - 1 = \varphi(m)$. L'équation précédente $f(\theta) = 0$ est donc *irréductible;* les nombres $\theta, \theta^2, \dots, \theta^{m-1}$ sont conjugués, et à ces nombres correspondent $m-1$ permutations, par lesquelles le corps normal Ω se change en lui-même; on a en même temps

$$\mathrm{N}(\mu) = m, \quad \mathfrak{o}m = \mathfrak{o}\mu^{m-1}.$$

L'idéal principal $\mathfrak{o}\mu$ est un *idéal premier;* si l'on avait, en effet, $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{b}$, $\mathfrak{a}$ et $\mathfrak{b}$ étant deux idéaux différents de $\mathfrak{o}$, il s'ensuivrait que $m = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$, et puisque m est un nombre premier, il faudrait que l'on eût, par exemple, $\mathrm{N}(\mathfrak{a}) = m, \mathrm{N}(\mathfrak{b}) = 1$, d'où $\mathfrak{b} = \mathfrak{o}$, ce qui est contraire à l'hypothèse. En même temps (§ 21, 3°), m est le plus petit nombre rationnel divisible par μ; les nombres $0, 1, 2, \dots, m-1$ forment un système complet de nombres incongrus suivant

le module μ. De là résulte encore qu'un nombre de la forme

$$\omega = k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2},$$

$k_0, k_1, k_2, \ldots, k_{m-2}$ désignant des nombres entiers, n'est divisible par m, et conséquemment par μ^{m-1}, que si tous les nombres k_0, $k_1, \ldots, k_{m-2}$ sont divisibles par m; car, puisque ω doit être aussi divisible par μ, il faut que k_0 soit divisible par μ, et partant aussi par m; il faut ensuite que $\omega - k_0$ soit divisible par m, et partant aussi par μ^2, d'où l'on conclut de même que k_1 doit être divisible par μ, et partant aussi par m; et, en continuant ainsi, on en déduit que les autres nombres $k_2, k_3, \ldots, k_{m-2}$ sont divisibles par m.

A l'aide de ce résultat, il est aisé de démontrer que les $m-1$ nombres $1, \theta, \theta^2, \ldots, \theta^{m-2}$ forment une base du domaine $\mathfrak{o}$ de tous les nombres entiers du corps Ω. Puisqu'on a

$$t^m - 1 = (t-1)f(t), \quad m\theta^{m-1} = (\theta - 1)f'(\theta),$$

il en résulte, en excluant le cas peu intéressant de $m = 2$,

$$\mathrm{N}[f'(\theta)] = m^{m-2},$$

à cause de $\mathrm{N}(\theta) = 1$ et de $\mathrm{N}(\theta - 1) = m$, et il s'ensuit de là (§ 17) que

$$\Delta(1, \theta, \theta^2, \ldots, \theta^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Comme, de plus, $\mu = 1 - \theta$, $\theta = 1 - \mu$, il est clair que les deux modules $[1, \theta, \ldots, \theta^{m-2}]$ et $[1, \mu, \ldots, \mu^{m-2}]$ sont identiques, d'où il résulte [§ 4, 3°, et § 17, (5)] que l'on a aussi

$$\Delta(1, \mu, \mu^2, \ldots, \mu^{m-2}) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Puisque les nombres $1, \mu, \mu^2, \ldots, \mu^{m-2}$ sont indépendants entre eux, tout nombre du corps Ω peut maintenant se mettre sous la forme

$$\frac{k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2}}{k} = \frac{\omega}{k},$$

$k, k_0, k_1, k_2, \ldots, k_{m-2}$ désignant des nombres rationnels entiers *sans diviseur commun;* pour que ce nombre soit entier, c'est-à-dire pour que ω soit divisible par k, il faudra (§ 18) que k^2 divise le

discriminant de la base $1, \mu, \mu^2, \ldots, \mu^{m-2}$, et, par suite, k ne pourra contenir d'autres facteurs premiers que le nombre m; comme, de plus, il a été démontré plus haut que ω ne peut être divisible par m que si les nombres $k_0, k_1, \ldots, k_{m-2}$ sont tous divisibles par m, k ne pourra non plus être divisible par m; il faudra donc que l'on ait $k = \pm 1$; donc tous les nombres entiers du corps sont de la forme

$$\omega = k_0 + k_1\mu + k_2\mu^2 + \ldots + k_{m-2}\mu^{m-2},$$

et, par suite, on aura

$$\mathfrak{o} = [1, \mu, \ldots, \mu^{m-2}] = [1, \theta, \ldots, \theta^{m-2}],$$

ou encore, à cause de $1 + \theta + \theta^2 + \ldots + \theta^{m-2} + \theta^{m-1} = 0$,

$$\mathfrak{o} = [\theta, \theta^2, \ldots, \theta^{m-1}], \quad \Delta(\Omega) = (-1)^{\frac{m-1}{2}} m^{m-2}.$$

Soit maintenant $\mathfrak{p}$ un idéal premier quelconque, différent de $\mathfrak{o}\mu$; le nombre premier rationnel positif p, divisible par $\mathfrak{p}$, sera différent de m, et l'on aura

$$\mathrm{N}(\mathfrak{p}) = p^f,$$

f désignant le degré de l'idéal premier $\mathfrak{p}$. Deux puissances θ^r, θ^s ne sont congrues relativement à un tel idéal premier $\mathfrak{p}$ que si elles sont égales entre elles, c'est-à-dire si l'on a $r \equiv s \pmod{m}$; car, dans le cas contraire, on a $\theta^r - \theta^s = \theta^r(1 - \theta^{r-s}) = \varepsilon\mu$, ε désignant une unité, et, par suite, θ^r ne pourra être $\equiv \theta^s \pmod{\mathfrak{p}}$. Comme on a maintenant (§ 26, 3°)

$$\theta^{\mathrm{N}(\mathfrak{p})} \equiv \theta \pmod{\mathfrak{p}};$$

il en résulte

$$p^f \equiv 1 \pmod{m}.$$

Soit a le diviseur de $\varphi(m) = m - 1$ auquel *appartient* le nombre p par rapport au module m, c'est-à-dire, soit a le plus petit exposant positif pour lequel on a

$$p^a \equiv 1 \pmod{m};$$

f devra être, comme on sait, divisible par a, et partant on aura $f \geqq a$. Or tous les nombres entiers du corps Ω étant de la forme

$$\omega = \mathrm{F}(\theta) = x_1\theta + x_2\theta^2 + \ldots + x_{m-1}\theta^{m-1},$$

où $x_1, x_2, \ldots, x_m$ représentent des nombres rationnels entiers, il résulte de théorèmes connus, vrais pour tout nombre premier p, que l'on a

$$\omega^p \equiv F(\theta^p), \quad \omega^{p'} \equiv F(\theta^{p'}) \pmod{p},$$

et, par suite,

$$\omega^{p^a} \equiv \omega \pmod{p}.$$

On conclut de là d'abord que l'idéal $\mathfrak{o}p$ est un produit d'idéaux premiers tous *différents entre eux;* car, si l'on avait $\mathfrak{o}p = \mathfrak{p}^2\mathfrak{q}$, il existerait un nombre ω divisible par $\mathfrak{p}\mathfrak{q}$, mais non divisible par p, et ω^2, et par suite aussi ω^{p^a} seraient donc divisibles par $\mathfrak{p}^2\mathfrak{q}^2 = p\mathfrak{q}$, et donc aussi par p, ce qui est en contradiction avec la congruence précédente. Comme, de plus, p est divisible par $\mathfrak{p}$, *tout* nombre entier ω du corps Ω satisfait donc à la congruence

$$\omega^{p^a} \equiv \omega \pmod{\mathfrak{p}};$$

le nombre de ses racines incongrues ω est donc $= N(\mathfrak{p}) = p^f$, et comme son degré $= p^a$, il faut que p^f soit $\leq p^a$, et partant $f \geq a$; mais il a été déjà démontré plus haut que f est $\geq a$; par conséquent $f = a$. On parvient ainsi au résultat suivant, qui forme le théorème principal de la théorie de Kummer (1) :

« Si le nombre premier p, différent de m, appartient, par rapport au module m, à l'exposant f, qui est toujours un diviseur de $\varphi(m) = ef$, on a

$$\mathfrak{o}p = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_e,$$

$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_e$ étant des idéaux premiers, différents entre eux, du degré f. »

Tout le reste s'en déduit facilement. On peut traiter d'une manière toute semblable le cas général, où m est un nombre composé quelconque. Le degré du corps normal Ω est toujours égal au nombre $\varphi(m)$ de ceux des nombres $1, 2, 3, \ldots, m$ qui sont premiers avec m; la loi précédente n'éprouve aucun changement, et la détermination des idéaux premiers qui divisent m ne présente non plus aucune difficulté.

---

(1) Les recherches de Kummer se trouvent dans le *Journal de Crelle,* t. 35, dans le *Journal de Liouville*, t. XVI; dans les *Mémoires de l'Académie de Berlin* pour l'année 1856.

D'après des recherches très-générales, que je publierai prochainement, on peut, étant connus les idéaux d'un corps normal Ω, indiquer immédiatement aussi les idéaux d'un *diviseur* quelconque de Ω, c'est-à-dire d'un corps quelconque H, dont les nombres soient tous contenus dans Ω. D'après cela, on connaîtra, par exemple, les idéaux de *tous* les corps H qui résultent de la division du cercle, et, pour donner une idée plus précise de la portée de ces recherches, je me permettrai de signaler le cas suivant.

Soit encore m un nombre premier, d'où $\varphi(m) = m - 1$, et soit e un diviseur quelconque de $m - 1 = ef$; dans la théorie des nombres rationnels, la congruence

$$h^f \equiv 1 \pmod{m}$$

aura précisément f racines h incongrues entre elles, qui se reproduiront par la multiplication, et qui, dans ce sens, formeront un *groupe*. Si θ est encore une racine primitive de l'équation $\theta^m = 1$, et Ω le corps correspondant du degré $m - 1$, tous les nombres $F(\theta)$ contenus dans ce corps et satisfaisant aux conditions $F(\theta) = F(\theta^h)$ formeront un corps H du degré e, et les e *périodes* [1] conjuguées $\eta_1, \eta_2, \ldots, \eta_e$, formées chacune de f termes, et dont l'une est

$$\eta = \Sigma\theta^h,$$

formeront une base du domaine $\mathfrak{e}$ composé de tous les nombres entiers contenus dans H. A l'aide des recherches générales dont je viens de parler (ou encore, immédiatement, par des conclusions semblables à celles qu'on a tirées plus haut pour le cas de $e = m - 1$), on obtient maintenant la détermination suivante des idéaux premiers appartenant à ce diviseur H du corps normal Ω. Si l'on pose

$$\rho = \Pi(1 - \theta^h),$$

ρ est un nombre entier du corps H, m est associé avec ρ^e, et $\mathfrak{e}\rho$ est un idéal premier; si, de plus, p est un nombre premier rationnel différent de m, et que p^f appartienne à l'exposant f' par rapport à m, f' sera nécessairement un diviseur de $e = e'f'$, et l'idéal prin-

---

[1] *Disquisitiones arithmeticæ*, art. 343.

cipal $\mathfrak{p}$ sera le produit de e' idéaux premiers, différents entre eux, du degré f'. Dans le cas de $e = m - 1$, $f = 1$, H est identique avec Ω, et l'on obtient encore le résultat démontré plus haut. Examinons maintenant de plus près le cas de $e = 2$, $f = \frac{m-1}{2}$.

Dans ce cas, les f nombres h sont les résidus quadratiques de m; en désignant par k l'ensemble des non-résidus quadratiques, les deux périodes conjuguées

$$\eta = \Sigma\theta^h, \quad \eta' = \Sigma\theta^k$$

forment une base du domaine $\mathfrak{e}$ composé de tous les nombres entiers contenus dans le corps quadratique H, et, par suite, son discriminant sera

$$\Delta(\mathrm{H}) = \begin{vmatrix} \eta & \eta' \\ \eta' & \eta \end{vmatrix}^2 = (\eta - \eta')^2,$$

à cause de $\eta + \eta' = -1$; le nombre m est associé avec le carré du nombre $\rho = \Pi(1 - \theta^h)$, et $\mathfrak{e}\rho$ est un idéal premier; de plus, $\mathfrak{e}\mathfrak{p}$ est le produit de deux idéaux premiers différents, du premier degré, ou bien $\mathfrak{e}\mathfrak{p}$ est un idéal premier du second degré, suivant que l'on a

$$p^{\frac{m-1}{2}} \equiv +1 \quad \text{ou} \quad \equiv -1 \pmod{m},$$

c'est-à-dire, d'après la notation de Legendre, suivant que l'on a

$$\left(\frac{p}{m}\right) = +1 \text{ ou } = -1.$$

Mais on peut étudier directement tous les corps quadratiques, sans avoir recours à la division du cercle, et nous avons déjà (§ 18) déterminé le discriminant D' d'un tel corps H. On peut déduire tout aussi facilement de D' les idéaux premiers (1) appartenant au corps H : si le nombre premier rationnel p divise D', l'idéal principal $\mathfrak{e}\mathfrak{p}$ qui lui correspond sera le carré d'un idéal premier; mais, si p ne divise pas D', et que p soit impair, $\mathfrak{e}\mathfrak{p}$ sera le produit de deux idéaux premiers différents du premier degré, ou bien un idéal

(1) *Voir* DIRICHLET, *Vorlesungen über Zahlentheorie*, § 168.

premier du second degré, suivant que l'on aura

$$\left(\frac{D'}{p}\right) = +1 \text{ ou } = -1;$$

si, de plus, D′ est impair et, par suite, $\equiv 1 \pmod 4$, $\mathfrak{e}(\mathfrak{a})$ sera le produit de deux idéaux premiers du premier degré, ou bien un idéal premier du second degré, suivant que l'on aura

$$D' \equiv 1 \text{ ou } \equiv 5 \pmod 8.$$

En comparant ces lois, vraies pour tous les corps quadratiques, avec le résultat déduit de la division du cercle pour le corps spécial précédent H, on voit d'abord que D′ doit être divisible par m, mais par aucun autre nombre premier, et, par suite, qu'on doit avoir (§ 18)

$$\Delta(H) = D' = (-1)^{\frac{m-1}{2}} m;$$

de cette manière on déduit de principes tout à fait généraux, sans aucun calcul, le résultat connu

$$(\eta - \eta')^2 = (-1)^{\frac{m-1}{2}} m,$$

que l'on démontre dans la division du cercle par la formation effective du carré de $\eta - \eta'$ (¹). En poursuivant cette comparaison, on est conduit encore au théorème

$$\left(\frac{p}{m}\right) = \left(\frac{\pm m}{p}\right),$$

$\pm m$ étant $\equiv 1 \pmod 4$, et au théorème

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

Cette démonstration de la loi de réciprocité, par laquelle on détermine en même temps le caractère quadratique du nombre -1, coïncide, au fond, avec la célèbre sixième démonstration de Gauss (²), reproduite plus tard sous les formes les plus différentes par Jacobi,

(¹) *Disquisitiones arithmeticæ*, art. 356.

(²) *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novæ ;* 1817.

Eisenstein et autres, et je ferai remarquer expressément que c'est en méditant sur le nerf de cette démonstration et des démonstrations analogues de la loi de réciprocité cubique et biquadratique, que j'ai été conduit aux recherches générales que j'ai indiquées plus haut et que je publierai prochainement.

Comme dernier exemple, nous considérerons le cas de $m = 4$; on a alors $\theta = i = \sqrt{-1}$, et les nombres entiers du corps quadratique Ω sont les nombres complexes entiers, introduits pour la première fois par Gauss, de la forme

$$\omega = x + yi,$$

x, y désignant des nombres rationnels entiers (§ 6); le discriminant de ce corps est

$$\begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4.$$

Le nombre $2 = i(1-i)^2$ est associé avec le carré du nombre premier $1-i$. Si p est un nombre premier rationnel positif impair, on a

$$i^p = (-1)^{\frac{p-1}{2}} i,$$

et, par suite,

$$\omega^p = (x+yi)^p \equiv x + (-1)^{\frac{p-1}{2}} yi \pmod{p};$$

si l'on a maintenant $p \equiv 1 \pmod 4$, tout nombre entier ω satisfera à la congruence

$$\omega^p \equiv \omega \pmod{p},$$

d'où il s'ensuit immédiatement que $\mathfrak{o}p$ est le produit de deux idéaux premiers du premier degré différents; mais, si l'on a $p \equiv 3 \pmod 4$, il vient

$$\omega^p \equiv \omega', \quad \omega^{p^2} \equiv \omega \pmod{p},$$

ω' désignant le nombre conjugué avec ω, et l'on en conclut facilement que $\mathfrak{o}p$ est un idéal premier du second degré. Or tout idéal $\mathfrak{a}$ de ce corps doit être un idéal principal; si, en effet, σ_0 est un des nombres de l'idéal $\mathfrak{a}$ dont les normes ont une valeur positive *minimum*, tout nombre α de l'idéal $\mathfrak{a}$ sera divisible par α_0; car on peut

(§ 6) choisir le nombre entier ω de manière que l'on ait

$$N(\alpha - \omega\alpha_0) < N(\alpha_0),$$

et comme les nombres α, α_0 et, par suite aussi, $\alpha - \omega\alpha_0$ appartiennent à l'idéal $\mathfrak{a}$, il faudra que l'on ait $N(\alpha - \omega\alpha_0) = 0$, d'où $\alpha = \omega\alpha_0$, et par conséquent $\mathfrak{a} = \mathfrak{o}\alpha_0$. C. Q. F. D.

Maintenant, puisque, dans le cas où p est un nombre premier rationnel et $\equiv 1 \pmod 4$, $\mathfrak{o}p$ est le produit de deux idéaux premiers du premier degré, il en résulte que l'on a

$$p = N(\alpha_0) = N(a + bi) = a^2 + b^2,$$

ce qui constitue le célèbre théorème de Fermat.

§ 28. — *Classes d'idéaux.*

Revenons maintenant à la considération d'un corps quelconque Ω du degré n, pour établir la distribution de ses idéaux en *classes*. Cette distribution s'appuie d'abord sur ce théorème (§ 25, 5°), que tout idéal $\mathfrak{a}$ peut, au moyen de la multiplication par un idéal $\mathfrak{m}$, se changer en un idéal principal, et sur la définition suivante : Deux idéaux $\mathfrak{a}$, $\mathfrak{a}'$ seront dits *équivalents*, lorsque, au moyen de la multiplication par un seul et même idéal $\mathfrak{m}$, ils pourront se changer en idéaux principaux $\mathfrak{am} = \mathfrak{o}\mu$, $\mathfrak{a}'\mathfrak{m} = \mathfrak{o}\mu'$. Alors on a évidemment $\mu'\mathfrak{a} = \mu\mathfrak{a}'$; et réciproquement, s'il existe deux nombres η, η' différents de zéro, qui satisfassent à la condition $\eta'\mathfrak{a} = \eta\mathfrak{a}'$, les idéaux $\mathfrak{a}$, $\mathfrak{a}'$ seront certainement équivalents; car si, en multipliant $\mathfrak{a}$ par $\mathfrak{m}$, on le change en un idéal principal $\mathfrak{am} = \mathfrak{o}\mu$, il s'ensuit que $\mathfrak{o}\mu\eta' = \eta'\mathfrak{am} = \eta\mathfrak{a}'\mathfrak{m}$; donc $\mu\eta'$ est divisible par η, d'où $\mu\eta' = \mu'\eta$, $\mathfrak{o}\mu'\eta = \eta\mathfrak{a}'\mathfrak{m}$, et partant $\mathfrak{a}'\mathfrak{m} = \mathfrak{o}\mu'$. C. Q. F. D.

Si deux idéaux $\mathfrak{a}'$, $\mathfrak{a}''$ sont équivalents à un troisième $\mathfrak{a}$, alors $\mathfrak{a}'$, $\mathfrak{a}''$ seront aussi équivalents entre eux; car, d'après l'hypothèse, il existe quatre nombres μ, μ', η, η'', satisfaisant aux conditions $\mu'\mathfrak{a} = \mu\mathfrak{a}'$, $\eta''\mathfrak{a} = \eta\mathfrak{a}''$, et l'on a, par suite, $(\eta''\mu)\mathfrak{a}' = (\mu'\eta)\mathfrak{a}''$; C. Q. F. D. De là résulte la distribution de tous les idéaux en classes : si $\mathfrak{a}$ est un idéal déterminé, le système A de tous les idéaux $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{a}''$, ... équivalents à $\mathfrak{a}$ s'appellera une *classe d'idéaux*, et $\mathfrak{a}$ sera dit le *représentant* de cette classe A. Deux idéaux quelconques contenus dans A seront équivalents, et à la place de $\mathfrak{a}$ on pourra

toujours choisir comme représentant tout autre idéal $\mathfrak{a}'$ contenu dans A.

Il est clair que le système de tous les idéaux principaux forme lui-même une classe; car chacun d'eux se change en lui-même quand on le multiplie par l'idéal $\mathfrak{o}$, et, par suite, ils sont équivalents; et si un idéal $\mathfrak{a}$ est équivalent à un idéal principal, et partant aussi à $\mathfrak{o}$, $\mathfrak{a}$ devra être lui-même un idéal principal; car il existe deux nombres μ, μ', qui satisfont à la condition $\mu'\mathfrak{a} = \mathfrak{o}\mu$, et de là résulte encore que μ est divisible par μ', d'où $\mu = \mu'\mu''$, et conséquemment $\mathfrak{a} = \mathfrak{o}\mu''$. Donc la classe représentée par $\mathfrak{o}$ contient tous les idéaux principaux et ne contient aucun autre idéal. Nous appellerons cette classe la *classe principale,* et nous la désignerons par O.

Si maintenant $\mathfrak{a}$ représente successivement tous les idéaux de la classe A, et de même $\mathfrak{b}$ tous ceux de la classe B, tous les produits $\mathfrak{ab}$ appartiendront à une seule et même classe K; car si $\mathfrak{a}'$, $\mathfrak{a}''$ sont contenus dans A, et $\mathfrak{b}'$, $\mathfrak{b}''$ dans B, il existe quatre nombres α', α'', β', β'' satisfaisant aux conditions $\alpha''\mathfrak{a}' = \alpha'\mathfrak{a}''$, $\beta''\mathfrak{b}' = \beta'\mathfrak{b}''$, et de là il s'ensuit que $(\alpha''\beta'')(\mathfrak{a}'\mathfrak{b}') = (\alpha'\beta')(\mathfrak{a}''\mathfrak{b}'')$, c'est-à-dire que $\mathfrak{a}'\mathfrak{b}'$ et $\mathfrak{a}''\mathfrak{b}''$ sont des idéaux équivalents. Nous désignerons cette classe K, à laquelle appartiennent tous les produits $\mathfrak{ab}$, par AB, et nous la nommerons le *produit* de A par B, ou la classe *composée* de A et de B. On a évidemment AB = BA, et de l'égalité $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ résulte, pour trois classes quelconques A, B, C, le théorème (AB)C = A(BC). On peut donc appliquer ici les mêmes raisonnements que pour la multiplication des nombres ou des idéaux, et démontrer que, dans la composition d'un nombre quelconque de classes $A_1, A_2, \ldots, A_m$, l'ordre des multiplications successives, qui réunissent chaque fois deux classes dans leur produit, n'a aucune influence sur le résultat final, que l'on peut désigner simplement par $A_1 A_2 \ldots A_m$. Si les idéaux $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ sont des représentants des classes $A_1, A_2, \ldots, A_m$, l'idéal $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_m$ sera un représentant de la classe $A_1 A_2 \ldots A_m$. Si les m facteurs sont tous = A, leur produit sera dit la $m^{\text{ième}}$ puissance de A, et nous le désignerons par A^m; nous poserons, en outre, $A^1 = A$ et $A^0 = O$. Les deux cas suivants sont particulièrement importants :

De l'égalité $\mathfrak{oa} = \mathfrak{a}$ résulte le théorème, vrai pour une classe quelconque A, OA = A.

Comme, de plus, tout idéal $\mathfrak{a}$ peut, au moyen de la multiplication par un idéal $\mathfrak{m}$, être transformé en un idéal principal $\mathfrak{am}$, il existera pour chaque classe A une classe correspondante M, satisfaisant à la condition $AM = O$, et il en existera une seule; car si la classe N satisfait aussi à la condition $AN = O$, il en résultera que

$$N = NO = N(AM) = M(AN) = MO = M.$$

Cette classe M s'appellera la classe *opposée* ou la classe *inverse* de A, et nous la désignerons par A^{-1}; il est clair que, réciproquement, A sera la classe inverse de A^{-1}. Si l'on définit, de plus, A^{-m} comme étant la classe inverse de A^m, on aura, pour des exposants rationnels entiers quelconques r, s, les théorèmes

$$A^r A^s = A^{r+s}, \quad (A^r)^s = A^{rs}, \quad (AB)^r = A^r B^r.$$

Enfin, il est évident que de $AB = AC$ on conclura, en multipliant par A^{-1}, que l'on a toujours $B = C$.

§ 29. — *Le nombre des classes d'idéaux.*

En prenant à volonté n nombres entiers $\omega_1, \omega_2, \ldots, \omega_n$, formant une base du corps Ω, tout nombre

$$\omega = h_1\omega_1 + h_2\omega_2 + \ldots + h_n\omega_n;$$

à coordonnées rationnelles entières $h_1, h_2, \ldots, h_n$, sera également un nombre entier du même corps. Si l'on attribue aux coordonnées toutes les valeurs entières qui, prises en valeur absolue, ne surpassent pas une valeur positive déterminée k, il est évident que les valeurs absolues des nombres correspondants ω, s'ils sont réels, ou leurs modules analytiques, s'ils sont imaginaires, seront tous $\leqq rk$, r étant la somme des valeurs absolues ou des modules de ω_1, $\omega_2, \ldots, \omega_n$, et, par suite, une constante entièrement indépendante de k. Comme, de plus, la norme $N(\omega)$ est un produit de n nombres conjugués ω de la forme ci-dessus, on aura en même temps

$$\pm N(\omega) \leqq sk^n,$$

s désignant pareillement une constante dépendant uniquement de la base. On tire de là le théorème suivant :

Dans toute classe d'idéaux M *il existe au moins un idéal* $\mathfrak{m}$ *dont la norme ne surpasse pas la constantes.*

Démonstration. — Prenons à volonté un idéal $\mathfrak{a}$ de la classe inverse M^{-1}, et choisissons pour k le nombre rationnel entier positif déterminé par les conditions

$$k^n \leqq N(\mathfrak{a}) < (k+1)^n;$$

si l'on attribue maintenant à chacune des n coordonnées $h_1, h_2, \ldots, h_n$ toutes les $k+1$ valeurs $0, 1, 2, \ldots, k$, on n'obtiendra que des nombres différents ω, et comme leur nombre $= (k+1)^n$, et, par suite, $> N(\mathfrak{a})$, il existe nécessairement, parmi ces nombres ω, deux nombres différents entre eux,

$$\beta = b_1\omega_1 + \ldots + b_n\omega_n, \quad \gamma = c_1\omega_1 + \ldots + c_n\omega_n,$$

qui sont congrus entre eux suivant $\mathfrak{a}$; par suite, leur différence

$$\alpha = (b_1 - c_1)\omega_1 + \ldots + (b_n - c_n)\omega_n$$

sera un nombre différent de zéro et divisible par $\mathfrak{a}$. Or les coordonnées b, c des nombres β, γ étant comprises dans la suite $0, 1, 2, \ldots, k$, les coordonnées $b - c$ du nombre α, prises en valeur absolue, ne surpassent pas la valeur k, et, par suite, on a

$$\pm N(\alpha) \leqq sk^n.$$

Mais, α étant divisible par $\mathfrak{a}$, on a $\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{m}$, où $\mathfrak{m}$ désigne un idéal de la classe M, et, par suite,

$$\pm N(\alpha) = N(\mathfrak{a})N(\mathfrak{m}) \leqq sk^n;$$

comme on a, de plus, $k^n \leqq N(\mathfrak{a})$, il en résulte $N(\mathfrak{m}) \leqq s$. C. Q. F. D.

Si l'on considère maintenant que la norme m d'un idéal $\mathfrak{m}$ est toujours divisible par $\mathfrak{m}$ (§ 20), il est clair qu'il ne peut exister qu'un nombre fini d'idéaux $\mathfrak{m}$ ayant une norme donnée m, parce que tout idéal, et partant aussi $\mathfrak{o}m$, est divisible seulement par un nombre fini d'idéaux (§ 25, 8°). Comme, en outre, il n'existe qu'un nombre fini de nombres rationnels entiers m ne surpassant pas une constante donnée s, il ne peut non plus y avoir qu'un nombre fini d'idéaux $\mathfrak{m}$ satisfaisant à la condition $N(\mathfrak{m}) \leqq s$, et de là résulte évidemment ce théorème fondamental :

Le nombre des classes d'idéaux du corps Ω *est fini.*

La détermination *exacte* du nombre des classes d'idéaux forme incontestablement un des problèmes les plus importants, mais aussi les plus difficiles de la Théorie des nombres. Pour les corps quadratiques, dont la théorie coïncide essentiellement avec celle des *formes* quadratiques binaires, le problème a été, comme on sait, complétement résolu pour la première fois par Dirichlet (1); cette solution, en exprimant tout avec la terminologie de la théorie des *idéaux,* repose sur l'étude de la fonction

$$\sum \frac{1}{N(\mathfrak{a})^s} = \prod \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}$$

pour des valeurs positives infiniment petites de la variable indépendante $s - 1$; la somme s'étend à tous les idéaux $\mathfrak{a}$, le produit à tous les idéaux premiers $\mathfrak{p}$, et l'identité des deux expressions est une conséquence immédiate des lois de la divisibilité (§ 25). A l'aide de ces principes, le nombre des classes de formes ou d'idéaux a été, depuis, déterminé par Eisenstein (2) pour un cas particulier des corps du troisième degré, et par Kummer (3) pour les corps de degré supérieur qui proviennent de la division du cercle. Les résultats de ces recherches excitent le plus vif intérêt par les relations étonnantes qu'elles offrent avec l'Analyse, l'Algèbre et les autres parties de la Théorie des nombres; ainsi, par exemple, le problème traité par Kummer se relie le plus étroitement avec la célèbre démonstration qui a été donnée par Dirichlet du théorème sur la progression arithmétique, et qui peut être considérablement simplifiée à l'aide de ces recherches. On ne peut faire aucun doute qu'en poursuivant l'étude du problème général on ne doive s'attendre à réaliser d'importants progrès dans ces branches des Mathématiques; mais, bien que l'on ait réussi à terminer d'une manière générale une partie de cette recherche pour un corps quelconque Ω (4), on est cependant encore très-loin de la solution complète, et

(1) *Journal de Crelle,* t. 19, 21.
(2) *Journal de Crelle,* t. 28.
(3) *Journal de Crelle,* t. 40; *Journal de Liouville,* t. XVI.
(4) DIRICHLET, *Vorlesungen über Zahlentheorie,* § 167.

l'on devra pour le moment se borner à étudier de nouveaux cas particuliers.

§ 30. — *Conclusion.*

Nous allons encore déduire quelques conséquences intéressantes du théorème fondamental que nous venons de démontrer. (Voir *Disquisitiones arithmeticæ,* art. 305-307.)

Soient h le nombre de toutes les classes d'idéaux du corps Ω, et A une classe déterminée; les $h+1$ puissances

$$O,\ A,\ A^2,\ \ldots,\ A^{h-1},\ A^h$$

ne pourront pas être toutes différentes; il se trouvera donc certainement, dans la suite $0, 1, 2, \ldots, h$, deux exposants différents r et $r+m > r$, pour lesquels on aura $A^{r+m} = A^r$, et, par suite,

$$A^m = O;$$

si, de plus, m est *le plus petit* exposant positif qui satisfasse à la condition précédente, il est aisé de voir que les m classes

$$O,\ A,\ A^2,\ \ldots,\ A^{m-1}$$

seront toutes différentes entre elles, et nous dirons que la classe A *appartient* à l'exposant m; on a évidemment $A^{m-1} = A^{-1}$, et, plus généralement, on aura $A^r = A^s$ toutes les fois, et seulement alors, que r sera $\equiv s \pmod{m}$. En désignant, de plus, par B une classe quelconque, les m classes

$$(B) \qquad B,\ BA,\ BA^2,\ \ldots,\ BA^{m-1}$$

seront aussi différentes entre elles, et deux complexes de m classes chacun, tels que le précédent (B) et le suivant :

$$(C) \qquad C,\ CA,\ CA^2,\ \ldots,\ CA^{m-1},$$

seront ou identiques ou entièrement différents; s'il se trouve, en effet, dans les deux à la fois, une seule et même classe $BA^r = CA^s$, on aura $C = BA^{r-s}$, d'où il s'ensuit immédiatement que les m classes du système (C) coïncident complétement avec celles du complexe (B). Donc le système de toutes les h classes se compose d'un nombre déterminé g de tels complexes différents entre eux, et, comme

chaque complexe contient m classes différentes, on aura $h = mg$, c'est-à-dire que l'exposant m, auquel appartient une classe A, est toujours un diviseur du nombre de classes h. Donc, pour toute classe A, on a le théorème

$$A^h = 0.$$

Maintenant, si $\mathfrak{a}$ est un idéal quelconque d'une classe quelconque A, $\mathfrak{a}^h$ appartiendra à la classe A^h, et par suite à la classe principale, c'est-à-dire que la $h^{\text{ième}}$ puissance de tout idéal est un idéal principal.

Par ce théorème important on arrive à concevoir la notion d'*idéal* sous un nouveau point de vue, auquel on peut rattacher en même temps une définition précise des *nombres idéaux*. Soit $\mathfrak{a}$ un idéal quelconque, et $\mathfrak{a}^h = \mathfrak{o}\alpha_1$; en désignant maintenant par α un nombre quelconque de l'idéal $\mathfrak{a}$, α^h sera contenu dans $\mathfrak{a}^h$, et, par suite, divisible par le nombre α_1, et il s'ensuit de là (§ 13, 2°) que α est divisible par le nombre entier $\mu = \sqrt[h]{\alpha_1}$, lequel toutefois n'appartient pas en général au corps Ω. Mais, réciproquement aussi, si α est un nombre entier appartenant au corps Ω et divisible par μ, α^h sera divisible par $\mu^h = \alpha_1$, et, par suite, $(\mathfrak{o}\alpha)^h$ le sera par $\mathfrak{o}\alpha_1 = \mathfrak{a}^h$, et l'on en conclut aisément, d'après les lois générales de la divisibilité (§ 25), que $\mathfrak{o}\alpha$ est divisible par $\mathfrak{a}$, c'est-à-dire que α est un nombre de l'idéal $\mathfrak{a}$. Donc l'idéal $\mathfrak{a}$ *est composé* de tous les nombres entiers contenus dans Ω et divisibles par le nombre entier μ; pour cette raison nous dirons que le nombre μ, lors même qu'il n'est pas contenu dans Ω, est *un nombre idéal du corps* Ω, et qu'il *correspond* à l'idéal $\mathfrak{a}$. Ou, un peu plus généralement, un nombre algébrique entier μ est dit un nombre idéal du corps Ω, lorsqu'il existe une puissance de μ, à exposant positif entier r, qui est associée à un nombre *existant* η du corps Ω, et qu'en même temps il existe un idéal $\mathfrak{a}$ du corps Ω, qui satisfait à la condition $\mathfrak{a}^r = \mathfrak{o}\eta$; cet idéal $\mathfrak{a}$ est l'idéal correspondant au nombre idéal μ, et il est toujours, et seulement alors, un idéal principal, quand μ est associé avec un nombre existant du corps Ω. (*Voir* l'Introduction et le § 10.)

Nous terminerons nos considérations par la démonstration du théorème suivant, annoncé déjà plus haut (§ 14) :

Deux nombres algébriques entiers quelconques α, β *admettent*

un commun diviseur δ, *qui peut être représenté sous la forme* $\delta = \alpha\alpha' + \beta\beta'$, α' *et* β' *étant également des nombres algébriques entiers.*

Démonstration. — Admettons que les deux nombres α, β soient différents de zéro, le théorème étant évident dans le cas contraire. Alors il existe toujours, comme il est aisé de s'en convaincre, un corps fini Ω, contenant les deux nombres α, β, et soit encore $\mathfrak{o}$ le domaine de tous les nombres entiers de ce corps, et de plus h le nombre des classes d'idéaux. Posons maintenant

$$\mathfrak{o}\alpha = \mathfrak{a}\mathfrak{d}, \quad \mathfrak{o}\beta = \mathfrak{b}\mathfrak{d}, \quad \mathfrak{d}^h = \mathfrak{o}\delta_1,$$

$\mathfrak{d}$ étant le plus grand commun diviseur de $\mathfrak{o}\alpha$, $\mathfrak{o}\beta$, et δ_1 étant contenu dans $\mathfrak{o}$. Puisque α^h, β^h sont divisibles par $\mathfrak{d}^h$, on peut poser

$$\alpha^h = \alpha_1\delta_1, \quad \beta^h = \beta_1\delta_1, \quad \mathfrak{o}\alpha_1 = \mathfrak{a}^h, \quad \mathfrak{o}\beta_1 = \mathfrak{b}^h,$$

α_1, β_1 étant pareillement contenus dans $\mathfrak{o}$. Comme, en outre, $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux premiers entre eux, $\mathfrak{o}$ sera aussi le plus grand commun diviseur de $\mathfrak{o}\alpha_1$, $\mathfrak{o}\beta_1$, et, comme le nombre 1 est contenu dans $\mathfrak{o}$, il se trouvera dans $\mathfrak{o}$ deux nombres α_2, β_2 satisfaisant à la condition

$$\alpha_1\alpha_2 + \beta_1\beta_2 = 1, \quad \text{ou} \quad \alpha^h\alpha_2 + \beta^h\beta_2 = \delta_1.$$

Si l'on pose maintenant

$$\delta_1 = \delta^h,$$

le nombre entier δ sera un commun diviseur entre α et β, puisque α^h, β^h sont divisibles par δ_1, et par conséquent on pourra poser, h étant $\geqq 1$,

$$\alpha_2\alpha^{h-1} = \alpha'\delta^{h-1}, \quad \beta_2\beta^{h-1} = \beta'\delta^{h-1},$$

α', β' désignant des nombres entiers qui satisfont à la condition $\alpha\alpha' + \beta\beta' = \delta$. C. Q. F. D.

Si l'un au moins des deux nombres α, β est différent de zéro, le nombre δ, aussi bien que tout nombre qui lui sera associé, méritera le nom de *plus grand* commun diviseur de α, β. Si δ est une unité, α, β pourront être dits des *nombres premiers entre eux*, et deux pareils nombres jouissent de la propriété caractéristique que tout nombre μ divisible par α et par β l'est aussi par le produit $\alpha\beta$;

car des égalités $\mu = \alpha\alpha'' = \beta\beta''$ et $1 = \alpha\alpha' + \beta\beta'$ on tire

$$\mu = \alpha\beta(\alpha'\beta'' + \beta'\alpha''),$$

et la conclusion réciproque est également permise, lorsque α, β sont tous les deux différents de zéro.

TABLE DES MATIÈRES.